NOVEL DESIGNS OF NONLINEAR COMPONENT FOR BLOCK CIPHERS AND ITS APPLICATIONS IN DIVERSE SECURITY SYSTEMS

by

Syeda Iram Batool Naqvi

Submitted to the Department of Mathematics
on February 28, 2018, in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Abstract

The improvement of the web make individuals bit by bit acquainted with transmit computerized data through different systems, the data incorporate content, advanced pictures and sight and sound data, and so on. Due to the extensive scale use of sight and sound innovation, advanced pictures turn into a critical method for correspondence. It is frequently evident that an expansive piece of this data is either classified or private. Therefore, extraordinary security procedures have been utilized to give the required insurance. With the headways of media and systems advances, an immense number of computerized pictures now transmitted over the Internet and through remote systems for advantageous getting to and sharing. Sight and sound security, as a rule, is given by a technique or an arrangement of strategies used to ensure the interactive media content. These days, we are living in a time where data is the extremely significant asset to us. Subsequently securing the data turns into all the more important. The correspondence media through which we send information does not give information security, so different techniques for securing information are required.

Data hiding/stowing away assumes an exceptionally critical part today. It gave techniques to encoding the data with the goal that it winds up muddled for any unintended client. There are three noteworthy data concealing methods to be specific watermarking, cryptography and steganography. Crypt means “hidden or secret” and graphein means “writing”. The term has been gotten from Greek dialect. Cryptography is a craft of changing information into a mixed up arrange called ciphertext. The recipient at another side, interprets or unscramble the message into plain content. Cryptography gives information secrecy, information uprightness, validation, and non-denial. Secrecy is constraining access or setting the confinement on specific sorts of data. Honesty is keeping up and guaranteeing the exactness of information being conveyed, i.e, the data contains no adjustment, erasure and so forth. Verification guarantees the character of sender and beneficiary of the data. Non-disavowal is the capacity to guarantee that the sender or beneficiary can’t preclude the legitimacy from securing their mark on the sending data that they started.

A watermark is a conspicuous picture or example that is inspired onto paper, which gives confirmation of its validness. Watermark shows up as different shades of softness/obscurity when seen in transmitted light. Watermarks are regularly observed as security highlights to

banknotes, identifications, postage stamps and other security papers. Computerized watermarking is an augmentation of this idea in the advanced world. Today there have been such a large amount of information over the web that it has constrained us to utilize systems that can secure responsibility for media. Robbery of computerized data is exceptionally normal, be it pictures, content, sound or video. These can be delivered and circulated effectively. Along these lines, it turns out to be critical to discover who is the proprietor of the report. Computerized watermarking is a standout amongst other answers for avoid illicit duplicating, altering and redistributing mixed media information. Encryption of sight and sound items keeps an interloper from getting to the substance without a legitimate unscrambling key. Yet, once the information is unscrambled, it can be copied and dispersed illicitly. Copyright insurance, information verification, secretive correspondence and substance ID can be accomplished by advanced watermarking. Computerized watermarking is a system to implant copyright or other data into the fundamental information. The implanted information ought to keep up the nature of the host flag. An advanced watermark is an example of bits embedded into a computerized picture, sound and video record that recognizes the document's copyright data.

Watermarking procedures is to give a proof of responsibility for information by inserting copyright articulations into a video or into a computerized picture. Watermarking convey an assortment of procedures how to stow away critical data, in an imperceptible as well as irremovable route, in a picture sound and video information. Watermarking are principle parts of the quick creating region of data covering up. Watermarking is an entirely unexpected method from cryptography. Cryptography just gives security by encryption and unscrambling. Dissimilar to Cryptography, watermarks can ensure content even after they are decoded. Computerized watermarking has gotten significant consideration as a supplement to cryptography for the security of advanced substance, for example, music, video, and pictures. Cryptography gives a way to secure conveyance of substance to the buyer. True blue shoppers are expressly or certainly given a key to unscramble the substance so as to view or hear it out. Strikingly, steganography receives a substitute methodology disconnected from everything the evidence that even a correspondence is happening. Steganography is changing the photo in a way that selects the sender and the proposed recipient can perceive the message sent through it. It is imperceptible, and in this way, the revelation isn't basic. It is a prevalent technique for sending secret messages than encoded messages or cryptography as it doesn't pull in respect for itself. The information concealed by a watermarking structure is always identified with the propelled question be guaranteed or to its proprietor while steganographic systems basically cover any information. The quality criteria are similarly extraordinary since steganography is generally stressed over the revelation of the covered message while watermarking concerns potential ejection by a privateer. The steganographic exchanges are ordinarily point-to-point (among sender and beneficiary) while watermarking techniques are regularly one-to-many.

This thesis mainly concern about cryptography, watermarking and steganographic techniques. The construction of different techniques in cryptography, watermarking and steganography is always been open task. Theses construction involves various mathematical structures which includes Boolean functions, finite Galois field and Galois ring. The construction of an important nonlinear component of block cipher namely substitution boxes are based on Boolean functions. The nonlinear component simply provides confusion capability in any information hiding techniques which is a fundamental component while constructing strong block cipher according to the Shannon theory of confusion and diffusion. Our main concern here is to pro-pose new algorithms for the construction of nonlinear component and utilize these in diverse multimedia applications. The basic cryptographic properties of S-boxes are discussed in chapter 1. The construction of new small S-boxes based watermarking and steganographic schemes were designed in chapters 2, 3 and 4 respectively. The cryptographic algebraic analyses play a vital role in order to test the validity of any component of block cipher specifically S-boxes. Moreover, there are several cryptographically strong algebraic analyses were developed in literature. Keeping in view the importance of these analyses, we have also tried to design a novel and innovative cryptographic analyses to check the strength of any S-boxes in chapter 5. The idea of Galois field is then replaced with Galois ring for the construction of strong S-boxes. The technique of chapter 6 is an innovative in the area of cryptographic algorithms development. The highly nonlinear Boolean functions observed in this construction which break the existing upper bound on nonlinearity of Boolean functions. Moreover, these functions are less balanced and more non balanced which qualify these Boolean functions to be near to bent Boolean functions. The idea of symmetric group S8 is applied to S-box based on which consequently generate 8! new S-boxes which surely add confusion capability in each frame of the proposed video encryption techniques. This novel and efficient video encryption technique is formally presented in chapter 7. The idea of more than one key is used in public key cryptography where various algorithms were developed already in literature whereas the single key based algorithms use only confusion and diffusion principles. In this sequel, the novel public-key cryptosystem that uses large abelian subgroup of general linear group of units of local ring of degree 2 is developed for different set of plaintext i-e., and in chapter 8. Moreover in chapter 8, based on general linear group, we have extended Diffie Hellman key exchange algorithm over matrices by incorporating chebyshev polynomials of first and second kind. Finally, the conclusions with future directions and recommendation are given in chapter 9.

Contents

Chapter 1

Preliminaries of Boolean Functions and Data Security

As the generation, stockpiling, and trade of data turn out to be broader and imperative in the working of social orders, the issue of shielding the data from unintended and undesired utilization turns out to be more unpredictable. In current social orders, insurance of data includes numerous associated innovative and approach issues identified with data privacy, integrity, anonymity, and authenticity, utility etc.

Data concealing procedures are getting much consideration today. Digital sound, video, and pictures are progressively outfitted with recognizing yet indistinct imprints, which may be consist of concealed copyright marks or some registration number or even help to avoid unapproved replicating straightforwardly. Digital watermarking and steganography may ensure data, cover insider facts, or are utilized as center natives in advanced rights administration plans. There are three noteworthy information concealing methods famously: watermarking, cryptography and steganography. We essentially talk about cryptography in this part because of its significance in Boolean algebra other two writes will be examined in different areas of this section.

Cryptography is the study of giving security to data and assets by utilizing suitable innovations. Cryptography makes secure sites and electronic safe transmissions conceivable. For a website to be secure the greater part of the information communicated between the PCs where the information is kept and where it is gotten must be scrambled. Because of the vast number of business exchanges on the web, cryptography is exceptionally entered in guaranteeing the security of the exchanges. Cryptography enables you to believe in your electronic exchanges. Encryption is utilized as a part of electronic exchanges to secure information, for example, account numbers and exchange sums, computerized marks supplant written by hand marks or mastercard approvals, and open key encryption gives privacy. Key administration is a vital perspective in encryption that enables you to apply basic encryption approaches over all information on all oversaw gadgets.

Cryptography in advanced world offers three center zones that shield you and your information from endeavor robbery, burglary or an unapproved utilization of your information and conceivable misrepresentation. Cryptography cover these basic authentication, integrity, and privacy.

The vocations of cryptography have colossally stretched out in the most recent years, as the utilization of the web has detonated. A most basic motivation behind cryptography is to connect with two social events to quietly present over an uncertain line of correspondence. This construes any adversary can't recoup the message (additionally called plaintext). The most comprehensively saw movement in cryptography is encryption and unscrambling. The term encryption depicts the distinction in the plaintext into the ciphertext. In the event that the ciphertext is utilized as a commitment to the turnaround change, by then we recuperate the plaintext. This portrays the unscrambling of a ciphertext.

We discuss symmetric key cryptography if the encryption change is unimportant related to the modify deciphering change. In case the encryption key can be made open, we discuss open key cryptography. This headway came up in the mid 1970's when Diffie and Hellman issued their article "New Directions in Cryptography".

Public key cryptography is consistently attractive over symmetric key cryptography since it grants to pass on protected without having effectively normal keys. In the late 1940s, Shannon [1] displayed the vital thoughts of disarray and dissemination to achieve security in cryptosystems. Disarray thinks the association between the key and the ciphertext as brain boggling as would be judicious. This is reflected in the nonlinearity of portions of the cryptosystem. Dispersion infers that the ciphertext depends on upon the plaintext in an unusual way. In this way, we have scattering while at the same time changing a little piece of plaintext prompts to an immense contrast in the ciphertext.

The inquiry develops whether there are capacities that can be utilized to achieve this. We will exhibit that suitable Boolean functions capacities easily give perplexity/ confusion and furthermore diffusion/ dispersion. Nonlinear parts of block ciphers and Boolean functions have a quite vital system of any data security schemes. These two imperative segments are firmly connected by direct change. That is, a nonlinear segment is by and large included distinctive exceptional yield Boolean functions, yet in the event that it is changed to only a solitary bits or different bits, is indistinguishable to a Boolean function. The S-box is a lone nonlinear segment of any block cipher which is capable confusion in any symmetric cryptographic techniques.

Boolean mapping are much of the time utilized as a part of the private key stream creation methodology of stream ciphers algorithms as these transformations are well proper for accepting bits of direct criticism move enrolls as contribution to request to go along with them as emphatically as conceivable to produce the single mystery key stream. Moreover, Boolean transforms have likewise displayed some critical properties, which are fundamental to restrict the great sort of assaults, so these mapping are a vital part in all stream and block ciphers.

The nonlinear component for block cipher is one of the vital importance in many block ciphers. It offers a method for making confusion in different blocks of bits for an absolutely divergent arrangement of yield bits. One thing which is imperative is the utilization of secure substitution boxes (those which hold amazing encryption properties) so the substitution shows a confounded relationship amongst info and yield bits of the substitution box. One of the fundamental elements of the substitution box, when utilized as a part of iterative round capacity, is to improve the exertion required to investigate any measurable structure in the protected information.

The nonlinear segments are talented to give the security of an encryption schemes by having brilliant encryption properties. Creating secure S-boxes to use them in different cryptosystems for growing their security is energy investigates issue. This is basically so in light of the way that the cryptanalytic structure winds up being more refined and with the difference in PC advancement that contributes also supporting and against secure correspondence.

The quality of nonlinear segment has a noteworthy bearing on secure correspondence.

Nonetheless, greater capacities generally require extra computational time and exertion keeping in mind the end goal to investigate their imperfections, so we pick up a decent computational multifaceted nature upgrade when attempting to discover extensive capacities with strikingly amazing measures of appealing encryption properties. This incorporates an extra piece of intricacy to the examination issue. Consequently, we oversee Boolean transformations and their cryptographic attributes.

This chapter of thesis for the most part exhibits a survey of hypothesis pertinent to the investigation of Boolean algebra, cryptography, watermarking and steganography.

1.1 Review on Boolean Functions in Cryptography

The investigation of Boolean functions is a boundless and summed up range in itself. This segment displays a little writing review of Boolean functions and their properties. To a specific degree, the overview gave in this part is a total association of that which is required for the peruser to totally know about the research displayed in this dissertation. Especially, we have talked about some vital cryptographic properties which are appropriate to this work.

1.1.1 Cryptographic Desirable Characteristics of Boolean Functions

The principle idea of this segment is to add some basic preliminary definitions on Boolean functions [11].

Definition 1 *[13] "Let $\mathbf{V}_2^n$ be the n dimensional vector space over the field of two element say $\mathbf{V}_2$. A Boolean function $g(x) : \mathbf{V}_2^n \rightarrow \mathbf{V}_2$ with the end goal that $x = (x_1, x_2, ..., x_n)$, is a mapping from n binary contributions to one yield. We let $\mathcal{B}_n$ speak to the arrangement of every one of the 2^{2^n} Boolean elements of n factors. Boolean function can be spoken to utilizing a different distinctive structures, each frame have diverse huge in data security primarily in calculations making and breaking."*

Definition 2 *[13] "A multi-esteemed or vector Boolean function is a change that maps a Boolean vector to another Boolean vector:"*

$$\xi : \mathbf{V}_2^n \rightarrow \mathbf{V}_2^m. \tag{1.1}$$

Definition 3 *[11] "A Boolean function $g : \mathbf{V}_2^n \to \mathbf{V}_2$ is viewed as linear iff it is a linear function from the vector space $\mathbf{V}_2^n$ to the vector space $\mathbf{V}_2$. This adds up to stating"*

$$\mathcal{L}_\alpha(x) = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus ... \oplus \alpha_n x_n, \tag{1.2}$$

where $\oplus$ denotes bitwise XOR operation and $\alpha_i \in \mathbf{V}_2^n$.

Definition 4 *[11] "The arrangement of affine Boolean functions is the arrangement of linear Boolean functions and their complements"*

$$A_{\alpha,c} = \mathcal{L}_\alpha(x) \oplus c, \tag{1.3}$$

where $x \in \mathbf{V}_2^n$.

Definition 5 *[10] "The Hamming-weight* $\mathbf{wt}(g)$*, of an n-variable Boolean function is a simple a function $g : \mathbf{V}_2^n \to \mathbf{V}_2$ which gives number of 1's in the truth table of g."*

Definition 6 *[10] "The Hamming-distance as the number of arguments where g and h have a difference, that is"*

$$d(g, h) = \#\{x \in \mathbf{V}_2^n \mid g(x) \neq h(x)\} = \mathbf{wt}(g \oplus h. \tag{1.4}$$

Definition 7 *[113] "The correlation value between two Boolean functions g and h is defined by"*

$$C(g, h) = 1 - \frac{d(g, h)}{2^{n-1}}.$$

Definition 8 *[13] "A Boolean function $g \in \mathcal{B}_n$ is said to be a balanced if output column in the truth table contains equal numbers of zeros and one. A function is balanced if its sequence is balanced that is* $\mathbf{wt}(g)$ *=2^{n-1}."*

It is easy to see that there are $\binom{2^n}{2^{n-1}}$ many balanced functions in the set of all $n-$variable Boolean functions. Note that the combining function in any cryptographic system need to be balanced.

Definition 9 *[11] "The autocorrelation function $\widehat{r}_{\widehat{g}}(a)$ with a shift $a \in \mathbf{V}_2^n$ is defined as"*

$$\widehat{r}_{\widehat{g}}(a) = \sum_{x \in \mathbb{Z}_2^n} \widehat{g}(x).\widehat{g}(x \oplus a). \tag{1.5}$$

Definition 10 *[10] "The algebraic degree/order of a Boolean function $g(x)$, denoted by deg(g), is defined to be the number of variables in the largest product term of the function's ANF having a non-zero coefficient."*

Definition 11 *The nonlinearity of a Boolean function g is denoted by N_g and is defined as follows*

$$N_g = d(g, \mathcal{A}_n) = \min_{\alpha \in A_n} d(g, \alpha). \tag{1.6}$$

Example 12 *Let $n = 2$, $g(x) = x_1 x_2$ and $a_i \in \mathbf{V}_2$. Then any affine function can be expressed as*

$$\Lambda_i(x) = a_0 \oplus a_1 x_1 \oplus a_2 x_2.$$

By taking all the combinations of a_i' s, we can generate all affine functions for n=2 and they are presented in the table. To find the nonlinearity of g, we calculate the distance between g and all affine functions that are presented in the following table. The minimum Hamming distance is nonlinearity of g.

Table 1.1: Distance between g and all affine functions.

	Affine functions							
g	Λ_1	Λ_2	Λ_3	Λ_4	Λ_5	Λ_6	Λ_7	Λ_8
0	0	0	0	0	1	1	1	1
0	0	1	0	1	1	0	1	0
0	0	0	1	1	1	1	0	0
1	0	1	1	0	1	0	0	1
$d(g, A_i)$	1	1	1	3	3	3	3	1

$$d_{\min} = 1 \Rightarrow N_g = 1.$$

Definition 13 *[10] "The Walsh transform of a function g on $\mathbf{V}_2^n$ is a map $\Omega : \mathbf{V}_2^n \to \mathbb{R}$ defined by"*

$$\Omega(g)(u) = \sum_{x\in\mathbb{Z}_2^n} g(x)(-1)^{<u,x>}, \tag{1.7}$$

where $< u, x >$ is the canonical scalar product.

Definition 14 *[13] "The Walsh-Hadamard matrix of order 2^n, signified by WH_n is produced by the recursive connection"*

$$WH_n = \begin{bmatrix} WH_{n-1} & WH_{n-1} \\ WH_{n-1} & -WH_{n-1} \end{bmatrix} = WH_1 \otimes WH_{n-1}, \tag{1.8}$$

for $n = 1, 2, ...and\ WH_0 = (1)$.

Theorem 15 *[13] "The nonlinearity of a Boolean function g can also be controlled by utilizing Walsh transform which is given below:"*

$$N_g = 2^{n-1} - \frac{1}{2}\max_{u\in\mathbb{Z}\ _2^n} \left|\Omega(\widehat{g})(u)\right|. \tag{1.9}$$

Definition 16 *[10] "A function $g : \mathbf{V}_2^n \to \mathbf{V}_2^m$ has the avalanche impact, if a normal of 1/2 of the yield bits change at whatever point a solitary information bit is complemented i.e.,"*

$$\frac{1}{2^n}\sum_{u\in\mathbb{Z}_2^n} \mathbf{wt}(g(x^i) - g(x)) = \frac{m}{2}, \quad for\ all\ i = 1, 2, ..., n. \tag{1.10}$$

Definition 17 *[10] "A function $g : \mathbf{V}_2^n \to \mathbf{V}_2^m$ of n input bits into m yield bits is said to be complete, if each yield bit relies upon each information bits, i.e. change at whatever point a solitary information bit is supplemented i.e."*

$$\forall\ i = 1, 2, ..., n,\ \ j = 1, 2, ..., m,\ \ \exists\ x \in \mathbf{V}_2^n\ \ \ with\ \ (g(x^i))_j \neq (g(x))_j. \tag{1.11}$$

Definition 18 *[13] "A function $g : \mathbf{V}_2^n \rightarrow \mathbf{V}_2^m$ fulfills the strict avalanche criterion, if each yield bit changes with a likelihood 1/2 at whatever point a solitary info bit is supplemented i.e."*

$$\forall\ i = 1, 2, ..., n,\ \ j = 1, 2, ..., m,\ \ Prob(g(x^i))_j \neq Prob(g(x))_j = \frac{1}{2}. \tag{1.12}$$

1.2 Nonlinear Component of Block Ciphers (S-Box)

In this fragment, we by and by turning our trades to the zone of a nonlinear segment of block ciphers. The fundamental implications of S-box theory are given to enable the examination to work performed in this proposal. In like manner in this portion, an overview of huge cryptographic properties as associated with S-boxes is given.

1.2.1 Definition of Nonlinear Component and Types

We list beneath a few vital S-box definitions, together with a short depiction of some S-box kinds important to this exploration.

An $i \times j$ substitution box (S-box) is a mapping from i input bits to j output bits, $S : \mathbf{V}_2^i \rightarrow \mathbf{V}_2^j$. The output vector $S(x) = (s_1, s_2, ..., s_j)$ can be decomposed into m component functions $S_k : \mathbf{V}_2^i \rightarrow \mathbf{V}_2,\ k = 1, 2, ..., m$. There are 2^i inputs and 2^j possible outputs for an $i \times j$ S-box. Often considered as a look-up table, an $i \times j$ S-box, S, is normally symbolized as a matrix of size $2^i \times j$, indexed as S_k $(0 \leq k \leq 2^i - 1)$ each an $j-$bit entry. There are, generally speaking, three types of S-boxes: Straight, compressed and expansion S-boxes. A straight nonlinear component of block cipher number of input and out remains same for instance AES nonlinear component take same number input and produces same outputs. A compressible nonlinear component of block cipher consists of more number of inputs as compared to output, DES S-boxes are the example of compressible nonlinear component of block ciphers. A expansion nonlinear component take less number of input and produce more outputs bits in general.

1.2.2 Cryptographic Possessions of Nonlinear Components

While a large number of the Boolean capacity properties examined in past areas have calculated equivalences when connected to nonlinear components, there are principal contrasts in the way by which these properties are inferred. As a nonlinear component, is involved various part Boolean capacities, watch that while considering the cryptographic properties of a nonlinear component, it isn't adequate to consider the cryptographic properties of the segment Boolean capacities separately. Or maybe, it is likewise important to consider the cryptographic properties of all the straight mixes of the part capacities. This is represented in the accompanying choice of applicable nonlinear component of block ciphers properties.

A $n \times m$ nonlinear component of block cipher which is adjusted is one whose part Boolean capacities and their direct mixes are altogether adjusted. In view of this adjust, there does not exist an exploitable inclination in that the similarly likely number of yield bits over all yield vector blends guarantees that an aggressor can't inconsequentially estimated the capacities or the yield.

The outstanding idea of disarray because of Shannon [1] is depicted as a technique for guaranteeing that in a figure framework a mind boggling relationship exists between the ciphertext and the key material. This thought has been extrapolated to imply that a noteworthy dependence on some type of substitution is required as a wellspring of this perplexity. The perplexity in a figure framework is accomplished using nonlinear segments. Not surprisingly, substitution boxes have a tendency to give the principle wellspring of nonlinearity to cryptographic figure frameworks. We now characterize the measure of nonlinearity for a $n \times m$ nonlinear component of block cipher. Since nonlinear component of block cipher is consist of single or multiple values Boolean functions, therefore all the basic properties which were defined for Boolean functions can be equally applicable for classification of cryptographically secure nonlinear component for block ciphers.

Definition 19 *The bit independence comparing to the impact of the i^{th} input bit change on the j^{th} and k^{th} bits of is β^{e_i} :*

$$Bic(\beta_j, \beta_k) = \max_{1 \leq i \leq m} |\boldsymbol{corr}(\beta_j^{e_i}, \beta_k^{e_i})|. \tag{1.13}$$

The bit independent criterion (BIC) for nonlinear component for block cipher function f is defined as follows:

$$Bic(f) = \max_{\substack{1 \leq j,k \leq m \\ j \neq k}} Bic(\beta_j, \beta_k), \tag{1.14}$$

which indicates how close is fulfilling the BIC [107].

Linear and Differential Cryptanalysis

Linear and differential cryptanalysis are connected assaults utilized basically against iterative symmetric key piece figures. An iterative figure (additionally called an item figure) directs different rounds of encryption utilizing a subkey for each round. Illustrations incorporate the Feistel Network utilized as a part of DES and the State rounds utilized as a part of AES. In the two assaults, a cryptanalyst examine changes to the transitional ciphertext between rounds of encryption. The assaults can be joined, which is called differential linear cryptanalysis. An objective of solid encryption is to deliver ciphertext that seem arbitrary where a little change in a plaintext brings about an irregular change in the subsequent ciphertext [105].

Linear Cryptanalysis Linear cryptanalysis is a known plaintext assault that expects access to a lot of plaintext and ciphertext sets scrambled with an obscure key. It centers around measurable investigation against one round of unscrambling on a lot of ciphertext. The cryptanalyst decodes each figure content utilizing all conceivable subkeys for one round of encryption and concentrates the subsequent middle figure content to look for the slightest irregular outcome. A subkey that delivers the minimum arbitrary middle cipher6 for all figure writings turns into an applicant key (the in all likelihood subkey).

Differential Cryptanalysis Differential cryptanalysis is a picked plaintext assault that looks to find the connection between ciphertext delivered by two related plaintexts. It centers around measurable examination of two data sources and two yields of a cryptographic calculation. A plaintext combine is made by applying a Boolean restrictive or (XOR) activity to a plain content. For instance, XOR the rehashing twofold string 10000000 to the plaintext. This makes a little contrast (thus the term differential cryptanalysis) between the two. The cryptanalyst at that point encodes the plaintext and its XOR-ed combine utilizing all conceivable subkeys, and it looks for indications of nonrandomness in each moderate ciphertext match. The subkey that makes the minimum irregular example turns into the applicant key [110].

Definition 20 *For a given vector Boolean function* $g : \mathbf{V}_2^n \rightarrow \mathbf{V}_2^m$ *it is defined the linear approximation table which elements are*

$$LAT_g(a,b) = \#\{x \in \mathbb{Z}_2^n | a.x = b.g(x)\} - 2^{n-1}, \tag{1.15}$$

where $a \in \mathbf{V}_2^n,\ b \in \mathbf{V}_2^m \backslash \{0\}$.

Definition 21 *For any given* Δ_x, Δ_y , Γ_x, Γ_y $\in \mathbf{V}_2^n$ *,the linear and differential approximation probabilities for each vector Boolean function (S-box) are defined as:*

$$LP^{S_i}(\Gamma_y \quad \rightarrow \quad \Gamma_x) = \left(2 \times \frac{\#\{x \in \mathbf{V}_2^n | x\Gamma_x = S_i(x)\Gamma_y\}}{2^n} - 1\right), \tag{1.16}$$

$$DP^{S_i}(\Delta_x \quad \rightarrow \quad \Delta_y) = \left(\frac{\#\{x \in \mathbf{V}_2^n | S_i(x) \oplus S_i(x \oplus \Delta_x) = \Delta_y\}}{2^n}\right), \tag{1.17}$$

where $x\Gamma_x$*, denotes the parity* (0 *or* 1) *of the bitwise product of* x *and* Γ_x *[110], [102], [105], [111].*

Definition 22 *The maximum linear and differential approximation probabilities of vector Boolean function (S-boxes) are defined as [112], [114]:*

$$p = \max_i \max_{\Gamma_x, \Gamma_y} LP^{S_i}(\Gamma_y \rightarrow \Gamma_x), \tag{1.18}$$

$$q = \max_i \max_{\Delta_x, \Delta_y} DP^{S_i}(\Delta_x \rightarrow \Delta_y). \tag{1.19}$$

Definition 23 *[87] "An element* $a \in \mathbf{V}_2^n$ *is a fixed point (opposite fixed point) of* $g : \mathbf{V}_2^n \rightarrow \mathbf{V}_2^m$ *if* $g(a) = a$ $(g(a) = \overline{a})$*."*

Definition 24 *[87] "The resistance of S-boxes to DPA attacks called transparency order of an S-box* $S = (s_1, s_2, ..., s_n)$ *on* $\mathbf{V}_2^n$ *is defined as:"*

$$T_F = \max_{\beta \in \mathbf{V}_2^n} \left(|n - 2HW(\beta)| - \frac{1}{2^{2n} - 2^n} \sum_{a \in \mathbf{V}_2^n} \left| \sum_{v \in \mathbf{V}_2^n} (-1)^{v.\beta} W_{D_a S(u,v)} \right| \right), \tag{1.20}$$

where $W_{D_aS(u,v)}$ is the Fourier transform of the sign function derivative of S with respect to vector $a \in \mathbf{V}_2^n$, $D_aS : x \longmapsto S(x) \oplus S(x \oplus a)$. The Fourier transform of the sign function derivative of S is defined as follows

$$W_{D_aS(u,v)} = \sum_{a \in \mathbf{V}_2^n} (-1)^{v.\{S(x) \oplus FSx \oplus a)\} \oplus u\ x} \tag{1.21}$$

Definition 25 *[87] "For any positive integers n and m, a function $S : \mathbf{V}_2^n \to \mathbf{V}_2^m$ is called differentially δ-uniform if for every $a \in \mathbf{V}_2^n \setminus \{0\}$ and every $b \in \mathbf{V}_2^m$, the equation $S(x) + S(x + a) = b$, admits at most δ solutions."*

Definition 26 *[87] "The sum of square indicator, also derived from the autocorrelation function, may be calculated as follows:"*

$$\sigma = \sum \widehat{r}^2(a) \qquad a \in \{1, 2, ..., 2^N - 1\}. \tag{1.22}$$

Definition 27 *[87] "The Boolean function obtained by the product of the TTs of two Boolean functions f, g by $f.g$ (note that this product is different from the dot product between two vectors x, y). The algebraic immunity (AI) of a Boolean function f on $\mathbf{V}_2^n$ is defined as the lowest degree of the function $g : \mathbf{V}_2^n \to \mathbf{V}_2$ for which $f.g = 0$ or $(f \oplus 1).g = 0$. The function g for which $f.g = 0$ is called an annihilator of f . Denote the set of all annihilators of f by $An(f)$."*

Definition 28 *[87] "Let $S = (s_1, s_2, ..., s_n)$ be an $n \times s$ nonlinear component of block cipher. Denote by L the largest value in the difference distribution table on F , and by N the number of nonzero entries in the first column of the table. In either case the value 2^n in the first is not counted. Then we say that F is R-robust against the differential cryptanalysis, where R is defined by*

Definition 29 *Representing by L the biggest incentive in the difference distribution table on F, and by N the quantity of nonzero sections in the main segment of the table. In either case the esteem 2^n in the first isn't tallied. At that point we say that F is R-powerful against the differential cryptanalysis, where R is characterized by"*

$$R = \left(1 - \frac{N}{2^n}\right)\left(1 - \frac{L}{2^n}\right). \tag{1.23}$$

Definition 30 *[87] DPA work factor is identified with genuine examinations, where the execution is surveyed by a signal to noise ratio (SNR). As of now said, regardless of whether the DPA isn't uproarious, it doesn't permit to specifically detect the correct pinnacle (k=0) in light of the fact that there exists auxiliary pinnacles notwithstanding for wrong keys* ($k \neq 0$)*. Secondary peaks are modeled as noise. DPA qualify is in this manner evaluated by the accompanying idea of SNR. To the extent the DPA signal is concerned, adjusted S-box F fulfills:*

$$\begin{aligned} DPA(0) &= \sum_{i,j} 2^{-p} \sum_{x} \left((-1)^{\langle l_i \oplus l_j | S(x) \rangle} \right), && (1.24) \\ &= \sum_{i,j} \delta(l_i \oplus l_j) = q, && (1.25) \\ DPA &= 2^{-2p} \sum_{i,j} \sum_{x} (-1)^{S(x)_i} \left(\sum_{k} (-1)^{S(x \oplus k)_j} \right), && (1.26) \\ &= 0, \quad (because\ S\ is\ balanced). && (1.27) \end{aligned}$$

As a result, SNR DPA is defined as follows:

$$SNR_{DPA(S)} = q 2^{2p} \left(\sum_{x} \left(\sum_{i=0}^{p-1} (-1)^{S_i}(k) \right)^4 \right)^{-1/2}, \tag{1.28}$$

where $\widehat{f}\ (k) = \sum_{x} (-1)^{\langle x|k \rangle} f(x)$ *is the Hadamard-Walsh transform of the function.*

1.3 Review on Information Security Preliminaries

The essential of information security inside an affiliation has encountered two critical changes over the latest a significant drawn-out period of time. The security of information felt to be gainful to an affiliation was given on a very basic level by physical and administrative files, already the limitless of data planning equipment. An instance of the latter is workforce screening system used in the midst of securing process. An instance of the past is the use of harsh filling pantries with a blend dart to store fragile reports.

With the presence of the PC, the requirement for automated gadgets for guaranteeing reports and other information set away on the PC wound up mandatory. This is required for a structure like the time-sharing system and moreover sooner or later requires is impressively more extreme for systems that can be gotten to over an open telephone data framework or web.

The second enormous change that affected security is the presentation of passed on structures and the utilization of systems and correspondences working environments for passing on information between terminal client and PC. Structure security is required to ensure information while in development. Everything considered, sort out security term is deluding since all business, government and scholarly connection interconnected their information dealing with hardware with a storing up of interconnected structures.

Cryptography is a science that applies complex number-crunching and justification to plot strong encryption methodologies. Cryptography is moreover a craftsmanship. Cryptography empowers people to keep confide in the electronic world. People can do their business on an electric channel without worrying of dishonesty and misleading.

Right when people started cooperating on the web and anticipated that would trade finances electronically; the employments of cryptography for trustworthiness began to beat its use for security. These days, a colossal number of people interface electronically reliably by different means like messages, ATM machines, web business or telephones. The speedy augmentation of information transmitted electronically achieved an extended reliance on cryptography and approval. This section is devoted to introducing the preliminaries related to information security systems to be discussed in this thesis. We explicitly define the basics of the cryptography, watermarking and steganography primitives which will be helpful in subsequent chapters.

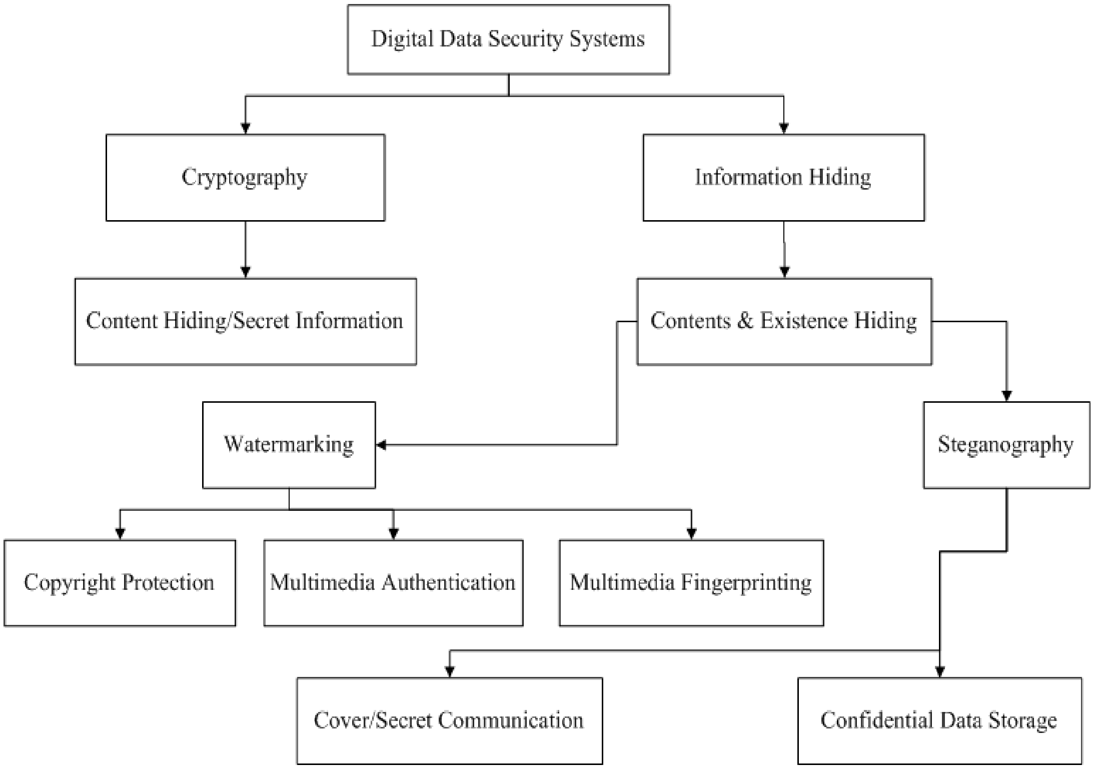

Digital Data Security Systems
Cryptography
Information Hiding
Content Hiding/Secret Information
Contents & Existence Hiding
Watermarking
Steganography
Copyright Protection
Multimedia Authentication
Multimedia Fingerprinting
Cover/Secret Communication
Confidential Data Storage

Fig. 1.1: Classification of information security systems.

1.4 Cryptology

Cryptology is the investigation of data security. The word cryptology is gotten from the Greek kryptos, which means covered up. Cryptology is the investigation of "mystery composing." In era of digitally advanced communication, secure information security is an important component of any nation.

1.4.1 Classification of Cryptology

The cryptology is additionally characterized by two branches cryptography and cryptanalysis. The term cryptography alludes to the workmanship or exploration of planning cryptosystems (to be characterized in no time), while cryptanalysis alludes to the science or craft of breaking them.

1.4.2 Basics Terminology of Cryptography

Plain Text

The plaintext is a simple information which can easily understand without any information.

Cipher Text

A message that come from some algorithm and which can't be understood with extra information.

Ciphers

A cipher/algorithm is a transformation that utilize the original message as an input and encoded message as an output is called cipher and some time algorithm.

Encryption

The process of transforming plaintext into ciphertext is encryption. The mathematical expression for encryption is given below:

$$C = E(P),$$

where P is plaintext, C is ciphertext and E is encryption function.

Decryption

The process of transforming encoded message into original message is called decryption. Let D is the decryption function, i.e.

$$P = D(C),$$

which means by applying the decryption process D to ciphertext C produces the plaintext P.

Key

A key is a simple information which is used to encrypt or decrypt plaintext and ciphertext. Fundamentally, key is a sort of knowledge which us used to that determines output of a cryptographic ciphers."

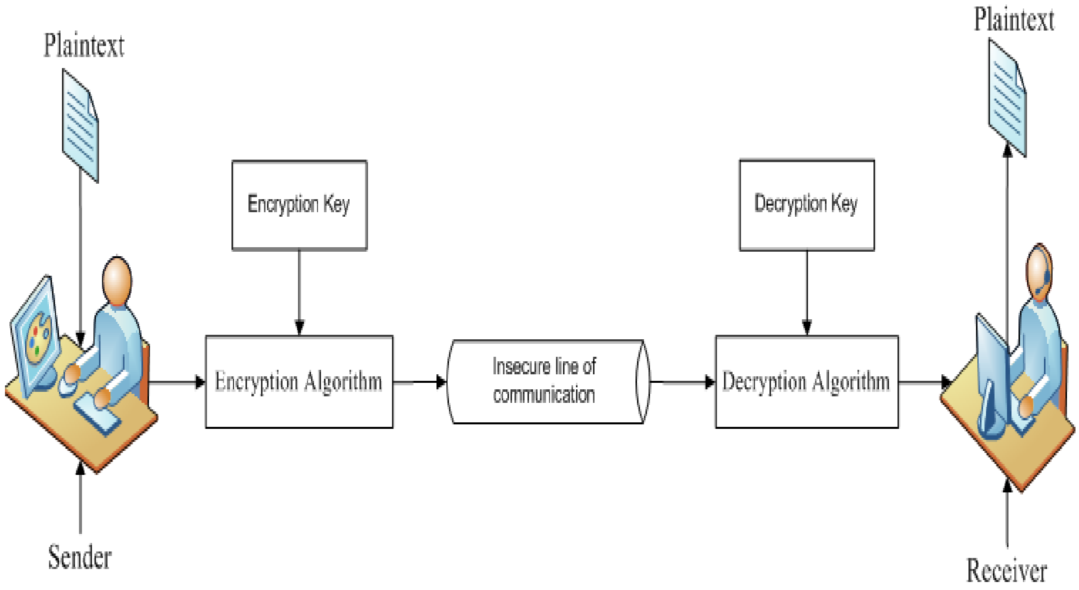


Fig. 1.2: Block diagram for encryption and decryption.

Definition 31 *A cryptosystem is a quintuplets* (M, C, K, E, D) *in which* M *is called the plaintext space;* C *is a called the ciphertext space;* K *is called the key space;* E *is an encryption rules;* D *is a decryption rules. For each* $K \in K$*, there is a function* $e_K \in E$ *and a corresponding function* $d_K \in D$ *such that for any plaintext message* $x \in P$*,* $d_K(e_K(x)) = x$*. Notice that this means* d_K *is the inverse of the function* e_K*.*

Definition 32 *A mapping* $T : X \to Y$ *is one-one or injective iff* $\forall\ a, b \in X,\ T(a) = T(b) \Rightarrow a = b$*.*

1.5 Prime Security Purposes of Cryptography

Cryptography is the art/craft of writing to secure communication in insecure lines of communications. There are four essential elements of cryptography today:

1.5.1 Confidentiality

Confidentiality/Privacy is the major security benefit gave by cryptography. It is a security benefit that keeps the data from an unapproved individual. It is once in a while alluded to as security or mystery. Secrecy can be accomplished through various means beginning from physical securing to the utilization of scientific calculations for information encryption.

1.5.2 Data Integrity

It is security benefit that arrangements with recognizing any change to the information. The information may get altered by an unapproved substance deliberately or accidently. Respectability benefit affirms that whether information is in place or not since it was last made, transmitted, or put away by an approved client. Information trustworthiness can't keep the adjustment of information, however gives a way to distinguishing whether information has been controlled in an unapproved way.

1.5.3 Authentication

Authentication/Verification gives the recognizable proof of the originator. It affirms to the collector that the information got has been sent just by a recognized and confirmed sender. Validation benefit has two variations:

i. Message authentication: recognizes the originator of the message with no respect switch or framework that has sent the message

ii. Person verification /authentication: is affirmation that information has been gotten from a particular element, say a specific site. Aside from the originator, verification may likewise give affirmation about different parameters identified with information, for example, the date and time of creation/transmission.

1.5.4 Non-repudiation

It is a security advantage that ensures that a component can't deny the obligation regarding past obligation or an action. It is an affirmation that the primary producer of the data can't deny the creation or transmission of the said data to a recipient or pariah. Non-disavowal is a property that is most alluring in conditions where there are chances of a contradiction in regards to the exchanging of data. For example, once a demand is sent electronically, a purchaser can't deny the purchase orchestrate, if the non-disavowal advantage was engaged in this trade.

1.6 Cryptographic Essentials

Cryptography natives/essentials are only the instruments and strategies that can be specifically used to give an arrangement of wanted security administrations:

1. Enciphering
2. One-to-one functions
3. Message verification codes (MAC)
4. Digital signatures

The accompanying table demonstrates the natives that can accomplish a specific security benefit without anyone else.

Table 1.2: Security services and its primitives.

Primitives ⟹	Encryption	Hash Function	MAC	Digital Signature
Services ⇓				
Confidentiality	Yes	No	No	Yes
Data Integrity	No	May be	Yes	Yes
Authentication	No	No	Yes	Yes
Non-repudiation	No	No	May be	Yes

Cryptographic natives are complicatedly related and they are regularly consolidated to accomplish an arrangement of wanted security administrations from a cryptosystem.

1.7 Classification of Cryptographic Algorithms

There are a few methods for categorizing cryptographic algorithms. For motivations behind this section, they will be sorted in light of the different amount of keys that are used at the time of encryption and unscrambling, and assist characterized by their request and use. The modern cryptographic algorithms can be classified into three following broad categories:

i. Private/Secret/Symmetric Key Cryptography

ii. Asymmetric/Public Key Cryptography

iii. One Way Hash Function

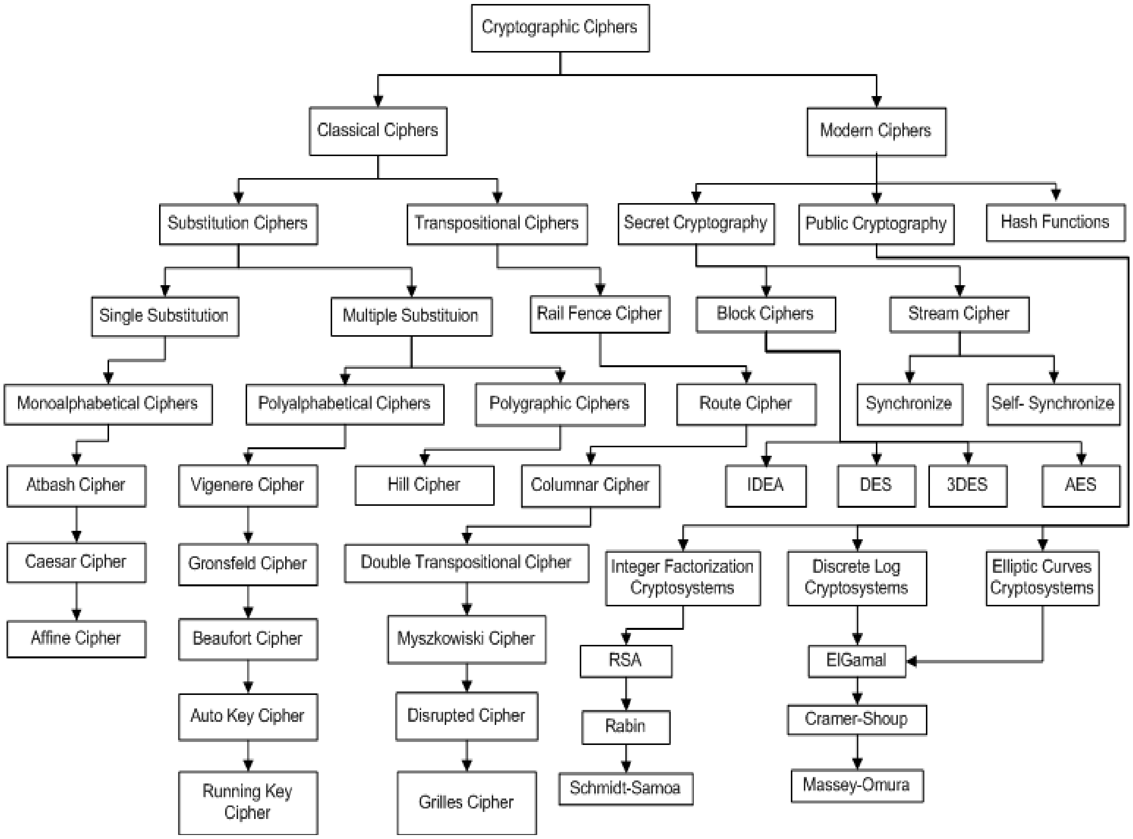


Fig. 1.3: Classification of cryptographic algorithms.

1.7.1 Private/Secret Key Cryptography

Private uses a single key for both encryption and unscrambling. Basically it is utilized for privacy and onfidentiality There are numerous private key algorithms such as DES and AES used in literature for the security of digital information. The secret key algorithms can further be classified into two sub-classes namely, block ciphers and stream ciphers which are defined in [18].

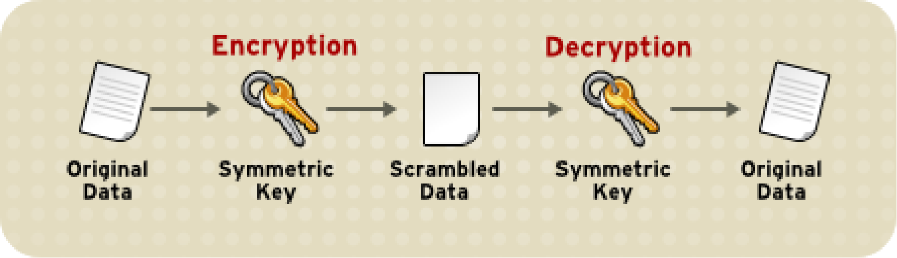


Fig. 1.4: Symmetric private-key encryption system.

1.7.2 Public Key Cryptography

Utilizes different keys for encryption and decryption; likewise called asymmetric encryption. Essentially utilized for authentication, non-repudiation, and key exchange. There are various public key encryption algorithms for instance RSA, Elgamal, Rabin and Elliptic curve cryptographic algorithms etc.

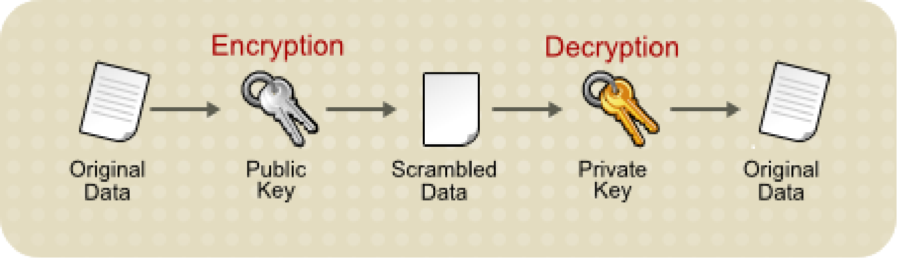


Fig. 1.5: Public-key encryption system.

1.7.3 Hash Function

Utilizations a numerical change to irreversibly "encode" information, giving a propelled extraordinary check. Essentially used for message respectability. Hash limits, moreover called message surveys and one-way encryption, are figuring that, in some sense, use no key. Hash limits, by then, give a measure of the trustworthiness of a record. Hash calculations that are in like way use today fuses message assimilation (MD) conspires, the safe hash calculation (SHA) and its distinctive variations.

1.7.4 Diffusion and Confusion

Confusion and diffusion are two properties of the activity of a safe algorithms in cryptography. Confusion and diffusion/dissemination were recognized by Claude Elwood Shannon in his paper, "Communication Theory of Secrecy Systems" distributed in 1949. In Shannon's unique definitions [1]:

i. Confusion makes the relationship between the key and the ciphertext as complex as possible

ii. Diffusion represents the characteristic that recurrence in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext

Dispersion is related with the reliance of the yield bits on the information bits. In a cipher with great dissemination, flipping an information bit should change each yield bit with a likelihood of one a large portion of (this is named the Strict Avalanche Criterion). Substitution (a control for supplanting plaintext images by another) has been recognized as a component for fundamentally perplexity (see S-box); then again transposition utilizing P-box (adjusting or swapping the request of images) is a strategy for dissemination, albeit different systems are likewise utilized as a part of present day hone, for example, straight changes (e.g. in AES, ShiftRow and Mix Column activities). Product ciphers utilize rotating substitution and transposition stages (rounds) to accomplish both perplexity and dispersion individually.

Current block ciphers utilize both perplexity and dispersion. The codebook parts of such frameworks give perplexity practically equivalent to however on a considerably more fabulous scale-a basic substitution. All around planned block ciphers spread any nearby insights all through the piece, along these lines utilizing the guideline of dispersion [1, 2].

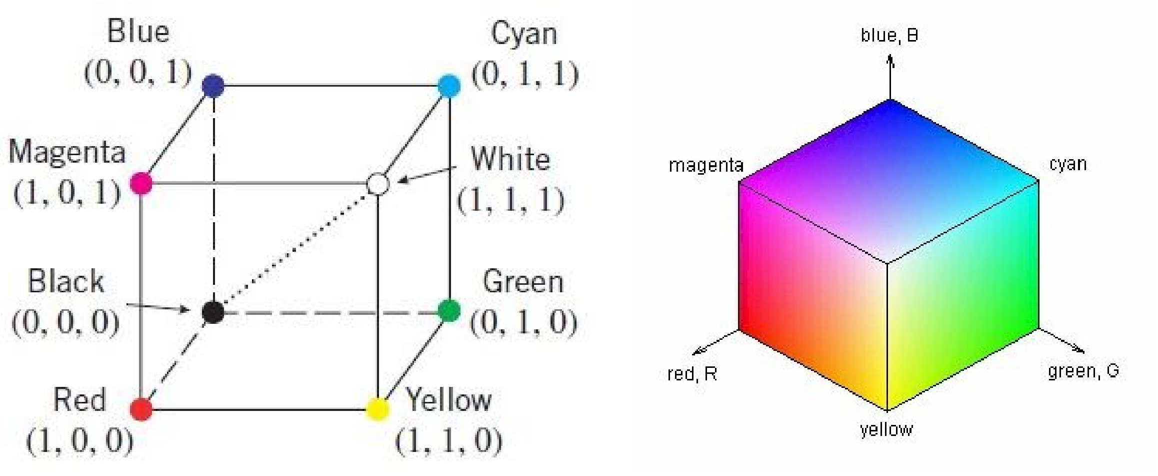
1.7.5 Digital image processing

Image process might be a strategy to play out a few operations on a photo, in order to ask an expanded image or to remove some accommodating information from it. it's a kind of signal processor inside which input is a photo and yield is likewise image or attributes/highlights identified with that image. These days, the imaging procedure is among rapidly developing advances. It frames center examination space inside building disciplines too.

Image handling is a strategy to play out a couple of exercises on a photo, with a particular true objective to get an enhanced picture or to isolate some accommodating information from it. It is a sort of banner taking care of in which input is a photo and yield may be picture or traits/features related with that photo. Nowadays, picture getting ready is among rapidly creating headways. It shapes focus inquire about an area inside building and programming designing orders too.

Digital Image

A picture is just a two dimensional exhibit. It is characterized by the scientific capacity $f(x, y)$ where x and y represents two arranges on a level plane and vertically. The estimation of $f(x, y)$ anytime is gives the pixel esteem by then of a picture running in the vicinity of 0 and 255. The measurements of the photo is really the measurements of this two dimensional cluster. These advanced pictures can be monochrome (bi-tone), grayscale or shading relying on the allowable force levels of every pixel i.e. regardless of whether every pixel is spoken to by just a single piece, $8-$bits or $24-$bits. As a rule, a monochrome picture can have just a single piece plane while there are 8-bit planes in a dark scale picture and 24 bit planes (8-bits each, as for the three channels Red, Green and Blue) in a shading picture. The slightest critical piece plane (LSB plane) is the plane that comprises of bits with least positional esteem ($2^0 = 1$) and the MSB plane (most noteworthy piece plane) comprises of bits with most astounding positional esteems i.e. $2^7 = 128$.



(*a*) (*b*)

Fig. 1.6: RGB color space.

1.8 Basics of Watermarking

Nowadays, billions of bits of data acquire into presence each a large portion of a second. What's more, because of extraordinary acknowledgment of the Internet alongside quick advancement of mixed media innovation, clients have more probability to utilize computerized information (picture, video and sound records, web distributed advanced storehouses and libraries). After all duplicating computerized information is a very sensitive issues of digital advanced world. Digital watermarking is an answer for these issues as it has different applications like copyright insurance, confirmation, secret communication, and estimation. E-trade, E-voting, medical safety, broadcasting observing, military and ordering can be ensured by computerized watermarking. Watermark stays in place to the cover picture regardless of the possibility that it is replicated, is the normal for watermarking. Consequently to guarantee responsibility for watermark is removed and tried. Digital watermarking is the strategy of installing a watermark in an interactive media object. This object might be picture, sound, video and any computerized content with the end goal of data covering up. Intense watermarking method ought to be chosen for strong watermark embedding [46]-[47].

1.9 Digital Watermarking

A computerized watermark or digital watermark is an example of bits embedded into an advanced medium (picture, sound or video). Such messages for the most part convey copyright data of the record. In any case, the principle contrast between them is that computerized watermarks should be imperceptible or possibly not changing the view of unique document, not at all like paper watermarks, which should be to some degree noticeable. For example, a digital camera that would use lossless watermarking to embed a biometric identifier together with a cryptographic hash value. A digital signature is a large unique integer generated by encrypting a hash value of a file, image, video, etc. The formal definition of watermarking is given as follows:

Definition 33 *A watermarking system is a quintuple* (C, W, K, E_K, D_K), *where* C *is space of cover image,* W *the set of all watermarks,* K *is the set of all possible keys,* C' *is the set of all original data with watermark. The two functions* $E_K : C \times W \times K \to C^{'}$, $D_K : C' \times K \to W$, *describe the embedding and detecting process.*

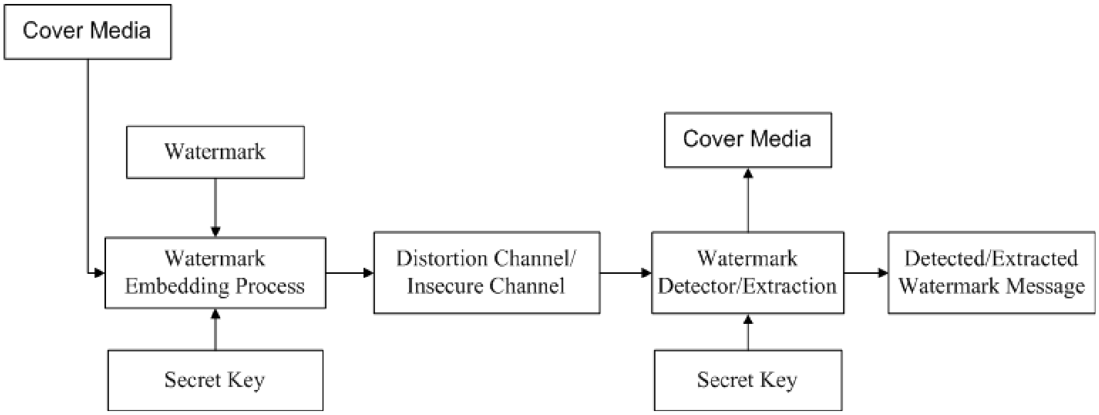

Cover Media
Watermark
Watermark Embedding Process
Secret Key
Distortion Channel/ Insecure Channel
Cover Media
Watermark Detector/Extraction
Secret Key
Detected/Extracted Watermark Message

Fig. 1.7: Basic procedure of digital watermarking.

1.9.1 Basic Terminologies of Watermarking

The general definitions of some common terms used in the area of watermarking are listed below:

Watermark The data to be covered up. The term watermark additionally contains an insight that the concealed data is straightforward like water.

Cover Media/Data The media utilized for conveying the watermark. At times the terms unique media, cover media and host media are additionally used to express it.

Watermark Data The computerized medium which contains the watermark.

Extraction The technique utilized for extricating the installed watermark from the watermark question.

Detection The technique utilized for identifying whether the given media containing a specific watermark.

1.9.2 Qualities of Computerized Watermarking

The necessities for picture watermarking can be dealt with as qualities, properties or characteristics of picture watermarking. Diverse applications request distinctive properties of watermarking. Necessities of picture watermarking fluctuate and result in different outline issues relying upon picture watermarking applications and reason. These necessities should be mulled over while outlining watermarking framework. There are fundamental five necessities as takes after [5].

Fidelity

Fidelity/Devotion is considered as a measure of perceptual straightforwardness or imperceptibility of watermark. It implies the similarity of un-watermarked and watermarked pictures. This perspective of watermarking mishandle limitation of human vision. Watermarking should not present unmistakable curves as it decreases business estimation of the watermarked picture.

Robustness

Watermarks ought not be expelled deliberately or inadvertently by basic picture handling activities. Thus watermarks ought to be strong against assortment of such assaults. Strong watermarks are intended to oppose typical handling. Then again, delicate watermarks are intended to pass on any endeavor to change computerized content.

Data Payload

Information payload is otherwise called limit of watermarking. It is the most extreme measure of data that can be covered up without debasing picture quality. It can be assessed by the measure of concealed information. This property portrays how much information ought to be implanted as a watermark with the goal that it can be effectively distinguished amid extraction.

Security

Secret key must be utilized for implanting and identification process in the event that security is a noteworthy concern. There are three kinds of keys utilized as a part of watermark frameworks: private-key, recognition key and open key. Hackers ought not have the capacity to expel watermark with hostile to figuring out research algorithm.

Computational Complexity

Computational many-sided quality shows the measure of time watermarking calculation takes to encode and decipher. To guarantee security and legitimacy of watermark, more computational unpredictably is required. On the other hand, constant applications require both speed and effectiveness.

1.10 Watermarking Attacks

There are distinctive possible malignant deliberate or surprising assaults/strikes that a watermarked question is presumably going to subject to. The availability of the broad assortment of pictures dealing with sensitive items made it possible to perform strikes on the quality of the watermarking structures. The purpose of these ambushes is shielding the watermark from playing out its arranged reason. A succinct introduction to various sorts of watermarking ambushes/attacks is given beneath:

1.10.1 Elimination Attack

Elimination Attack hopes to remove the watermark data from the watermarked dissent. Such ambushes abuse how the watermark is regularly an additional substance racket hail show in the host signal.

1.10.2 Intrusion Assault

Intrusion strikes are those which add additional confusion to the watermarked challenge. Lossy weight, quantization, plot, denoising, demodulation, averaging, and commotion storm are a couple of instances of this arrangement of ambushes.

1.10.3 Shapes Attacks

All controls that impact the geometry of the photo, for instance, flipping, turn, trimming, et cetera should be observable. A trimming ambush from the right-hand side and the base of the photo is an instance of this attack.

1.10.4 Security Attack

Particularly, if the watermarking computation is known, an aggressor can furthermore endeavor to perform modifications to render the watermark invalid or to assess and change the watermark. For this circumstance, we examine a strike on security. The watermarking computation is seen as secure if the embedded information can't be pulverized, recognized or fabricated.

1.10.5 Protocol Attack

The protocol/tradition ambushes do neither go for destroying the embedded information nor at devastating the recognizable proof of the embedded information (deactivation of the watermark). Instead of that, they abuse semantic deficiencies of the watermark's use. In this way, a solid watermark must not be invertible or to be recreated. A copy strike, for example, would go for recreating a watermark from one media into another without data of the puzzle key.

1.10.6 Cryptographic Assaults

Cryptographic assaults manage the breaking of the security. For instance, finding the mystery watermarking key utilizing comprehensive beast compel strategy is a cryptographic assault. Another case of this sort of assault is the prophet assault. In the oracle assault, a non-watermarked protest is made when an open watermark locator gadget is accessible. These assaults are like the assaults utilized as a part of cryptography.

1.10.7 Dynamic Attacks

Here, the programmer tries intentionally to expel the watermark or basically make it imperceptible. This is a major issue in copyright security, fingerprinting or duplicate control for instance.

1.10.8 Passive Attacks

For this situation, the assailant isn't endeavoring to expel the watermark yet just endeavoring to decide whether a given check is available or not. Cox et al (2002) recommend that assurance against latent assaults is absolutely critical in incognito interchanges where the basic information of the nearness of the watermark is frequently in excess of one needs to concede.

1.10.9 Collusion Attacks

In deceitful assaults, the objective of the programmer is the same with respect to the dynamic assaults yet the strategy is somewhat extraordinary. Keeping in mind the end goal to evacuate the watermark, the programmer utilizes a few duplicates of similar information, containing each extraordinary watermark, to build another duplicate with no watermark. This is an issue in fingerprinting applications (e.g. in the film business) yet isn't the broadly spread in light of the fact that the assailant must approach various duplicates of similar information and that the number required can be entirely vital.

1.10.10 Digital Image Degradation

These kinds of assaults harm vigorous watermarks by evacuating parts of the picture. The parts that are supplanted may convey watermark data. Cases of these tasks are incomplete editing, push expulsion and segment evacuation. Addition of Gaussian clamor additionally goes under this classification, in which the picture is corrupted by including commotion controlled by its mean and its difference.

1.10.11 Image Augmentation

These assaults are convolution activities that desynchronize the watermark data in a picture. These assaults incorporate histogram leveling, honing, smoothing, middle sifting and complexity improvement.

1.10.12 Image Firmness

So as to diminish the storage room and cut the cost of transmission capacity required for transmitting pictures, pictures are for the most part packed with JPEG and JPEG2000 pressure strategies. These lossy pressure strategies are more unsafe when contrasted with lossless pressure techniques. Lossless pressure strategies can recoup the watermark data with backwards activity. However lossy pressure strategies create irreversible changes to the pictures. Subsequently likelihood of recuperating watermarked data is constantly low.

1.10.13 Image Alterations

These sorts of assaults are likewise called synchronization assaults or geometrical assaults. The well-known programming Stir Mark utilizes little neighborhood geometrical contortions to refute watermark recognition. Geometrical assaults incorporate revolution, scaling and interpretation likewise called RST assaults. A few scientists center around RST strength while planning the powerful watermarking frameworks, since it is basic issue. Other than RST changes, picture changes additionally incorporate different changes, for example, viewpoint proportion change, shearing, response and projection.

1.11 Watermarking Applications

With the fast improvement of the data innovation and PC arrange innovation, the security of advanced sight and sound data has turned into a vital issue. The customary data security innovation in view of cryptography hypothesis generally has its restrictions. Keeping in mind the end goal to determine the inadequacies of customary data security innovation, an ever-increasing number of specialists has been beginning to consider the computerized watermarking innovation since it can successfully adjust for the lacks of the security and insurance utilization of conventional data security innovation. The watermark data can be copyright data, verification data or control data in order to decide the copyright proprietor of the computerized works, affirm the legitimacy and honesty of interactive media works, control duplicating as per the inserted control data, and accomplish the reason for copyright assurance. Advanced watermarking innovation has numerous applications in assurance, certification, distribution, anti-counterfeit of the computerized media and name of the client data. It has turned into an imperative report region in data covering up. As a rising interdisciplinary application innovation, computerized watermarking includes the thoughts and speculations of various subject scopes, for example, flag handling, cryptography, likelihood hypothesis and stochastic hypothesis, arrange innovation, calculation outline, and different strategies. It can implant copyright data into the mixed media information through specific calculations; the data might be creator's serial number, organization logo, pictures or content with uncommon noteworthiness, et cetera. Their capacity is filled in as copyright security, mystery correspondence, credibility recognize the information document, and so forth. The installed famous data is normally not noticeable or subtle, and it must be identified or removed through various extraordinary indicators or pursuers. A computerized watermark is firmly coordinated with and hided into the source information and it is turning into an indivisible piece of the last mentioned. This section depicts seven utilizations of watermarking: secretive correspondence, communicate scrutiny, proprietor recognizable proof, confirmation of possession, verification, value-based watermarks and duplicate control [51].

1.11.1 Secretive Correspondence

One of the most punctual utilizations of watermarking, or all the more absolutely, information covering up, is a strategy for sending covert communications. The application has been point by point by Simmons as the detainee's stress, in which we envision two detainees in independent cells endeavoring to pass messages forward and in turn around. Their stress is that they can't pass these messages especially, yet rather, must depend upon the remedial office overseer to go about as an operator. The chief will pass on harmless messages between them, regardless; will censure them in the event that he finds that, for instance, their messages identify with a strategy for escape. The strategy is to cover the escape-layout messages by concealing them in safe messages. There are two or three mechanically open endeavors expected for this application, including stego tools.

1.11.2 Communicate Scrutiny

In 1997, an embarrassment softened out up Japan with respect to TV promoting. No less than two locations had been regularly overfilling broadcast appointment. Promoters stood recompensing for a large number of advertisements that were never publicized. The training had remained to a great extent undetected for more than twenty years, to some degree on the grounds that there were no frameworks set up to screen the genuine communicate of promotions. There are a few sorts of associations and people intrigued by communicating checking. Publicists, obviously, need to guarantee that they get the transmission appointment bought from propagation firms. Artists and on-screen characters need to guarantee that they get exact eminence installments for communicates of their performances.

1.11.3 Proprietor Recognizable Proof

Despite the way that a copyright see isn't any more basic to ensure copyrights, it is still proposed. The kind of the copyright see is regularly "c date, proprietor". On books and photos, the copyright is put in plane sight. In films, it is joined to the total of the credits. In like manner, on prerecorded music, it is resolved to the bundling. One weight of such substance copyright sees is that they can as regularly as conceivable be expelled from the secured material. Bundling can be lost, motion pictures can have the credits cut off, and pictures can be spatially trimmed.

An electronic watermark can be utilized to give looking at copyright checking comfort since it changes into a fundamental piece of the substance, i.e. the copyright data is inserted in the music to supplement the substance see engraved on the bundling. The Digimarc affiliation has propelled a watermarking framework made arrangements for this application. Their watermark inserted and pioneers are packaged with Adobe's unmistakable picture managing the program, Photoshop. Right when the identifier finds a watermark, it contacts a focal database to perceive the watermark's proprietor (who must pay a cost to keep the data in the database).

1.11.4 Confirmation of Possession

Sight and sound proprietors may need to utilize watermarks not simply to perceive copyright possession, yet rather to really show proprietorship. To design the issue, we ought to rapidly show a few characters that are surprising in the watermarking forming. Acknowledge Alice makes a photograph and puts it on her site, with a copyright. Skip by then takes the photograph, utilizes a photograph managing the dare to supplant the copyright see with, and a brief time frame later claims to have the copyright himself. By what means can the request resolve? Normally, Alice could enlist the photograph with the copyright office by sending a duplicate to them. The copyright office records the photograph, together with data about the genuine proprietor. Right when the common contention among customer A and customer B comes up, customer A contacts the copyright office to obtain certification that she is the good 'old-fashioned proprietor. On the off chance that customer A did not enlist the photograph, by then she ought to on any event can display the film negative. In any case, with the quick certification of bleeding edge photography, there might never have been a negative. On a fundamental level, it is down to earth for Alice to utilize a watermark acquainted in the photograph with the show that she promises it.

1.11.5 Verification

As both still and camcorders continuously get a handle on cutting edge development, the limit with respect to intangible adjusting in like manner increases. The substance of mechanized photographs can without a doubt be balanced to such an extent that it is particularly difficult to recognize what has been changed. For this circumstance, there isn't even a one of a kind negative to take a gander at. There are different applications where the veracity of a photograph is squeezing, particularly in genuine cases and helpful imaging. Check is a particularly considered issue in cryptography. Friedman [13, 14] first talked about its application to make a "strong camera" by figuring a cryptographic stamp that is related to a photograph. In the event that even one piece of one pixel of the photograph is adjusted, it will never again compose the check, so any altering can be perceived. In any case, this check is metadata that must be transmitted adjacent the photo, potentially in a header field of a specific picture coordinate. In the event that the photograph is fittingly reproduced to another record layout that does not contain this header field, the stamp will be lost, and the photograph can never again be avowed. The best course of action is to bring the register straightforwardly with the photograph utilizing watermarking. This sheds the issue of guaranteeing that the check remains with the photograph. It likewise opens up the likelihood that we can take in extra about what changing has happened since any developments made to the photograph will in like way be made to the watermark. In this manner, there are a few frameworks that can show the hostile zone of changes that have been made to the photograph. There are also structures proposed to permit certain developments, for example, JPEG weight, and essentially prohibit more huge changes, for example, expelling a man from a terrible conduct scene.

1.11.6 Value-based Watermarks

Checking and proprietor perceiving affirmation applications put a practically identical watermark on all duplicates of a similar substance. Regardless, electronic stream of substance permits each duplicate scattered to be changed for every beneficiary. This point of confinement engages a novel watermark to be presented in every individual duplicate. Regard based watermarks, besides called fingerprints, permit a substance proprietor or substance shipper to see the wellspring of an unlawful duplicate. This is conceivably basic both as an obstruction to unlawful utilize and as a creative manual for examination. One conceivable usage of huge worth based watermarks is over the span of film dailies. Over the cross of affecting a development to picture, the postponed result of reliably photography is a great part of the time passed on to various individuals associated with its creation. These dailies are exceedingly private, yet periodically, a reliably is spilled to the press. Precisely when this happens, studios rapidly endeavor to perceive the wellspring of the break. Obviously, if each duplicate of the well-ordered contains a one of a kind regard based watermark that perceives the beneficiary, by then prominent affirmation of the wellspring of the break is impressively less asking. Another utilization of huge worth construct watermarks was passed with respect to by the DivX wander. DiVX displayed a changed understanding of DVD. One of the security tries executed in DivX equipment was a regard based watermark that could be utilized to see a player utilized for theft. On the off chance that unlawful duplicates of a DivX film turned up on the mystery advertise, DivX could utilize the watermark to track them to the source.

1.11.7 Reproduction Controller

Esteem based watermarks and besides watermarks for watching obvious proof, and check of proprietorship don't ruin unlawful replicating. Or then again, potentially, they fill in as convincing obstructions and investigative mechanical congregations. In any case, it is likewise pragmatic for recording and playback gadgets to respond to presented signals. Subsequently, a yearly gadget may deter recording of a flag on the off chance that it perceives a watermark that shows recording is blocked. Obviously, for such a framework to work, every single made recorder must unite watermark recognizing verification hardware. Such frameworks are beginning at now being made for DVD video and for motorized music disseminating. Abnormally, the uses of watermarks in a video to control equip retreats to no under 1989 and in sound to conceivably 1953.

1.12 Classification of Computerized/Digital Watermarking

We will discussed the division of watermarking with respect to different characteristics that are currently available for real time applications. The detail flow diagram of classification of watermarking is given in Fig. 1.8.

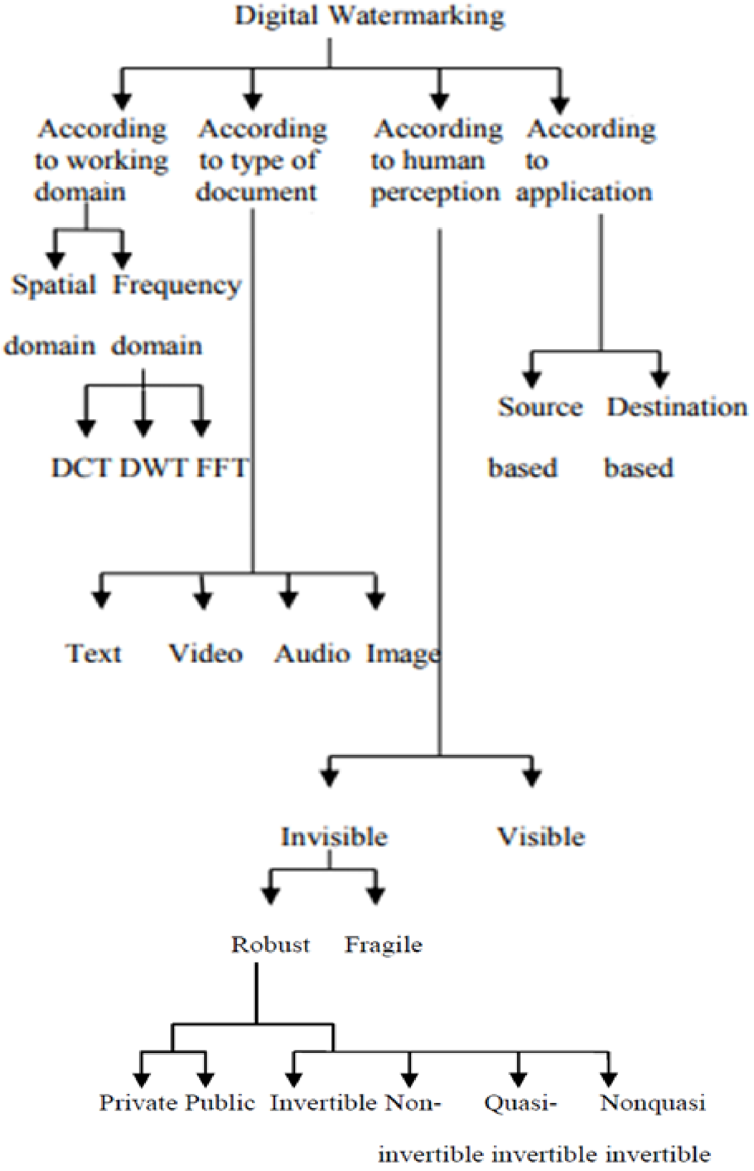


Fig. 1.8: Classification of Digital Watermarking Techniques.

1.13 Steganography

Steganography is a sort of hidden correspondence. The term gets from the old Greek steganos (covered up) and grafein (composing/writing). While cryptography is proposed to ensure/ protect the contents of messages, creating limitless content, steganography shrouds the message itself, without leaving a trace of its reality.

While steganography conceals a message inside another message, leaving the typical picture, video or music record practically unaltered and regardless rolling out improvements to the first documents indistinct, cryptography encodes the message, making an arrangement of immense images. While an arrangement of realistic pictures, video or music documents inside which the message is covered up does not excite doubt, a record of boundless characters does. While steganography requires consideration while reusing pictures or music documents, cryptography requires consideration while reusing keys. While there is no confinement in utilizing steganography, there are sure limitations utilizing certain types of cryptography.

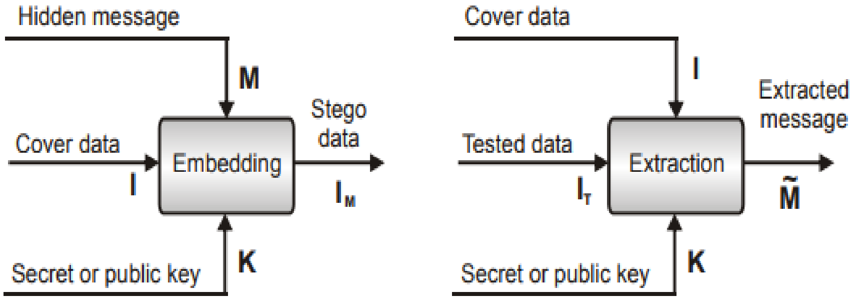


Fig. 1.9: General embedding and extracting scheme for information hiding.

1.13.1 Applications of Steganography

There are different applications in steganography; it changes among the client prerequisites, for example, copyright control, incognito/covert correspondence/communication, smart ID's applications, printers and so on etc. [41].

1.14 Assessment Factors for a Steganography Schemes

The principle targets for any steganography calculation are limit, imperceptibility and vigor. In spite of the fact that it is troublesome for a steganography calculation to have every one of the attributes in the meantime, on the grounds that there is by and large exchange off among these qualities [41].

1.14.1 Capacity

The measure of information to be installed in cover medium and can recovered later effectively without altogether changing the cover medium.

1.14.2 Imperceptibility

There ought to be no visual distinction amongst cover and stego question i.e. inserted message ought not be obvious to human eye.

1.14.3 Robustness

A stego framework is said to be robust, in the event that it can support any assault and on the off chance that it experiences change, for example, scaling, turn, filtering and lossy pressure and so forth. It ought to stay in place.

1.14.4 Security

An installing algorithm is said to be secure, if the inserted data couldn't be expelled after recognition by the eavesdropper. It depends on the information about the embedded algorithm and mystery key.

1.14.5 Embedding Rate

It is by and large indicated in supreme estimation, with the end goal that the span of the mystery message or in relative estimation called information inserting rate given generally in bits per non zero DCT pixel coefficient (BPNPC) and bits per pixel (BPP).

1.14.6 Indistinctness or Fidelity

Stego pictures are relied upon not to have any critical visual curios under a similar level of security and limit. Higher devotion of stego pictures suggests better indistinctness.

1.14.7 Sort of Pictures Supported

As images are accessible in countless, it is essential to comprehend which kind of pictures are appropriate for the steganographic technique of different sorts. Pictures essentially utilize lossy or lossless pressure instrument and the properties of pictures influence the steganographic strategies pertinent to those pictures.

1.14.8 Time Complexity

Steganographic algorithm differs as per the space of inserting. In less complex frameworks, the inserting work is less tedious yet may not be as secure as some other more entangled frameworks offering better execution. By and by, time multidimensional nature of a algorithm is critical for judging the relevance of scheme for inserting into huge pictures and furthermore their usage is low asset framework, for example, cell phones and so on.

1.15 Features of Robust Steganography

Regardless of the way that steganography's most clear target is to cover data, there are a couple of other related goals used to judge a method's steganographic quality. These join restrict (how much data can be hidden), intangibility (weakness for individuals to perceive a mutilation in the stego-question), indistinctness (disappointment for a PC to use experiences or other computational procedures to isolate among covers and stego-objects), vigor (message's ability to continue despite weight or other customary adjustments), change security/alter protection (message's ability to endure regardless of dynamic measures to wreck it), and flag to commotion proportion (how much data is encoded versus what amount disengaged data is encoded). The three essential parts, which work in opposition to each other, are limit, impalpability, and heartiness. Extending one of these influences the others to decrease; consequently, no steganographic procedure can be faultlessly indistinct and powerful and have the most extreme limit. When in doubt, a limit of the data isn't as basic as the other two, and however watermarking favors strength most firmly, general steganography considers subtlety the most fundamental.

An once-over of the properties of good steganography is shown in figure underneath.

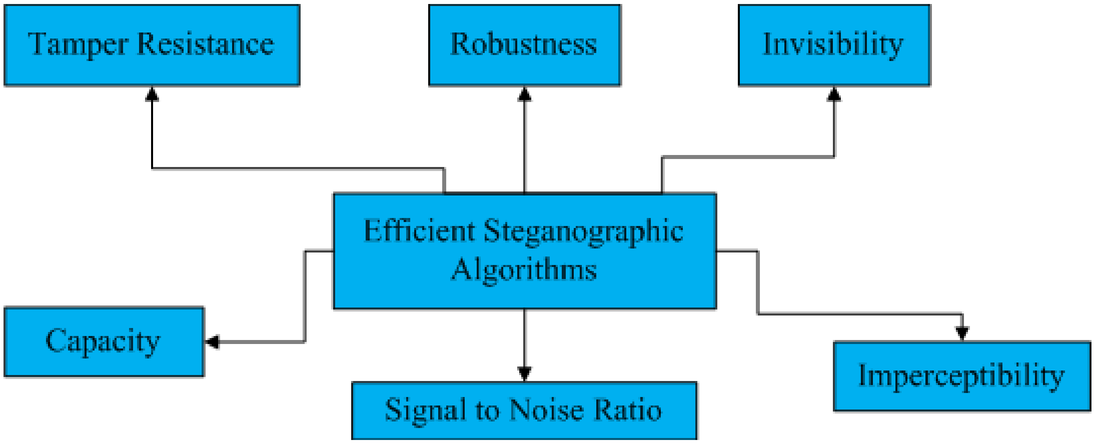


Fig. 1.10: Properties of Good Steganography

1.16 Basic Components of Steganography

1.16.1 Secret Message

The message to be embedded

1.16.2 Cover Image

An image in which secret message will be embedded.

1.16.3 Stego Image

Cover image that contain embedded message.

1.16.4 Key

Additional data that is needed for embedding and extracting process.

1.16.5 Embedding Steganography Algorithm

Steganography algorithm used toembed secret message with cover image.

1.16.6 Extracting Steganography Algorithm

Inverse function of embedding, in which it is used to extract the embedded message (secret message) from stego image.

1.16.7 Embedding Domain

The Embedding area alludes to the cover medium qualities that are abused in inserting message into it. It might be spatial space, when coordinate alteration of the constituent components of the cover is changed (e.g. pixels in a picture) or it can be the recurrence area or change space if scientific changes are carried on the medium before inserting.

1.17 Steganographic Models

Steganography can be divided into steganographic models, the principle ones being:

i. Injective steganography;

ii. Substitutive steganography;

iii. Generative steganography;

iv. Selective steganography;

v. Constructive steganography.

In injective steganography, the secret information is truly infused into the cover. Much of the time, this outcomes in an expansion in the memory control of the first cover and this might be a sign for a potential programmer to the presence of a mystery message inside the cover. Thusly, the bigger the measure of the cover is, the more data can be embedded, and the lesser the likelihood of location of the mystery message.

In substitutive steganography, some portion of the data of the cover is properly supplanted with the mystery message data, decreasing however much as could reasonably be expected detectable quality of the adjustment. This procedure brings about no expansion to the span of the cover and in that capacity is exceptionally viable. It is a standout amongst the most usually utilized methods. A run of the mill case is the substitution of the clamor in the correspondence channel with the mystery message.

In generative steganography, the cover is truly created to duplicate, in a reasonable way, the mystery message utilizing a fitting calculation. This strategy is extremely successful in that it is exceptionally hard to recognize the nearness of a mystery message inside the cover. On the off chance that the cover is a picture, it is still extremely hard to produce a sensible picture.

In particular steganography, just records that as of now have a property are chosen, from each one of those conceivable documents, and this property is utilized to shroud the mystery message. Thus, this system is extremely tedious and all things considered is seldom utilized despite the fact that it is exceptionally impervious to assaults.

In constructive steganography, the operation is fundamentally the same as that of the substitution steganography. When all is said in done, it is abused by utilizing the channel commotion, where a fitting model is first developed and afterward supplanted the clamor with the mystery message, continually following the model made. Indeed, even for this situation, it is greatly hard to capture the mystery message, yet its shortcoming is in making a legitimate clamor demonstrate.

1.18 Steganographic Protocols

The three basic types of steganographic protocols are:

1.18.1 Pure Steganography

We call a steganography framework unadulterated when it doesn't require earlier trade of some mystery data before sending information.

Definition 34 *A pure steganography is consisting of four parts* (C, S, D, E)*, where* C *is the set of possible covers,* S *is the set of secret massages with* $|C| \geq |S|$*,* $E : C \times S \rightarrow C$*,the embedding function and* $D : C \rightarrow S$*, is the extraction function with the property that* $D(E(c, s)) = S$ $\forall$ $c \in C$ *and* $s \in S$*.*

1.18.2 Private Steganography

We call a steganographic framework a private when it require an earlier trade of information like shared keys. In this case, sender chooses the cover and installs the mystery knead into the cover utilizing a mystery key. On the off chance that the mystery enter utilized as a part of inserting process, is known to the recipient he can switch the procedure and concentrate the mystery rub.

Definition 35 *A private key steganography is consisting of five parts* (C, S, K, E_K, D_K), *where* C *is the set of possible covers,* S *is the set of secret massages,* K *is the set of secret keys,* $E_K : C \times S \times K \rightarrow C$,*the embedding function and* $D : C \times K \rightarrow S$, *is the extraction function with the property that* $D_K(E_K(c, s)) = s \ \forall \ c \in C, \ s \in S$ *and* $k \in K$.

1.18.3 Asymmetric Steganography

This sort of steganography does not depend on shared key trade. Rather it depends on people in general key cryptography, guideline in which there are two keys one being open key which can be typically acquired from the general population database and the other a private key. For the most part for this situation people in general key is utilized as a part of the inserting procedure and the private key in the disentangling procedure.

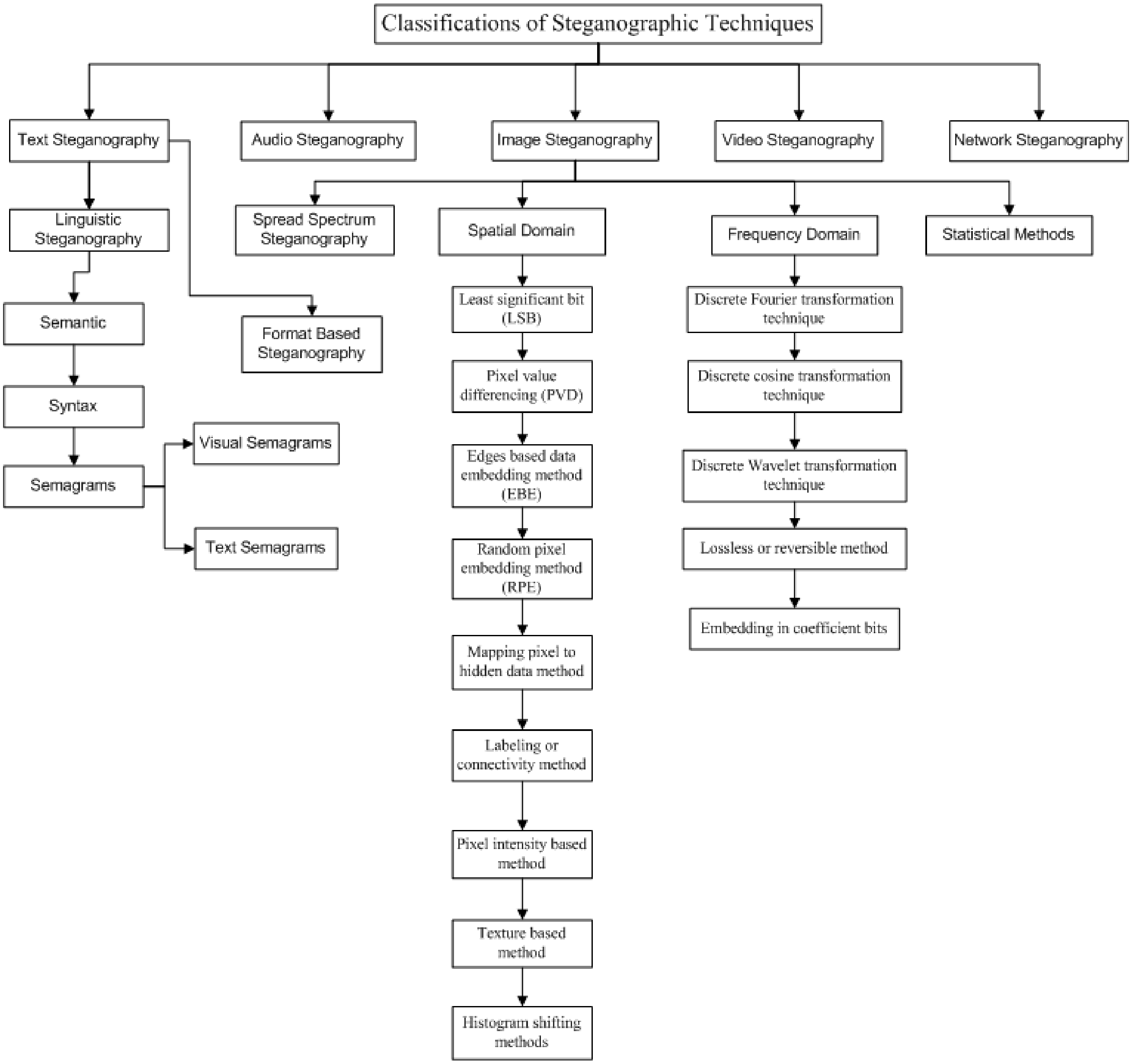

Classifications of Steganographic Techniques
Text Steganography
Audio Steganography
Image Steganography
Video Steganography
Network Steganography
Linguistic Steganography
Semantic
Syntax
Semagrams
Visual Semagrams
Text Semagrams
Format Based Steganography
Spread Spectrum Steganography
Spatial Domain
Frequency Domain
Statistical Methods
Least significant bit (LSB)
Pixel value differencing (PVD)
Edges based data embedding method (EBE)
Random pixel embedding method (RPE)
Mapping pixel to hidden data method
Labeling or connectivity method
Pixel intensity based method
Texture based method
Histogram shifting methods
Discrete Fourier transformation technique
Discrete cosine transformation technique
Discrete Wavelet transformation technique
Lossless or reversible method
Embedding in coefficient bits

Fig. 1.11: Classifications of Steganographic Algorithms.

1.19 Significance of Cryptography, Steganography and Watermarking

The space of digital security is growing practically consistently. It has turned into a multidisciplinary operation. The quantity of cyber incidents is on the rise. A few security firms have recognized numerous updates to misuse packs which have as of late begun utilizing steganography as a fundamental part of their operations as they utilize steganography as an approach to shroud abuses and malware payloads as PNG records. The Stegano abuses pack (otherwise called Astrum) is utilized to exchange diverse malevolent code by means of PNG flag advertisements. Once a web program hits such sites, JavaScript will extricate the code from the PNG document and divert the client to an alternate site that will taint the PC with malware. This recently refreshed endeavor unit was utilized by numerous malvertising efforts to circulate malware.

The most influenced nations were Japan, Canada, and France, however Japanese clients represented over 30% of the aggregate target. Steganography has been helpful in ensuring media copyrights (through computerized watermarks). Unfortunately, there may be a larger number of drawbacks than benefits. On the extraordinary end, fear based oppressor associations totally depend on steganography as their methods for correspondence. It is utilized to pass mystery messages without anybody yet the planned beneficiaries monitoring it. For instance, what has all the earmarks of being a family photograph may surreptitiously contain the plans for an arranged psychological oppressor assault. Shockingly, steganography is likewise giving chances to cybercriminals. There are numerous steganography instruments at present accessible running from open source to business items. These instruments give a lot of alternatives for cybercriminals.

To battle this issue, there is a requirement for people who know how to recognize and unscramble this concealed information. Just a couple of scholarly establishments offer these courses that spend significant time in these innovative regions. These advances ought not be limited to just a couple of passages or parts in existing courses. They ought to be offered as partitioned courses in cryptography, steganography, and watermarking. The objective of these three advancements is the same, to secure correspondences to just the expected sender and beneficiary. These courses ought to be offered in an organized arrangement that manufactures a far reaching comprehension of the idea, hypothesis, and utilization of cryptography, steganography, and watermarking. The capacity to split encoded records and find messages covered up through steganography will get ready understudies as they enter a world in which digital fighting has turned into the standard. This will fill in as a door to more particular, specific courses driving them to vocations in steganalysis, cryptography, cryptology, computerized media (sound, video, and pictures) legal sciences, and digital criminal investigation.

1.20 Some Differences in Information Security Systems

In this section, we mainly discuss the differences among the different information security systems.

1.20.1 Steganography Versus Watermarking

The fundamental objective of steganography is to conceal a message m in some sound or video (cover) information C, to acquire new information C', for all intents and purposes vague from C, by individuals, such that a busybody can't distinguish the nearness of m in C'. The primary objective of watermarking is to conceal a message m in some sound or video (cover) information C, to acquire new information C', basically unclear from C, by individuals, such that a busybody can't evacuate or supplant m in C'.

The data covered up by a watermarking framework is constantly related to the advanced question be ensured or to its proprietor while steganographic frameworks simply shroud any data "heartiness" criteria are likewise unique, since steganography is fundamentally worried about identification of the concealed message while watermarking concerns potential evacuation by a privateer steganographic correspondences are normally point-to-point (amongst sender and collector) while watermarking systems are generally one-to-many.

1.20.2 Cryptography Versus Watermarking

Cryptography is the most widely recognized technique for ensuring computerized content and is extraordinary compared to other created science. Be that as it may, encryption can't enable the dealer to screen how a true blue client handles the substance after unscrambling. Computerized watermarking can ensure content even after it is decoded.

1.20.3 Cryptography Versus Steganography

Cryptography is the examination of hiding information, while Steganography oversees framing covered messages so simply the sender and the beneficiary understand that the message even exists. In Steganography, simply the sender and the beneficiary know the nearness of the message, however in cryptography the nearness of the mixed message is clear to the world. Along these lines, Steganography empties the bothersome thought setting off to the covered message. Cryptographic procedures try to guarantee the substance of a message, while Steganography uses techniques that would stow away both the message and what's more the substance. By solidifying steganography and cryptography one can achieve better security. In essential words, cryptography is tied in with securing the substance of messages (their significance) and steganography is tied in with camouflaging the nearness of messages.

1.21 Combination of Different Security Techniqes

1.21.1 Joined Cryptography and Steganography

Both the systems can be consolidated to give one more level of insurance. The message can be first scrambled utilizing cryptography to encode the given information. This encoded message at that point can be implanted in a cover media utilizing steganography. This consolidated approach will fulfill the three objectives of information concealing: security, limit, robustness.

1.21.2 Joined Watermarking and Steganography

To secure the validness of the information, watermarking can be connected to it. This watermarked record can be implanted in the cover image by utilizing a stego-key and transmitted over the correspondence medium. At the collector end, the data can be first decoded utilizing the turnaround system and after that it can be approved for its genuineness utilizing the watermarking. This consolidated approach will fulfill each of the four objectives of information concealing: security, limit, vigor, and detectable quality.

1.22 Cybersecurity vs. Network Security vs. Information Security

We are in a period where organizations are more carefully progressed than any other time in recent memory, and as innovation enhances, associations' security stances must be improved too. Inability to do as such could bring about an expensive information rupture, as we've witnessed with numerous organizations. Risk actors are pursuing any kind of association, so with a specific end goal to ensure your business' information, cash, and notoriety, it is important that you put resources into a propelled security framework. Be that as it may, before you can begin building up a security program for your association, it's important that you comprehend the diverse sorts of security and how they all cooperate.

1.22.1 Information security

Data or information security (otherwise called InfoSec) guarantees that both physical and advanced information is shielded from unapproved get to, utilize, revelation, interruption, adjustment, review, recording or decimation. Data security contrasts from cybersecurity in that InfoSec intends to keep information in any frame secure, though cybersecurity ensures just computerized information. On the off chance that your business is beginning to build up a security program, data security is the place you should initially start, as it is the establishment for information security.

At the point when InfoSec specialists are creating arrangements and techniques for a successful data security program, they utilize the CIA (secrecy, integrity and availability) group of three as a guide.

The CIA group of three has turned into the true standard model for keeping your association secure. The three crucial standards help fabricate an incredible arrangement of security controls to safeguard and ensure your information.

1.22.2 Cybersecurity

Cybersecurity, a subset of data security, is the act of protecting your association's systems, PCs, and information from unapproved computerized access, assault or harm by executing different procedures, advancements and practices. With the incalculable refined danger actors focusing on a wide range of associations, it is important that your IT foundation is secured constantly to keep a full-scale assault on your system and hazard uncovering your organization' information and notoriety.

At the point when digital danger actors focus on your association, they investigate your business, as well as your workers too. They realize that workers outside of IT security aren't as mindful of digital dangers, so they execute cyber-attacks that adventure human vulnerabilities. Through the procedure of social designing, danger actors control individuals into giving the entrance to touchy data.

As a business pioneer, it is your duty to assemble a culture of security mindfulness and fill in the holes in your group's cybersecurity information and comprehension. It's basic that your workforce is educated of cybersecurity dangers, so it will be more improbable for a representative to succumb to an assault. Give your workers the vital preparing and innovation to fortify your association's human firewall and moderate the likelihood of a digital assault.

1.22.3 Network security

Network security, a subset of cybersecurity, plans to ensure any information that is being sent through gadgets in your system to guarantee that the data isn't changed or captured.

At the point when your system security is traded off, your first need ought to be to get the aggressors out as fast as could be expected under the circumstances. The more they remain in your system, the additional time they need to take your private information. As indicated by Ponemon Institute's 2013 Cost of Data Breach ponder, barring disastrous or uber information security breaks, the normal cost of an information rupture for each bargained record in the U.S. is $188. The normal total cost to an association in the U.S. is more than $5.4 million. The best technique for reducing the total cost is by getting the aggressors out of your system at the earliest opportunity.

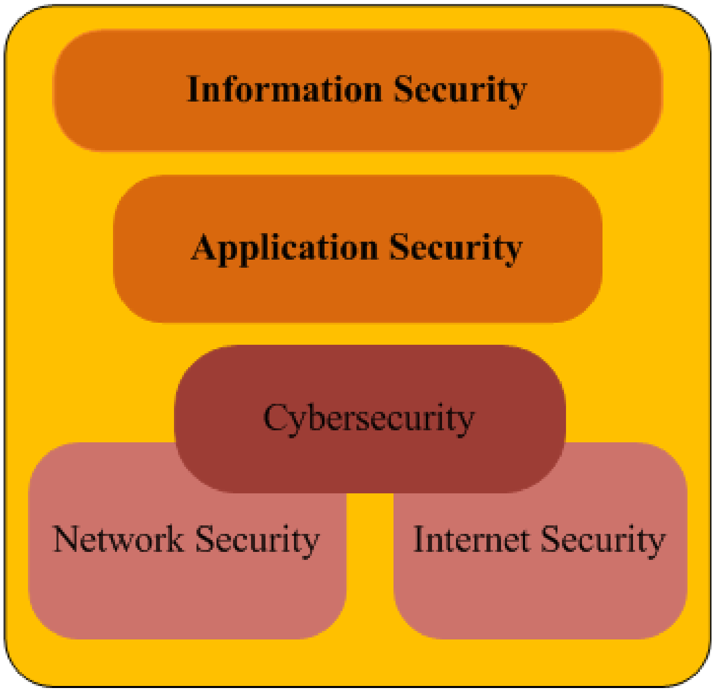


Fig. 1.12: Fundamental Security Classifications.

1.23 Conclusion

The aim focus of this chapter is to characterized the applicable supporting concepts of Boolean functions, nonlinear component of block ciphers, cryptography, watermarking and steganography. Specifically, we have given various since a long time ago settled definitions and hypotheses for different parts of the hypothesis. The important cryptographic properties which are utilized to investigate the quality of single and multiple output functions have likewise been characterized and talked about. The main point of this part of the theory is to give a study of existing data hiding techniques, their central focuses and preventions. A couple of methodologies for hiding data in content, picture, and sound are depicted, with proper acquaintances with the earth of every medium, and additionally the qualities and weaknesses of every procedure. Most data disguising structures misuse human perceptual deficiencies, yet have weaknesses they could call their own. In zones where cryptography and encryption are being denied, locals are looking to circumvent such methodologies and pass messages covertly. Business employments of modernized watermarks are at present being used to track the copyright and responsibility for media. This section moreover explains why data concealing is grabbing noteworthiness these days and the destinations that must be proficient by any data hiding system. The essentials of cryptography, watermarking and steganography are presented that will help us similarly in different parts of this thesis.

Chapter 2

A Color Image Watermarking Scheme Based on Affine Transformation and S_4 Permutation

With the improvement of computerized innovations and internet advances, digital contents could be effectively acquired by means of diverse transmission channels, for example, internet, remote systems. Because of focal points of digital technologies, impeccably recurrent and effort lessly adjusted, numerous issues have gotten more attention, for example, copyright security and content authentication. Particularly speaking, from perspectives of content suppliers, they need to present or offer their items through systems or different channels without dangers of any privateer. Subsequently, contents suppliers are excited to discover some novel measures to ensure their items. Also, in the wake of accepting a bit of computerized substance from authentic channel, clients expect that their gained item is simply from the genuine trader and is the first items without any alteration. Subsequently, there ought to be a validation component that backings the security of this kind activity and its way.

Luckily, one making a guarantee to technology to unravel these issues has been proposed from the earliest starting point of 1990s, that is computerized watermarking, which is appropriating operations by putting additional data over host ones and is utilized for content verification, tracking, copyright assurance, phony aversion and numerous other purposes [19]-[24]. Watermark could be characterized into two types according to its utility, namely robust watermark for copyright security and fragile watermark for integrity confirmation. The dominant part of watermarking strategies is to apply watermarks formed from pseudo-irregular number arrangements [21]-[27]. Chaotic maps such logistic map, skew map, cat map and Bernoulli maps have been generally used to produce water-mark sequences [28]-[29].

These watermarking systems can offer vagueness, security and strength as examined in [30], however, the fundamental obstruction lies in the implanting of the watermark in the original image. The binary map as a watermark is acquired by the development of pseudo-irregular arrangement of real numbers. As of late, chaotic structures have been utilized within watermarking mechanisms. In [31], a system for image watermark focused around chaotic sequences provided by diverse functions. The chaotic watermarking plan that embeds the chaotic sequence in the frequency domain was accounted in [32].

The significant purpose of advanced watermarking is to discover the equalization among the view points, for example, vigor to different assaults, sanctuary and imperceptibly. The invisibility of watermarking method is focused around the power of implanting watermark. Improved hiddenness is attained for a reduced amount of force watermark. Therefore, we must select the ideal force to embed watermark. There is slight compromise between the embedding strength and quality. Increase robustness obliges stronger embedding that builds the visual damage of the images. For a watermark to be powerful, it ought to vagueness, promptly extractable, unmistakable and vigor. The digital image watermarking schemes can be divided into two classes. These are visible watermarking and invisible watermarking strategies. Visible watermarking, the data are obvious in the picture or video. Commonly, the information is content or a logo which distinguishes the holder of the original documentation. Invisible watermarking, data are added as digital information to sound, picture or feature; however, it cannot be seen as being what is indicated. Further, the undetectable watermarks are arranged into watermarking procedures as delicate and vigorous. For the most part, a vigorous imprint is by and large utilized for copyright assurance and proprietorship distinguishing proof on the grounds that they are intended to withstand assaults, for example, regular picture preparing operations, which endeavor to uproot or demolish the imprint. These calculations guarantee that the picture transforming operations do not delete the implanted watermark indicator. Then, again a delicate or semidelicate watermark is predominantly connected to content confirmation and honesty check in light of the fact that they are extremely touchy to assaults, i.e., it can identify slight progressions to the watermarked picture with high likelihood. For a watermark to be effective, it should satisfy the following features [33]:

1. **Imperceptibility:** It ought to be perceptually undetectable so that information quality is not corrupted and aggressors are kept from discovering and erasing it.
2. **Promptly extractable:** The information manager or a free control power ought to effortlessly separate it.
3. **Unambiguous:** The watermark recovery ought to clearly recognize the information holder.
4. **Robustness:** It ought to endure a percentage of the regular image processing assaults.

A few routines have been proposed in writing. Two classes of digital watermarking algorithms are spatial space methods and recurrence area strategies. Least significant bit (LSB) will be the least complex method in the spatial space procedures which specifically changes the intensities of some selected pixels. The recurrence area method converts a picture into a set of recurrence space coefficients. In characteristic based watermarking plan, watermark will be created by applying a few operations on the pixel estimation of host picture rather than taking from outside source. Late explores on secure advanced watermarking strategies have uncovered the way that the substance of the pictures could be utilized to enhance the imperceptibility and the power of a watermarking plan [34]-[39]. This chapter suggests a novel methodology for watermarking which is a gigantic exploration territory that is dynamically developing. This scheme is basically based on applying the Galois field $GF(2^4)$, S_4 permutation and least significant bits. The investigation of these methods prompts systems for assaults and counter measures which are utilized to discover blames and limitations in applications, empowering the improvement of better ones. Computerized watermarking is distinctive relying upon its strategies and applications. The extent of this examination is invisible computerized image watermarking for color images. The exploratory consequences of the proposed strategies are dissected utilizing entropy, contrast, homogeneity, energy, means square error, root means square error, mean absolute error, peak signal-to-noise ratio, universal image quality index, mutual information, structural similarity, structural dissimilarity and structure content are used to measure the similarity between the cover image and watermarked image [43]-[44],[67]-[68], [45].

2.1 Some Algebraic Definitions

2.1.1 Definition

Let V and W be real vectors paces (their dimensions are different) and let T be a function with domain V and range in W (written as $T : V \to W$). We say T is a Iinear transformation if

For all $\alpha, \beta \in V, T(\alpha+\beta) = T(\alpha) + T(\beta)$, (T is additive),

For all $\alpha \in V, \gamma \in R,\ T(\gamma\alpha) = \gamma T(\alpha)$, ($T$ is homogeneous).

2.1.2 Definition

A mapping T from V^n to V^m is an affine transformation if T is linear mapping followed by a translation. In other words, there exist a matrix A and vector b such that $T(x) = Ax + b$; for all x.

The nonlinear component of AES is fundamentally based on affine transformation [43]

$$y = Ax \oplus b \mod m(x), \tag{2.1}$$

where $A \in GL_8(\mathbf{F}_2)$, $b \in M_{n\times 1}(\mathbf{F}_2)$ and $m(x)$ is an irreducible polynomial in $\mathbf{F}_{2^8}$. To be useful as nonlinear component of block cipher generator, matrix A should be non-singular. The new techniques can easily be derived with the basis from $\mathbf{F}_{2^8}$. As $\mathbf{F}_{2^8}$ is a finite field, therefore, the multiplicative inverse of every element exists and $0 \to 0$. This multiplicative inversion for the function $K(x)$ is as follows:

$$K(x) = \begin{cases} x^{-1} & x \neq 0, \\ 0 & x = 0. \end{cases} \tag{2.2}$$

The affine transformation is decomposed into two steps:

1. $T(x)$ be a linear mapping defined over $\mathbf{F}_{2^8}$ given as:

$$T(x) = Ax. \tag{2.3}$$

2. The AES which is famous block cipher, its nonlinear component involves an affine function $G(x)$ in over $\mathbf{F}_{2^8}$ as:

$$G = x \oplus d.$$

   The original nonlinear component of block cipher of AES is the composition of these functions given as [43]:

$$AES\ S_{box} = G \circ T \circ K, \tag{2.4}$$

   which clearly represents the affine transformation in AES nonlinear component of block cipher.

2.2 Algebra of New Watermarking Technique

The proposed watermark technique is based on small field of sixteen elements ,i.e., $GF(2^4)$ whose elements have of the form:

$$\begin{aligned} \mathbf{F}_{2^4} &= \frac{\mathbf{F}_2[x]}{(x^4+x+1)}, && (2.5)\\ &= \{b_0 + b_1\ x + b_2\ x^2 + b_3\ x^3; b_i \in \mathbf{F}_2\}, && (2.6) \end{aligned}$$

where $p(x) = x^4 + x + 1$, is a primitive irreducible polynomial of degree 4. The following table represents the elements of $\mathbf{F}_{2^4}$ along with its inverse elements and their corresponding binaries (Table 2.1).

Table 2.1: Representation of Galois field $GF(2^4)$ and its inverse elements.

Elements of $GF(2^4)$	Binary representations of $GF(2^4)$	Multiplicative inverses of each elements of $GF(2^4)$	Binary representations of inverse elements of $GF(2^4)$
1	0001	1	0001
2	0010	9	1001
3	0011	14	1110
4	0100	13	1101
5	0101	11	1011
6	0110	7	0111
7	0111	6	0110
8	1000	15	1111
9	1001	2	0010
10	1010	12	1100
11	1011	5	0101
12	1100	10	1010
13	1101	4	0100
14	1110	3	0011
15	1111	8	1000

The S- box is generated by determining the multiplicative inverse for a given number in $\mathbf{F}_{2^4} = \mathbf{F}_2[x]\ /(x^4 + x + 1) = \{b_0 + b_1\ x + b_2\ x^2 + b_3\ x^3; b_i \in \mathbf{F}_2\}$. The multiplicative inverse is then transformed using the following affine transformation:

$$AES\ S_{box} = G \circ T \circ K,$$

where $T(x)$ is the $\mathbf{F}_2$ linear mapping and matrix over $\mathbf{F}_2$ is used to describe the $\mathbf{F}_2$ linear matrix. The circulant matrix over $\mathbf{F}_2$ is of the form [44]

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Finally, we have apply the permutations to each elements of affine mini nonlinear component of block ciphers which can be represented by:

$$S_4 - AES\ S_{box}\ = P_\pi\ (G \circ L \circ K),$$

where $P_\pi^T = [e_{\pi(1)}, e_{\pi(2)}, ..., e_{\pi(m)}] \in S_4$ (symmetric group) and e_j denotes a row vector of length m with 1 in the j^{th} position and 0 in every other position (Tables 2.2, 2.3, 2.4). The proposed mini S_4 S-box is given as follows:

Table 2.2: Inversion in $\mathbf{F}_{2^4}$.

Input	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Output	0	1	9	14	13	11	7	6	15	2	12	5	10	4	3	8

Table 2.3: $\mathbf{F}_2-$ linear mapping in $\mathbf{F}_{2^4}$.

Input	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Output	0	13	11	6	13	7	10	1	14	3	5	8	9	4	2	15

Table 2.4: Proposed mini S-box.

$i \setminus j$	0	1	2	3
0	12	11	5	4
1	2	14	7	10
2	9	13	15	6
3	3	1	0	8

2.2.1 Least Significant Bits

The least significant bit (lsb or LSB) is the bit position in an adjusting entire number giving the units regard, that is, making sense of if the number is even or odd. It is like the least significant digit of a decimal number, which is the digit in the ones (right-most) position [29]-[30].

2.2.2 Most Significant Bits

The most significant bit (msb or MSB, similar to insightful called the high-arrange bit) is the bit position in a parallel number having the most noteworthy esteem. The msb is now and again proposed to as the furthest left bit as a result of the gathering in positional documentation of forming more significant digits further to one side.

2.2.3 Suggested Copyright Protection Scheme

In this section, we have implemented the proposed algebraic structure to watermarking. Our main purpose here is to hide an invisible watermarked with the help of proposed small nonlinear components of block ciphers and least significant digits (see Fig. 2.1). The algorithm of the proposed watermarking scheme is give as follow:

Algorithm 36 *1. Choose a digital image,*

2. Convert values of every pixels into a string of eight bits,

3. Distribute MSBs and LSBs for each pixel,

4. Apply nonlinear transformation on LSBs that signify the position of values in S_4 $S-box$,

5. S_4 S-box that has to be replacing with binaries of LSBs of an image,

6. Reiterate step 5 until the whole image is replaced,

7. Finally, reconstruct MSBs and transform LSBs.

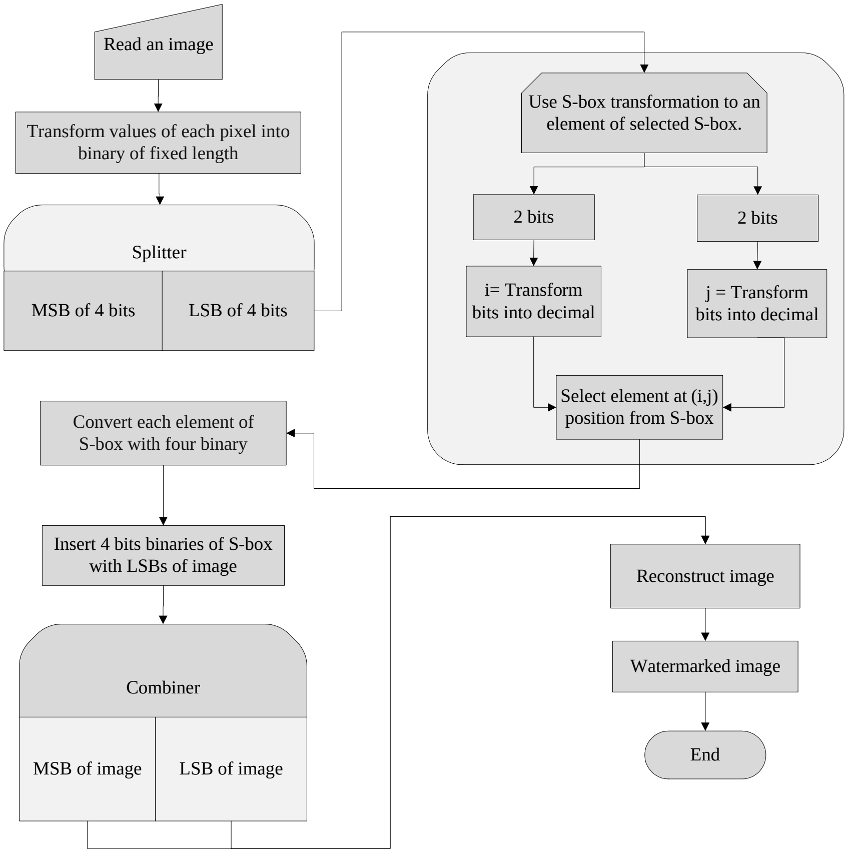
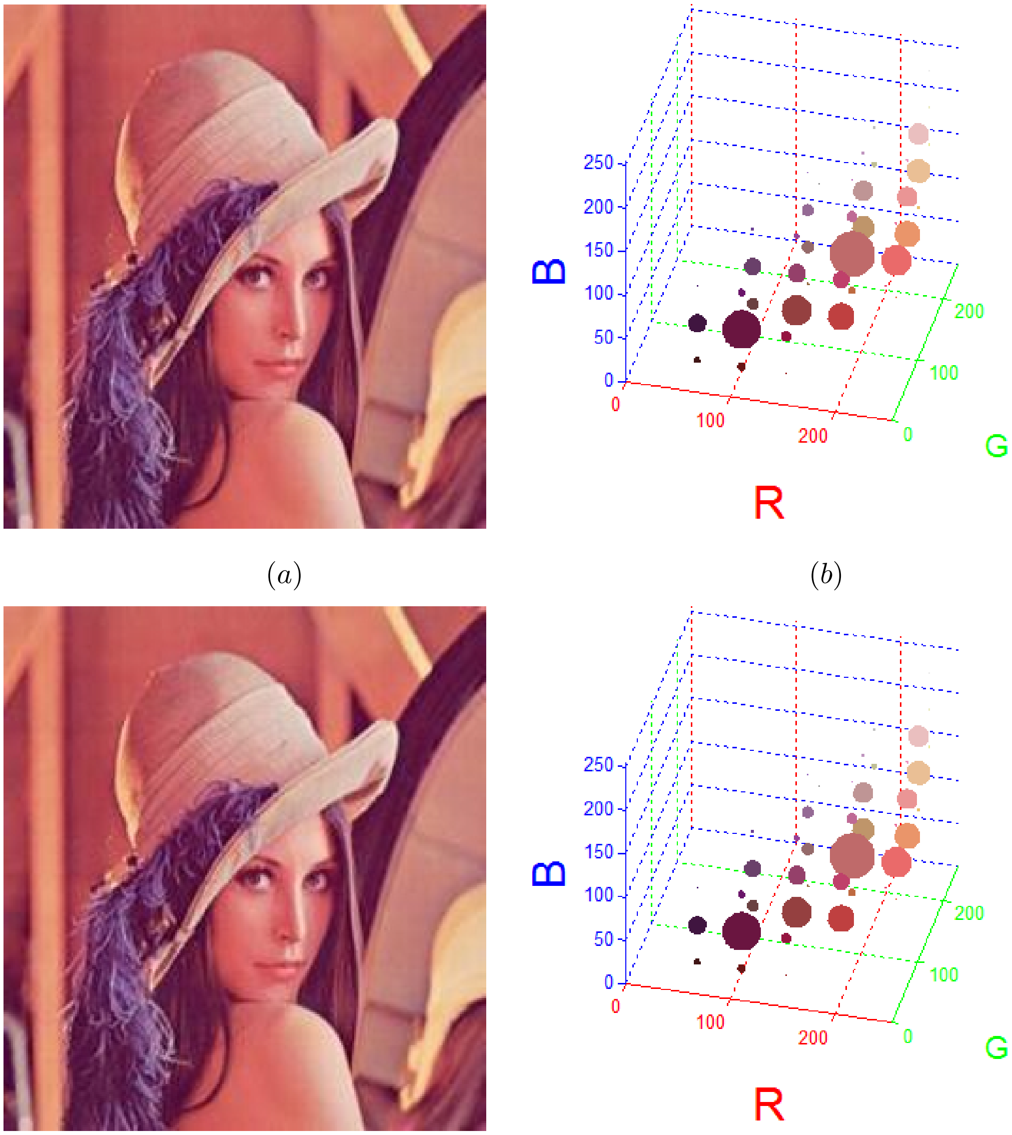

Read an image
Transform values of each pixel into binary of fixed length
Splitter
MSB of 4 bits
LSB of 4 bits
Use S-box transformation to an element of selected S-box.
2 bits
2 bits
i= Transform bits into decimal
j = Transform bits into decimal
Select element at (i,j) position from S-box
Convert each element of S-box with four binary
Insert 4 bits binaries of S-box with LSBs of image
Combiner
MSB of image
LSB of image
Reconstruct image
Watermarked image
End

Fig. 2.1: Suggested watermarking scheme based on $GF(2^4)$ and LSBs.



(a) (b)

(c) (d)

Fig. 2.2: $(a) - (c)$ Original and watermarked lena image of size $512 \times 512 \times 3$; $(b) - (d)$ $3D$ histogram visualization of original and watermarked lena image of $512 \times 512 \times 3$.

2.3 Statistical Analyses

In this section, we primarily talked about some tests which will show the competence of our proposed watermarking design [67]-[45].

2.3.1 Entropy

Entropy is a factual measure of randomness that might be utilized to portray the surface of the picture. Entropy is characterized as:

$$H = -\sum_{j=0}^{N} p(x_j) \log_b \ p(x_j). \tag{2.7}$$

Table 2.5 shows the results of entropy analysis of the original and watermarked images. These analyses show that there will be no leakage of information in original and watermarked images.

2.3.2 Contrast

The contrast dissection of the picture empowers the viewer to vividly distinguish the objects in surface of a picture. The watermarked picture same contrast levels as unique picture. We measure the contrast parameters of the watermarked picture and assess the adequacy of nonlinear components of block ciphers in watermarking applications. This investigation gives back a measure of the intensity contrast between a pixel and its neighbor over the entire picture and is mathematically represented as:

$$C = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} |i-j|^2 \ p(i,j), \tag{2.8}$$

where the number of gray-level co-occurrence matrices is represented by $p(i,j)$. Table 2.5, shows the results of contrast analysis when applied to watermarked images corresponding to various nonlinear components of block ciphers.

2.3.3 Homogeneity

The homogeneity investigation measures the closeness of the dispersion of components in the gray-level co-occurrence matrix (GLCM). The GLCM demonstrates the facts of combinations of pixel shine values or gray levels in plain structure. The recurrence of the examples of gray levels might be translated from the GLCM table. The mathematical expression of homogeneity is given as follow:

$$K = \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \frac{p(i,j)}{1+|i-j|}, \tag{2.9}$$

where the gray-level co-occurrence matrices in GLCM is represented by $p(i,j)$. Tables 2.5 and 2.6 show the results of homogeneity analysis for watermarked image.

2.3.4 Energy

In this analysis, we measure the energy of the watermarked images as processed by various nonlinear components of block ciphers. This measure gives the sum of squared elements in the gray-level co-occurrence matrix:

$$E = \sum_{i,j} p(i,j)^2, \tag{2.10}$$

where $p(i,j)$ is the number of gray-level co-occurrence matrices. The numerical values of entropy, contrast, energy and homogeneity show that our proposed scheme is robust. The tabulated measures clearly elucidate that our scheme is useful and quite compatible with applications.

Table 2.5: Comparison of entropy, contrast, energy and homogeneity analyses of proposed S-box for original and watermarked images.

Analysis	Original image	Watermarked image
Entropy	7.8362	7.8263
Contrast	0.2988	0.3199
Homogeneity	0.8960	0.8854
Energy	0.0955	0.0908

Table 2.6: The comparison of entropy, contrast, energy and homogeneity analyses of proposed S-box for color components of original and host images.

Proposed Properties	Color image components of original image			Color image components of watermarked image		
	Red	Green	Blue	Red	Green	Blue
Entropy	7.7637	7.8664	7.7226	7.7700	7.8472	7.7284
Contrast	0.3014	0.2914	0.2966	0.3140	0.2972	0.3075
Homogeneity	0.1129	0.0962	0.1090	0.1089	0.0949	0.1061
Energy	0.8941	0.9000	0.8975	0.8879	0.8967	0.8914

2.3.5 Mean Squared Error

To evaluate the reliability of the proposed algorithm, mean square error (MSE) between marked image and original image is measured. MSE is calculated using the following equation:

$$"MSE = \frac{1}{M \times N} \sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j) - g(i,j))^2, \tag{2.11}$$

where $M \times N$ is the size of the image. The parameters $f(i,j)$ and $g(i,j)$ refer to the pixels located at the ith row and the jth column of original image and marked image, respectively (see Fig. 2.1). The larger the MSE value, the better the watermarking quality (Fig. 2.1).

2.3.6 Root Mean Square Error

To evaluate the proposed watermarking system, this method is tested on the color Lena image of 512 × 512 pixels as shown in Fig. 2.2 (a) and 2.2 (b). The marked result is shown in Fig. 2.2 (c) and 2.2 (d). To find the accuracy of the results and the robustness of the watermarking, a root mean square of error is calculated. These criteria provide the error between source image and watermarked image. The RMSE value can be described by the following relation:

$$RMSE = \sqrt{\frac{1}{M \times N} \sum_{i=1}^{M}\sum_{j=1}^{N}(f(i,j) - g(i,j))^2}, \tag{2.12}$$

where the $f(i,j)$ is the pixel intensity of the original image and $g(i,j)$ is the pixel intensity of the watermarking image. The row and column numbers of these two images are defined by $M \times N$.

2.3.7 Mean Absolute Error

To evaluate the reliability of the proposed algorithm, mean absolute error (MAE) between watermark image and original image is measured. MAE is calculated using the following equation

$$MAE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} |f(i,j) - g(i,j)|, \tag{2.13}$$

where $M \times N$ is the size of the image. The parameters $f(i,j)$ and $g(i,j)$ refer to the pixels located at the ith row and the jth column of original image and marked image, respectively.

2.3.8 Peak Signal to Noise Ratio

The watermarked image quality is evaluated using peak signal-to-noise ratio (PSNR) which is described by the following expressions:

$$PSNR = 10 \log_2 \left(\frac{I_{\max}^2}{MSE} \right), \tag{2.14}$$

where $I_{\max}$ is the maximum of pixel value of the image. The PSNR should be a low value which corresponds to a great difference between the original image and marked image. The effectiveness of the proposed method, evaluated in terms of MSE and PSNR are tabulated in Table 2.7.

2.3.9 Universal Image Quality Index

Let X and Y be two digial images consists of $N \times N$ pixels each. The universal quality index is defined as:

$$Q = \frac{4\sigma_{XY}\overline{XY}}{(\sigma_X^2 + \sigma_Y^2)(\overline{X}^2 + \overline{Y}^2)}, \tag{2.15}$$

where $\overline{X}$ is a mean of X, $\overline{Y}$ is a mean of Y, σ_X^2 standard deviation of X, σ_Y^2 standard deviation of Y and σ_{XY} is a covariance of X and Y respectively.

2.3.10 Structure Similarity

The structural similarity (SSIM) index is a technique for measuring the similarity between two pictures. The SSIM metric is calculated on various sizes of an image. The measure between original and marked images of size $N \times N$ is:

$$SSIM(X,Y) = \frac{(2\overline{XY} + b_1)(2\sigma_{xy} + b_2)}{(\overline{X}^2 + \overline{Y}^2 + b_1)(\sigma_x^2 + \sigma_y^2 + b_2)}, \tag{2.16}$$

where $\overline{X}$ is the average of $X, \overline{Y}$ is the average of Y, σ_x is standard deviation of X, σ_y is standard deviation of y and σ_{xy} is covariance of X and Y, $b_1 = (k_1 L)^2, b_2 = (k_2 L)^2$ two variables which is to stabilize the weak denominator, L is the dynamics range of the pixels-values.

2.3.11 Mutual Information

Shared/mutual data is an essential idea from information theory, estimating the factual reliance between two irregular factors that one variable contains about the other. The mutual information is given as takes after:

$$I(x,y) = \sum_{x \in X} \sum_{y \in Y} p(x,y) \log \left(\frac{p(x,y)}{p(x)p(y)} \right), \tag{2.17}$$

where $p(x,y)$ is joint probability distribution function of original and marked images and $p(x), p(y)$ are the probability density functions in the individual images.

2.3.12 Structure Dissimilarity/Uniqueness

Structural dissimilarity (DSSIM) is a separation metric got from SSIM (however the triangle imbalance isn't really fulfilled)

$$DSSIM(X,Y) = \frac{1 - SSIM(X,Y)}{2}. \tag{2.18}$$

This analysis basically analyze the dissimilarities between original and watermarked images.

2.3.13 Structure Contents

The structure content (SC) of original and watermarked images is defined as follow:

$$SC = \frac{\sum_{n=1}^{n}\sum_{m=1}^{m}[f(n,m)]^2}{\sum_{n=1}^{n}\sum_{m=1}^{m}[g(n,m)]^2}, \tag{2.19}$$

where $f(n,m)$ is an original image and $g(n,m)$ is a watermarked image.

Table 2.7: The numerical results of MSE, PSNR, RMSE, MAE, UIQI, MI, SSIM, DSSIM and SC of proposed S-box for color watermarked image.

Proposed Analyses	Color image	Color image components of watermarked image		
		Red	Green	Blue
MSE	8.73510	11.4537	10.1302	11.8925
PSNR	38.7181	37.5414	38.0746	37.3781
RMSE	2.95550	3.38430	3.18280	3.44860
MAE	2.17580	2.50400	2.33680	2.57840
UIQI	0.85250	0.83820	0.85060	0.86110
MI	0.25313	0.25059	0.25646	0.23425
SSIM	0.95030	0.9447	0.9476	0.9447
DSSIM	0.02485	-	-	-
SC	1.00100	1.0018	1.0009	1.0004

The values of MSE, PSNR, RMSE, MAE, UIQI, MI and SSIM clearly elucidate the authentications of robustness in our proposed algorithm. As it is evident from the analysis of Table 2.7, lower MSE, RMSE, MAE values and higher PSNR values imply good embedding results where are higher values (in probability sense) of UIQI, SSIM and lower values of MI signify that there is no change after watermarked is placed in original image and no sharing between the original and host image. Also values of SC and DSSIM represent good embedding quality.

2.4 Conclusion

The principal idea of this part of the thesis is to develop a novel technique for digital copyright for advanced digital mediums. There has been a vast amount of literature available for the construction of new algorithms for digital watermarking and information hiding techniques. There are various new teachnues which are based on spatial and frequency domains were available in writing. Our suggested technique which is basically based on LSBs insertion with the help of new proposed nonlinear components of block cipher, which is quite easy and more effective design methodology as compared to other schemes. The suggested design of digital copright protection is robust due to its algebraic as well as statistical charactersitics.

Chapter 3

Construction of New nonlinear components of block ciphers Based on Permutation Matrices and its Implementation in Digital Patent Security

Multimedia technology is being widely used nowadays. Besides, computer networking has also become a lot common which resulted in problems regarding copyright protection of digital content (audio, video and image). Regarding copyright protection, digital watermarking/patent security has proved to be very potent and favorable. One of the main advantages is that one can hide information in images using this technique. This technique has advantages such as it provides protection, robustness and the quality of being unnoticeable but to that, there is a hindrance. In this chapter, we have designed a novel procedure for the construction of substitution boxes (nonlinear components of block ciphers) which is mainly based on permutations matrices of S_4 and Galois field $GF(2^4)$. We have analyze our nonlinear components of block ciphers with statistical analyses along with watermarking application. The scope of this research is invisible digital image watermarking for color and gray-scale images. We have testified our nonlinear components of block ciphers through some algebraic and statistical analyses. The algebraic analysis includes Nonlinearity, Strict avalanche criteria (SAC), Bit independent criteria (BIC), Linear approximation probability (LP) and Differential approximation probability (DP) whereas statistical tests are Mean squared error (MSE), Mean absolute error (MAE), Peak signal to noise ratio (PSNR), Universal image quality index (UIQI) and Structural similarity (SSIM).

3.1 Basic Definitions

In this section, we have presented some basic definitions of permutations and their algebraic properties which will be useful in next sections.

3.1.1 Permutations

Let X be a non empty set with n objects. A permutation of a set X is a mapping $\delta : X \rightarrow X$ that is a one-to-one and onto mapping that is bijective transformation.

3.1.2 Permutation Matrix

A permutation matrix is a square matrix obtained from the same size identity matrix by a permutation of rows. Such a matrix is always row equivalent to an identity. (see Table 3.1).

Table 3.1: Permutation matrices of S_4.

Elements	**Cycle decomposition notation**	**Matrix (right action)**	**Order of element**
1	()	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	1
2	(3,4)	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	2

Elements	**Cycle decomposition notation**	**Matrix (right action)**	**Order of element**
3	(2,3)	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	2
4	(2,3,4)	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	2
5	(2,4,3)	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	3
6	(2,4)	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	2
7	(1,2)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	2
8	(1,2)(3,4)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	2
9	(1,2,3)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	3

Elements	Cycle decomposition notation	Matrix (right action)	Order of element
10	(1,2,3,4)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	4
11	(1,2,4,3)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	4
12	(1,2,4)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	3
13	(1,3,2)	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$	3
14	(1,3,4,2)	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	4
15	(1,3)	$\begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	2
16	(1,3,4)	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	3

Elements	**Cycle decomposition notation**	**Matrix (right action)**	**Order of element**
17	(1,3)(2,4)	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	2
18	(1,3,2,4)	$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	4
19	(1,4,3,2)	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	4
20	(1,4,2)	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	3
21	(1,4,3)	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$	3
22	(1,4)	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	2

Elements	Cycle decomposition notation	Matrix (right action)	Order of element
23	(1,4,2,3)	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$	4
24	(1,4)(2,3)	$\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$	2

3.1.3 Permutation Group

A permutation group is a finite group G whose elements are permutations of a given set and whose group operation is composition of permutations in G. Permutation groups have orders dividing $n!$.

3.2 Mathematical Structure of Suggested Nonlinear Component

The nonlinear componet is generated by determining the multiplicative inverse for a given number in $GF(2^4)$. The nonlinear component transformation therefore consists of three functions, namely linear transformation L, invertible function I and affine transformation G :

$$S(x) = G \circ L \circ I. \tag{3.1}$$

The proposed symmetry group S_4 based nonlinear components of block ciphers are given as follows (see Table 3.2):

$$S - box = S_4 \times S, \tag{3.2}$$

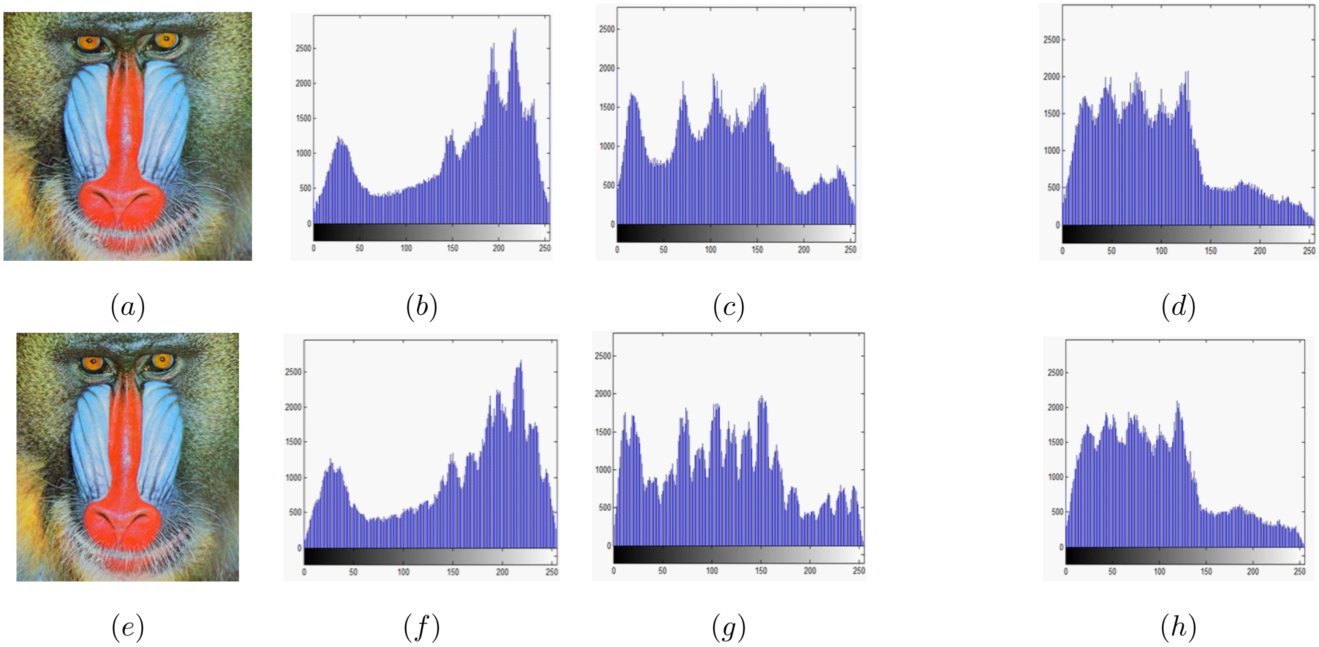
which is action of S_4 over small AES nonlinear components of block ciphers.

Table 3.2: Elements of proposed nonlinear components of block ciphers.

S_1	12	13	5	2	1	7	11	10	3	14	0	9	6	8	15	4
S_2	12	14	6	1	7	2	11	9	3	8	5	15	0	13	10	4
S_3	12	13	5	2	7	1	11	10	3	8	6	15	0	14	9	4
S_4	12	8	0	7	1	2	11	15	3	14	5	9	6	13	10	4
S_5	12	14	10	1	2	11	7	5	3	13	0	6	9	4	15	8
S_6	12	4	0	11	2	1	7	15	3	13	10	6	9	14	5	8
S_7	12	4	0	11	1	2	7	15	3	14	9	5	10	13	6	8
S_8	12	13	15	2	11	7	1	0	3	4	10	9	6	8	5	14

3.3 Suggested nonlinear components of block ciphers in Watermarking Application

In this section, we have implemented the proposed nonlinear components of block ciphers (see table 3.2) to watermarking. Our main purpose here is to hide an invisible watermarked with the help of proposed small nonlinear components of block ciphers and least significant digits. The algorithm of the proposed watermarking scheme is same as discussed in previous chapter but using different nonlinear component of block cipher.



(a) (b) (c) (d)

(e) (f) (g) (h)

Fig. 3.1 : (a) Original baboon image of size $512 \times 512 \times 3$, along with histograms of color components $(b, c$ a
(e) Watermarked image of size $512 \times 512 \times 3$, along with histograms of color components (f, g, h).

3.4 Statistical Analysis of Watermarking Scheme

To classify the large multimedia data, there exists no techniques other than the statistical analyses in order to justify the effectiveness of proposed schemes in information hiding. The most commonly used statistics which are discussed in literature are, GLCM texture features (gray level co-occurrence matrix) based measures, pixel difference-based measures, correlation-based measures and human visual system-based measures.

Texture is one of the critical attributes utilized as a part of distinguishing articles or areas of enthusiasm for a picture. Surface of an image contains critical data about the basic course of action of textures. The textural highlights in view of dim tone spatial conditions have a general relevance in picture arrangement. The three key example components utilized as a part of human elucidation of pictures are ghostly, textural and relevant highlights. Otherworldly highlights depict the normal aggregate varieties in different groups of the unmistakable as well as infrared part of an electromagnetic range. Textural highlights contain data about the spatial circulation of tonal varieties inside a band. The fourteen textural highlights proposed by Haralick et., [67] contain data about picture surface attributes, for example, homogeneity, dark tone straight conditions, difference, number and nature of limits introduce and the many-sided quality of the picture. Logical highlights contain data got from pieces of pictorial information encompassing the zone being broke down. Haralick et.,[68] all initially presented the utilization of co-event probabilities utilizing GLCM for separating different surface highlights. GLCM is additionally called as dark level reliance lattice. It is characterized as a two dimensional histogram of dark levels for a couple of pixels, which are isolated by a settled spatial relationship.

Different GLCM parameters are identified with particular first-order statistical concepts. For example, contrast would mean pixel pair repetition rate, variance would mean spatial frequency detection etc. Relationship of a textural significance to every one of these parameters is extremely basic. Generally, GLCM is dimensioned to the quantity of dark levels G and stores the co-occurrence probabilities g_{ij}. To decide the surface highlights, choose measurements are connected to each GLCM by repeating through the whole grid. The textural highlights depend on insights which outline the relative recurrence appropriation which depicts how regularly one dark tone will show up in a predefined spatial relationship to another dim tone on the picture. The accompanying documentations are utilized to clarify the different textural highlights:

3.4.1 Entropy

This measurement measures the turmoil or many-sided quality of a picture. The entropy is substantial when the picture isn't literarily uniform and numerous GLCM components have little esteems. Complex surfaces have a tendency to have high entropy. Entropy is firmly, yet contrarily connected to vitality. A totally arbitrary circulation would have high entropy since it speaks to tumult. Strong tone picture would have an entropy estimation of 0. This component can be valuable to let us know whether entropy is greater for substantial surfaces or for the smooth surfaces giving us data about which kind of surface can be considered factually more tumultuous.

3.4.2 Angular Second Moment

It gauges the textural consistency that is pixel combine reiterations. It identifies clutters in surfaces. Vitality achieves a most extreme esteem equivalent to one. High vitality esteems happen when the dim level appropriation has a steady or occasional frame. Vitality has a standardized range. The GLCM of less homogeneous picture will have huge number of little sections. Vitality is a measure of neighborhood homogeneity and in this manner it speaks to the inverse of the entropy. Fundamentally this element will reveal to us how uniform the surface is. The higher the vitality esteem, the greater the homogeneity of the surface. The scope of vitality is [0,1], where vitality is 1 for a steady picture.

3.4.3 Inertia

This measurement measures the spatial recurrence of a picture and is contrast snapshot of GLCM. This measure is additionally called differentiate. It is the distinction between the most noteworthy and the least estimations of an adjacent arrangement of pixels. It quantifies the measure of neighborhood varieties display in the picture. A low inactivity picture presents GLCM focus term around the important corner to corner and highlights low spatial frequencies. On the off chance that the neighboring pixels are fundamentally the same as in their dim level esteems then the differentiation in the picture is low. If there should be an occurrence of surface, the dim level varieties demonstrate the variety of surface itself. High differentiation esteems are normal for substantial surfaces and low for smooth, delicate surfaces.

3.4.4 Dissimilarity

Dissimilarity is a measure that characterizes the variety of dim level matches in a picture. It is the nearest to stand out from a distinction in the weight - differentiate not at all like divergence develops quadratically.

$$D = \sum_{i=0}^{N_g-1} \sum_{j=0}^{N_g-1} (i-j)P(i,j).$$

It is normal that these two measures act similarly for a similar surface since they compute a similar parameter with various weights. Contrast will dependably give somewhat higher esteems than dissimilarity. Dissimilarity ranges from [0,1] and acquire greatest when the dim level of the reference and neighbor pixel is at the extremes of the conceivable dim levels in the surface sample.

3.4.5 Inverse Difference Moment

Inverse difference moment is the neighborhood homogeneity. It is high when nearby dim level is uniform and opposite GLCM is high. Reverse distinction minute weight esteem is the opposite of the differentiation weight. It quantifies picture homogeneity as it expect bigger esteems for littler dim tone contrasts in combine components. It is more delicate to the nearness of close inclining components in the GLCM. It has most extreme esteem when all components in the picture are same. The scope of homogeneity is [0,1]. On the off chance that the picture has little variety then homogeneity is high and if there is no variety then homogeneity is equivalent to 1. Subsequently, high homogeneity alludes to surfaces that contain perfect dreary structures, while low homogeneity alludes to enormous variety in both, surface components and their spatial courses of action. An inhomogeneous surface alludes to a picture that has almost no redundancy of surface components and spatial comparability in it is truant.

3.4.6 Correlation

Correlation is a measure of dark tone straight conditions in the picture, specifically, the heading under scrutiny is the same as vector removal. High connection esteems suggest a direct connection between the dim levels of pixel sets. Hence, GLCM relationship is uncorrelated with GLCM vitality and entropy, i.e., to pixel sets reiterations. Relationship achieves it most extreme paying little mind to pixel combine event, as high connection can be estimated either in low or in high vitality circumstances.

3.4.7 Variance

This measurement is a measure of heterogeneity and is emphatically related to first request factual variable, for example, standard deviation. Variance/Fluctuation increments when the dim level esteems contrast from their mean.

$$Entropy = -\sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1} P_{i,j}\log P_{i,j,}, \tag{3.3}$$

$$Angular\ second\ moment = \sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1} P_{i,j}^2, \tag{3.4}$$

$$Inertia = \sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1}(i-j)^2 P_{i,j}, \tag{3.5}$$

$$Dissimilarity = \sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1}\sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1}(i-j)P(i,j), \tag{3.6}$$

$$Inverse\ difference\ moment = \sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1} \frac{P_{i,j}}{1+(i-j)^2}, \tag{3.7}$$

$$Correlation = \frac{\sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1} ijP_{i,j} - \mu_x\mu_y}{\sigma_x\sigma_y}, \tag{3.8}$$

$$Variance = \sum_{i=0}^{N_g-1}\sum_{j=0}^{N_g-1}(i-\mu)^2 P_{i,j}, \tag{3.9}$$

where $P_{i,j}$ is the (i,j) th entry of the co-occurrence matrix, N_g is the number of gray levels of an image, μ_x, μ_y, σ_x and σ_y are the means and standard deviations of the marginal probabilities $P_x(i)$ and $P_y(j)$ obtained by summing up the rows or the columns of matrix $P_{i,j}$ respectively. A complete second order texture analyses of proposed technique is presented in Tables 3.3 – 3.4. The rest of the textural features are secondary whose mathematical expressions are given below:

$$Sum\ Average\ (sa) = \sum_{i=2}^{2N_g} iP_{x+y}(i), \tag{3.10}$$

$$Sum\ Entropy\ (sa) = -\sum_{i=2}^{2N_g} P_{x+y}(i)\log P_{x+y}(i), \tag{3.11}$$

$$Sum\ variance = \sum_{i=2}^{2N_g}(i-sa)^2 P_{x+y}(i), \tag{3.12}$$

$$Difference\ variance = varaince\ of\ P_{x-y}, \tag{3.13}$$

$$Sum\ Entropy\ (sa) = -\sum_{i=0}^{N_g-1} P_{x-y}(i)\log P_{x-y}(i), \tag{3.14}$$

$$Maximum\ Correlation\ Coefficient\ (MCC) = (\text{Second largest eigen value of } Q)^{0.5}, \quad (3.15)$$

where

$$Q(i,j) = \sum_k \frac{P(i,k)P(j,k)}{P_x(i)P_y(k)}, \quad (3.16)$$

$$\begin{aligned} \text{Information Measures of Correlation 1} &= \frac{H_{XY} - H_{XY1}}{\max\{H_X, H_Y\}}, & (3.17) \\ \text{Information Measures of Correlation 2} &= \sqrt{(1 - \exp[-2.0(H_{XY2} - H_{XY})}, & (3.18) \end{aligned}$$

where

$$\begin{aligned} H_{XY} &= -\sum_i \sum_j P_{i,j} \log_2 P_{i,j}, \text{ where } H_X \text{ and } H_Y \text{ are entropies of } P_x \text{ and } P_y, & (3.19) \\ H_{XY1} &= -\sum_i \sum_j P_{i,j} \log_2 \{P_x(i)P_y(j)\}, & (3.20) \\ H_{XY2} &= -\sum_i \sum_j P_x(i)P_y(j) \log_2 \{P_x(i)P_y(j)\}. & (3.21) \end{aligned}$$

$$Cluster\ Shade\ = \sum_{i=0}^{N_g-1} \sum_{j=0}^{N_g-1} (i + j - \mu_x - \mu_y)^3 P_{i,j}. \quad (3.22)$$

$$Cluster\ Prominence\ = \sum_{i=0}^{N_g-1} \sum_{j=0}^{N_g-1} (i + j - \mu_x - \mu_y)^4 P_{i,j}, \quad (3.23)$$

$$\textit{Inverse difference normalized (IDN)} = \sum_{i=0}^{N_g-1} \sum_{j=0}^{N_g-1} \frac{P_{i,j}}{1 + |i - j| / N_g}, \quad (3.24)$$

$$\textit{Inverse difference moment normalized (IDM)} = \sum_{i=0}^{N_g-1} \sum_{j=0}^{N_g-1} \frac{P_{i,j}}{1 + (i - j)^2 / N_g^2}. \quad (3.25)$$

The pixel difference-based measures were derived based on pixel to pixel error such as mean square error(MSE), mean absolute error (MAE), peak signal to noise ratio(PSNR) and universal image quality index (UIQI), structural similarity index metric (SSIM) are included in human visual system-based measures. The pixel difference-based and human visual system-based measures defined as follows:

3.4.8 Mean Squared Error (MSE)

The mean squared error (MSE) is the least difficult, and the most generally utilized, full reference picture quality estimation. Closeness is controlled by registering the mistake between the watermarked picture and the first picture.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (C(i,j) - W(i,j))^2, \tag{3.26}$$

where $M \times N$ is the measure of the picture. The parameters $C(i,j)$ and $W(i,j)$ allude to the pixels situated at the i^{th} push and the j^{th} section of unique picture and watermarked picture because of the installing of the mystery data. The mean square error (MSE) speaks to the combined squared mistake between the watermarked and plain picture. A lower figure of MSE passes on bring down error/mutilation between the cover and watermarked picture.

3.4.9 Mean Absolute Error (MAE)

MAE is average of absolute difference between the reference signal and test image. It is given by the equation MAE is normal of total contrast between the reference and test images. It is given by the following mathematical expression:

$$MAE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left| C(i,j) - W(i,j)) \right|. \tag{3.27}$$

3.4.10 Peak Signal to Noise Ratio (PSNR)

Peak signal to noise ratio is to estimate the image distortions containing the watermark after the watermark is embedded into the original image, and reflects a digital watermarking algorithm‘s imperceptibility indicator. It can be used as a good empirical rule to measure watermark‘s imperceptibility. The formula of PSNR is:

$$PSNR = 10 \log_{10} \left[\frac{255^2}{MSE} \right]. \tag{3.28}$$

3.4.11 Universal Image Quality Index (UIQI)

The universal image quality index can also be defined as the product of three components:

$$Q = C_1 \times L_2 \times C_3, \tag{3.29}$$

where

$$C_1 = \frac{\sigma_{xy}}{\sigma_x \sigma_y}, \tag{3.30}$$

$$L_2 = \frac{2\overline{xy}}{\overline{x}^2 + \overline{y}^2}, \tag{3.31}$$

$$C_3 = \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2}, \tag{3.32}$$

where first term defines the correlation, second term measures the luminance and third term represents the contrasts of the images. Therefore through UIQI, we are measuring three characteristic at a time.

3.4.12 Structural Similarity Index Metric (SSIM)

The general form of the SSIM index between signal X and Y is defined as:

$$SSIM(X,Y) = [l(X,Y)]^{\alpha}.[c(X,Y)]^{\beta}.[s(X,Y)]^{\gamma}, \tag{3.33}$$

where α, β and γ are parameters to define the relative importance of the three components. Specifically, we set $\alpha = \beta = \gamma = 1$, and the resulting SSIM index is given by

$$SSIM(X,Y) = \frac{(2\mu_X \mu_Y + c_1)(2\sigma_{XY} + c_2)}{(\mu_X^2 + \mu_Y^2 + c_1)(\sigma_X^2 + \sigma_Y^2 + c_2)}. \tag{3.34}$$

Table 3.3: The GLCM analyses of original and watermarked color image.

GLCM features	Original image			Watermarked image		
	Color components			Color components		
	Red	Green	Blue	Red	Green	Blue
Entropy	4.83290	4.7339	4.8837	4.8906	4.7656	4.9143
Angular Second Moment	0.00067	0.00081	0.0006	0.0006	0.0008	0.0006
Inertia	45.7318	50.3293	50.658	50.517	51.448	52.160
Dissimilarity	3.80220	3.99200	4.0573	4.0308	4.0674	4.1270
Inverse Difference Moment	0.19955	0.19637	0.1912	0.1915	0.1911	0.1878
Correlation	0.54859	0.48133	0.5565	0.5385	0.4773	0.5531
Autocorrelation	923.109	784.852	687.06	922.82	784.41	687.16
Variance	946.616	810.573	712.56	948.72	810.69	713.41
Sum Average	46.6716	43.8016	38.612	46.667	43.804	38.647
Sum Entropy	3.07445	2.94570	3.0895	3.0837	2.9489	3.0953
Sum Variance	3321.87	2815.68	2455.3	3324.3	2814.6	2456.3
Difference Variance	45.7316	50.3293	50.658	50.517	51.448	52.160
Difference Entropy	1.86210	1.89370	1.9041	1.9000	1.9057	1.9049
Information Measures of Corr. 1	-0.11886	-0.08192	-0.1121	-0.1095	-0.0785	-0.1084
Information Measures of Corr. 2	0.58027	0.51804	0.57313	0.56976	0.51195	0.56895
Cluster Shade	4113.93	-477.06	10071.4	3816.51	-477.73	9891.97
Cluster Prominence	795070	303246	1192263	812460	303883	1194388
Inverse Difference Norm. (IDN)	0.61612	0.61398	0.61305	0.61341	0.6130	0.61222
Inverse Difference Mom. (IDM)	0.65640	0.65542	0.65531	0.65538	0.65518	0.65501

Table 3.4: The pixel difference based features of proposed watermark scheme for color watermarked image.

Pixel difference and correlation based features	Color watermarked image	Color components of watermarked image		
		Red	Green	Blue
MSE	68.8406	74.0624	71.4861	76.8383
PSNR	29.7524	29.4348	29.5886	29.2750
MAE	6.25782	6.54219	6.41020	6.66985
UIQI	0.88755	0.88297	0.88709	0.89380
SSIM	0.90180	0.89774	0.90134	0.90295

The feature is defined as a function of one or more measurements, each of which specifies some quantifiable property of an object, and is so computed that it quantifies some significant characteristics of the object. All features can be coarsely classified into low-level features and high-level features. Low-level features can be extracted direct from the original images, whereas high-level feature extraction must be based on low-level features. Texture is a surface property. It is characterized by the spatial distribution of gray levels in a neighborhood. Since texture shows its characteristics both by pixel coordinates and pixel values, there are many approaches used for texture classification. The image texture depends on the scale or resolution at which it is displayed. A texture with specific characteristics in a sufficiently small scale could become a uniform texture if it is displayed at a larger scale. The GLCM seems to be a well-known statistical technique for feature extraction. The GLCM is a tabulation of how often different combinations of pixel gray levels could occur in an image. The goal is to assign an unknown sample image to one of a set of known texture classes. Textural features can be scalar numbers, discrete histograms or empirical distributions. They characterize the textural properties of the images, such as spatial structure, contrast, roughness, orientation, etc. and have certain correlation with the desired output. Here we have calculated mainly second order texture features of plain and watermarked image in order to authenticate the presence of watermark in an original color image. There is minute difference in all GLCM texture features which justify the existence of watermark statistically which cannot be seen through naked eye (see Table

3.3). Moreover the values of pixel difference based features namely, MSE, PSNR and MAE and, correlation based measures UIQI and SSIM clearly

3.5 Cryptographic Properties of Secure Nonlinear Component of Block Ciphers

The projected nonlinear component is also verified by algebraic methods to determine the strength and resistance against cryptanalysis. The primary objective of the nonlinear component is to induce nonlinearity in plaintext. In order to determine the extent of nonlinearity after transformation, a nonlinear test is conducted. The performance of the nonlinear component is further evaluated by observing the behavior of output when input is changed according to different criteria namely strict a. The effects of bit changes in the system at different stages are also analyzed. Similarly, linear and differential approximation probability tests are performed to evaluate resistance against linear and differential cryptanalysis, respectively. The detail description for each cryptographic properties namely nonlinearity, Bit independent criterion (BIC), Strict avalanche criterion (SAC), Linear approximation probability (LP) and differential approximation probability already given in chapter 1. Here we have only apply these cryptographic properties on our proposed nonlinear components of block cipher.

Table 3.6: Nonlinearity, SAC and LP analyses for proposed nonlinear components of block ciphers.

nonlinear components of block ciphers	Nonlinearity			SAC			LP
	Max.	Min.	Avg.				
S_1	4	2	3.5	0.6250	0.3750	0.5000	0.3750
S_2	4	2	3.5	0.6250	0.3750	0.5000	0.3750
S_3	4	2	3.5	0.6250	0.3750	0.5000	0.3750
S_4	4	2	3.5	0.5000	0.3750	0.4921	0.3750
S_5	4	2	3.5	0.6250	0.5000	0.5078	0.3750
S_6	4	2	3.5	0.5000	0.3750	0.4843	0.3750
S_7	4	2	3.5	0.6250	0.3750	0.5000	0.3750
S_8	4	2	3.5	0.6250	0.3750	0.5000	0.3750
S_9[142]	4	2	3.5	0.6250	0.3750	0.4922	0.3750
S_{10}[143]	4	2	3.5	0.7500	0.2500	0.5000	0.2500
S_{11}[144]	4	4	4	0.5000	0.5000	0.5000	0.2500
S_{12}[145]	4	2	3.5	0.6250	0.3750	0.4531	0.3750
S_{13}[146]	4	4	4	0.6250	0.2500	0.4375	0.3750
S_{14}[147]	4	2	3.5	0.7500	0.2500	0.4688	0.3750

Table 3.7: BIC-Nonlinearity, BIC-SAC and DP analyses for proposed nonlinear components of block

nonlinear components of block ciphers	BIC-Nonlinearity			BIC-SAC			
	Max.	Min.	Avg.	Max.	Min.	Avg.	Max.
S_1	4	2	2.5	0.5417	0.4166	0.5052	0.5000
S_2	4	2	2.5	0.5417	0.4166	0.4844	0.5000
S_3	4	2	2.5	0.5000	0.3750	0.4739	0.5000
S_4	4	2	2.5	0.6250	0.3750	0.4739	0.5000
S_5	4	2	2.5	0.6250	0.3750	0.4844	0.5000
S_6	4	2	2.5	0.5417	0.4166	0.4844	0.5000
S_7	4	2	2.5	0.6667	0.3750	0.4687	0.5000
S_8	4	2	2.5	0.5833	0.3333	0.4479	0.5000
S_9[142]	4	0	2.5	0.6250	0.4167	0.5052	1
S_{10}[143]	4	0	2.5	0.5833	0.4167	0.4688	1
S_{11}[144]	4	0	2.75	0.5833	0.4167	0.4688	1
S_{12}[145]	4	0	2.5	0.5833	0.4167	0.5000	1
S_{13}[146]	4	0	2.5	0.5417	0.4167	0.5000	1
S_{14}[147]	4	0	3.0	0.5417	0.4167	0.4739	1

We are taking only eight nonlinear components of block ciphers from twenty four proposed nonlinear components of block ciphers and compare these with some well known existing nonlinear components of block ciphers. By investigating the tabulated values in tables 3.6 and 3.7, it is quite evident from that our proposed methodology clearly fulfill the cryptographic need of nonlinear component. The nonlinearity of proposed nonlinear components of block ciphers is comparable to existing nonlinear components. Additionally, the SAC, BIC-SAC are near to 0.5 which shows the balancedness of Boolean functions involved in the present construction. The linear approximation and differential approximation probabilities of proposed nonlinear components of block ciphers values provides strong resistance against differential and linear attacks.

3.6 Conclusion

In this part, we have examined digital picture watermarking which is one of the unmistakable techniques to satisfy the hole between copyright issues and advanced dispersion of information. It is principally in light of data concealing systems and empowers helpful security instruments. It goes about as a decent medium for copyright issues as it implants an image or a logo as a watermark, which can't be adjusted physically. One imperative segment that must be remembered while utilizing watermarking plan is to turn away any modifications to the creativity of the picture in the wake of installing the information. At the point when the picture with the mystery information is transmitted over the web, unapproved gatherings might need to hack the information covered up finished the picture or change it. On the off chance that the inventiveness of the picture has been changed, at that point it will be simpler to hack the data by unapproved people. Keeping in mind the end goal to enhance the security, the advanced watermarks are dominatingly embedded as the changed computerized motion into the source information utilizing key based inserting calculation and pseudo clamor design. The best known watermarking strategy that works in the spatial area is the Least Significant Bit (LSB), which replaces the minimum noteworthy bits of pixels chose to shroud the data. Our plan fundamentally here triple, right off the bat build another nonlinear components of block ciphers, also present new factual and arithmetical examinations which depend on gray level co-occurrence matrix (GLCM), and thirdly utilized these development to outline new watermarking plan.

Chapter 4

Small Nonlinear Components in Image Encryption and Information Hiding

The upswing of internet is one of the most important factors of information technology and communication which ultimately needs the security of information that passes through any insecure line of communications. There are several information security techniques available for securing information. The cryptography is one of technique used to safeguard the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Inappropriately it is occasionally not enough to preserve the insides of a communication secret, it may also be essential to preserve the presence of the communication secret. The procedure used to device this, is called steganography. Steganography is the skill of hiding messages in a medium called cover object in such a way that presence of message is untraceable. Imperceptibility is clearly is the most important requirement in steganographic schemes. The cover object could be a digital image, an audio file, or a video file. The secret message called payload could be a plain text, an image, a video file or an audio. Steganographic methods are classified into spatial domain embedding and frequency domain embedding. In frequency domain, images are transformed into frequency components by using DCT, FFT or DWT and then messages are embedded either in bit level or in block level. In spatial domain LSB replacing is the most widely used data hiding method. Because of low computational complexity and high embedding capacity this chapter mainly deals with LSB steganography method. The proposed work in chapter displays a novel procedure for image steganography in view of the S-Box mapping. The pre-processing of emit image is conveyed by rearranging of hidden image segments by utilizing three 4×4 nonlinear components of block ciphers. The preprocessing give abnormal state of security as extraction is unrealistic without the learning of mapping guidelines of nonlinear component. The proposed plan is additionally equipped for holding self-extraction system to recoup the hidden image.

4.1 Logarithmic Permutation of $GF(2^4)$

In this section, we report a new class of nonlinear components of block ciphers developed in $GF(2^4)$. These small nonlinear components of block ciphers can be used to construct a compact cipher for the devices with limited computing and memory resources, such as those in wireless sensor or mobile communications. We found these permutations by means of the multiplication table of $GF(2^4)$ (see table 4.2). We notice that the inverses defined in Table 4.2 is equivalent to $\alpha \longmapsto \alpha^{14}$ in $GF(2^4)$, which belongs to the class of permutations generated by the power functions $\alpha \longmapsto \alpha^k$ $(k = 1, 2, 4, 7, 8, 11, 13, 14)$. In the present work, we investigate an alternative class of permutations defined by the $\alpha \longmapsto \log_m \ \alpha$ $(m = 2, 3, 4, 5, 9, 11, 13, 14)$

in $GF(2^4)$.

Table 4.2: Logarithmic permutations.

x	Permutations							
	P_2	P_3	P_4	P_5	P_9	P_{11}	P_{13}	P_{14}
0	0	0	0	0	0	0	0	0
1	15	15	15	15	15	15	15	15
2	1	4	8	2	14	13	7	11
3	4	1	2	8	11	7	13	14
4	2	8	1	4	13	11	14	7
5	8	2	4	1	7	14	11	13
6	5	5	10	10	10	5	5	10
7	10	10	5	5	5	10	10	5
8	3	12	9	6	12	9	6	3
9	14	11	7	13	1	2	8	4
10	9	6	12	3	6	12	3	9
11	7	13	11	14	8	1	4	2
12	6	9	3	12	9	3	12	6
13	13	7	14	11	2	4	1	8
14	11	14	13	7	4	8	2	1
15	12	3	6	9	3	6	9	12

4.2 Mathematical Structure for Proposed nonlinear components of block ciphers

The nolinear component of block cipher is by using the the multiplicative inverse for a given number in $GF(2^4) = \mathbb{Z}_2[x]/\{x^4 + x + 1\} = \{b_0 + b_1x + b_2x^2 + b_3x^3/b_i \in \mathbb{Z}_2\}$.The multiplicative inverse is then transformed using the following affine transformation:

$$S - box = G \circ L \circ J, \tag{4.1}$$

where $L(x)$ is the 4×4 linear map over $GF(2)$ and $G(x) = x \oplus d$ and J is inverse function as defined in chapter 3. The linear map over $GF(2)$ is given as follows:

$$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}. \tag{4.2}$$

The proposed affine logarithmic permutation based nonlinear components of block ciphers are given as follows:

Table 4.3: Proposed affine logarithmic permutation based nonlinear components of block ciphers.

nonlinear components of block ciphers	Elements of nonlinear components of block c														
S_1	12	3	11	1	2	7	6	9	5	4	0	8	15	13	14
S_2	12	3	1	11	7	2	6	9	10	14	15	13	0	8	4
S_3	12	3	7	2	11	1	9	6	0	8	10	14	5	4	13
S_4	12	3	2	7	1	11	9	6	15	13	5	4	10	14	8
S_5	12	3	4	14	13	8	3	6	10	11	15	7	0	2	1
S_6	12	3	13	8	14	4	6	9	0	2	10	11	5	1	7
S_7	12	3	8	13	4	14	6	9	15	7	5	1	10	11	2
S_8	12	3	14	4	8	13	9	6	3	1	0	2	15	7	11

4.3 Proposed Steganographic Technique

Proposed steganography scheme is based on scrambling and transposition transformation which clearly satisfy the idea of Shannon principal of diffusion and confusion using nonlinear component mapping. A complete flow chart of suggested algorithm is give as follows:

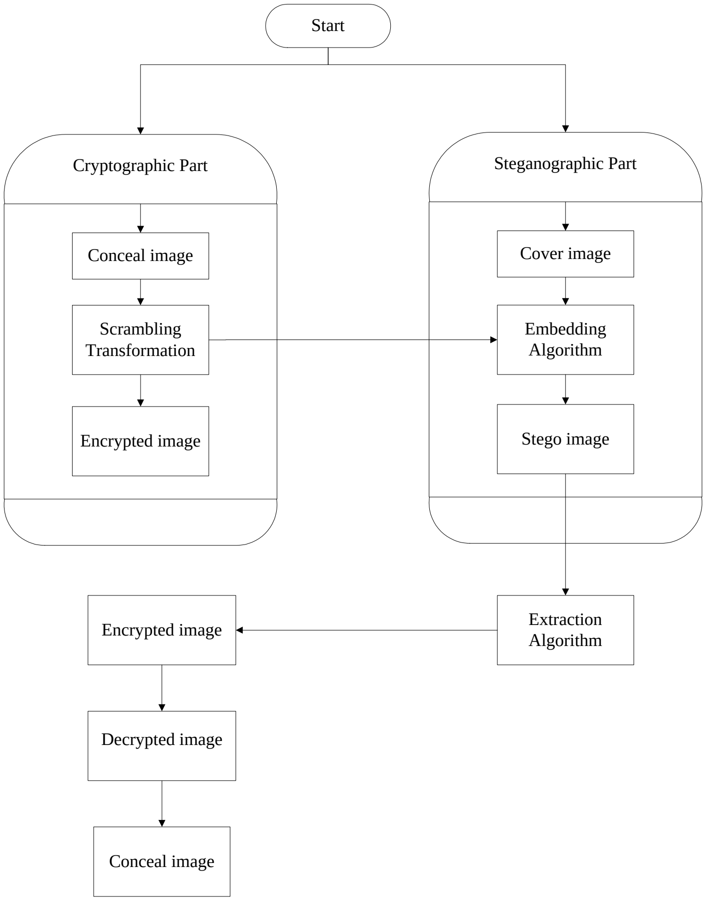


Fig. 4.1: Flow chart for suggested steganographic process.

4.3.1 Scrambling Transformation

Establishment of chunks from Conceal image

The first part of this hiding technique includes the conversion of secret image into blocks of fixed size and then divides the size of secret image by the size of blocks in order to assign a unique address to each block in secret image. In order to understand this scrambling function, we are giving a toy example which shows how our scrambling function work. Let us consider a secret image of size 256×256 and is distributed into blocks of 4×4 pixel.

Chunk dimension = 4 × 4 pixel = 16 Pixel

Total number of chunks = 256 × 256/4 × 4 = 4096 Chunks

Bits required to signify discourse of 4096 chunks = 12

Allocating the discourse of primary chunk = 000000000000 address of latter chunk = 111111111111

4.3.2 Algorithm for Transposition of Blocks using Nonlinear Component Transformation

The clusters of 4 bits of the locations block are inputted to the first, second and third nonlinear components of block ciphers correspondingly. These nonlinear components of block ciphers fulfilled alluring mathematical cryptographic properties. Each block in the input image now exchanges to the new address figured by three nonlinear components of block ciphers. The operational detail and meaning of S-box as takes after:

Table 4.4: S-box Transformation.

S_1

	00	**01**	**10**	**11**
00	12	3	11	1
01	2	7	6	9
10	5	4	0	8
11	15	13	14	10

S_2

	00	**01**	**10**	**11**
00	12	3	1	11
01	7	2	6	9
10	10	14	15	13
11	0	8	4	5

S_3

	00	**01**	**10**	**11**
00	12	3	7	2
01	11	1	9	6
10	0	8	10	14
11	5	4	13	15

$$\text{Address of Block} = \underbrace{1\ \ 0\ \ 1\ \ 1}_{S_1}\ \ \underbrace{0\ \ 1\ \ 0\ \ 1}_{S_2}\ \ \underbrace{0\ \ 0\ \ 1\ \ 1}_{S_3}$$

The info 1011 is linked to S_1, 0101 to S_2 and 0011 associated to S_3. The first two bits gives direction of row and last two bits give direction about column. To start with and fourth bits of info speak to line and second and third piece speak to section in nonlinear component of block cipher. So the information 1011 regarded as a 10 (third line) and 11 (fourth column) giving yield 8 in first nonlinear component. This yield is presently changed over into four bit binary grouping giving 1000. In like manner 0101 and 0011 contributing gives yield 2 (0010) and 2 (0010). Hence concluding firsthand block address is: 1000 0010 0010. So the firsthand position of 1011 0101 0011 (2899^{th} Block) is 1000 0010 0010 (2082^{th} Block). In the similar techniques the new addresses of all the 4096 blocks are calculated and reordered consequently.

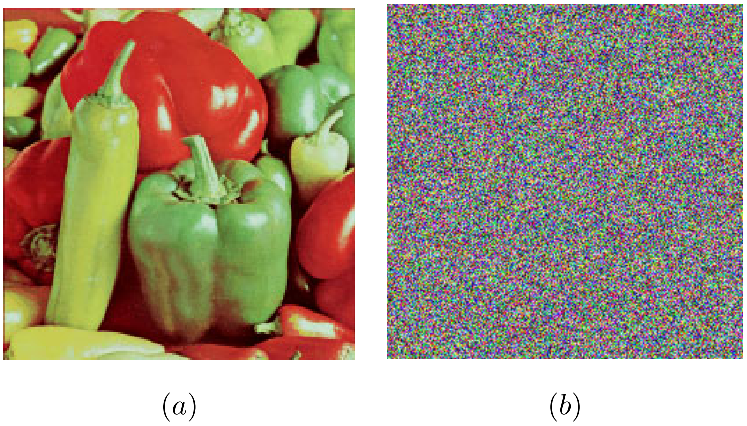

(a) (b)

Fig. 4.2: Original secret image (a), Encrypted secret image (b).

4.4 Inserting Algorithm

The implanting component contains:

4.4.1 Process of Hiding Address into Cover Image

We are now taking original image mean cover image of size $M \times N$ is dividing into four $M/2 \times N/2$ segments the first segment contain information about the address of block and rest three segments contain information about encrypted image.

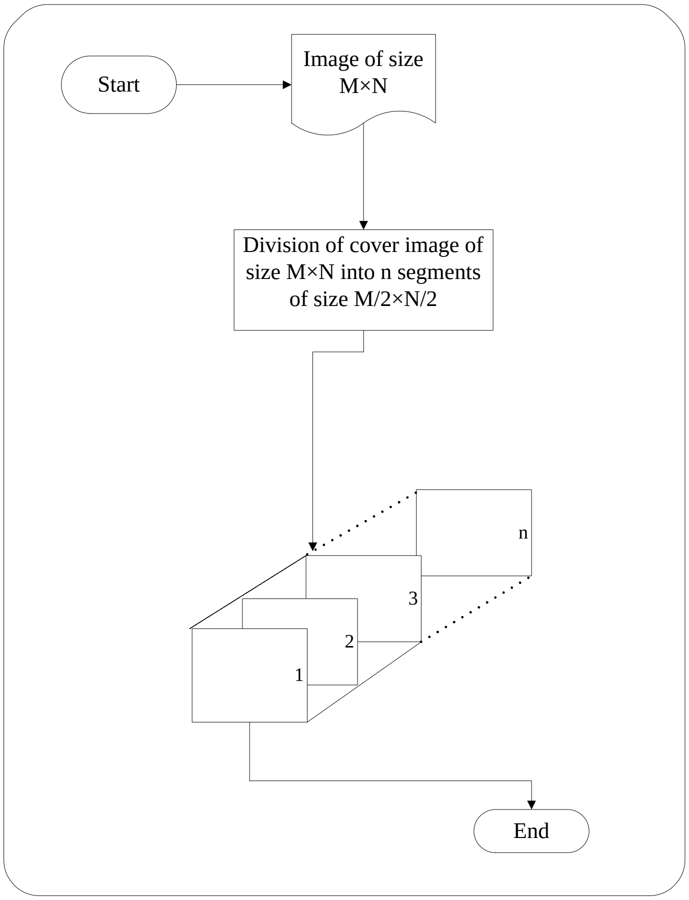

Start
Image of size M×N
Division of cover image of size M×N into n segments of size M/2×N/2
n
3
2
1
End

Fig. 4.3: Division of stego image.

For instance the first segment of the original image is divided into 2^{12} blocks of size 4×4. The total 12 bit modified address of each segment is stored in first 12 pixels and four continuing stay unaffected. Now the LSB of all 12 pixels is altered and interchanged by the bits of the block address.

4.4.2 Hiding of Secret Encrypted Image into Cover Image

The pixel value of encrypted image is hidden in the corresponding pixel in the cover image. The first 3 bits of first pixel of encrypted image is distributed in 2^{nd} region, next 3 bits in 3^{rd} region and 2 bits in 4^{th} region. The bits from encrypted image replace the bits of cover image (see Fig. 4.4).

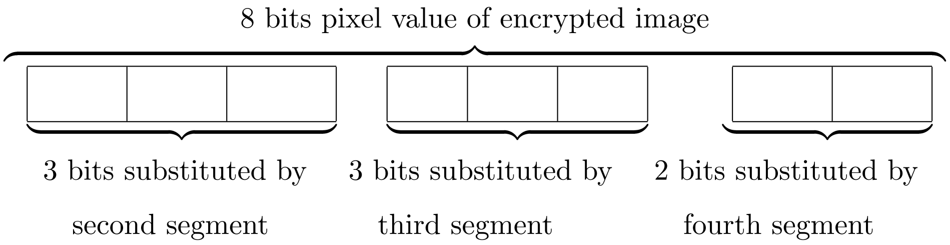
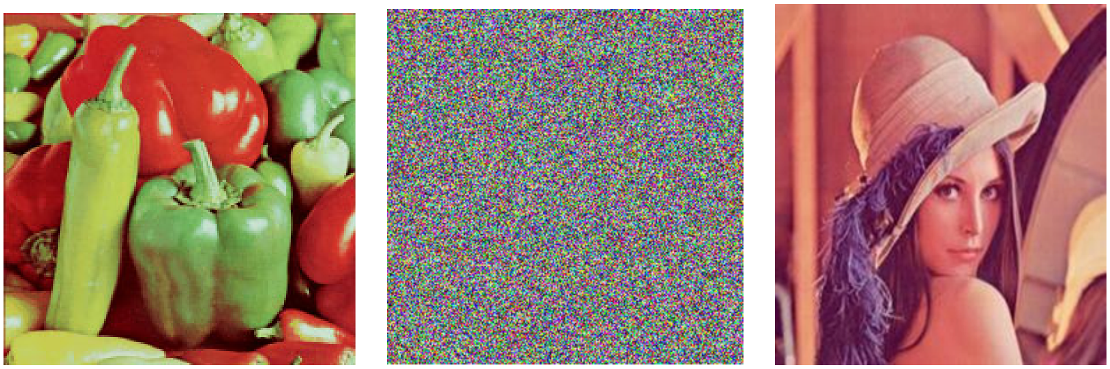

8 bits pixel value of encrypted image
3 bits substituted by second segment
3 bits substituted by third segment
2 bits substituted by fourth segment

Fig. 4.4: Distribution of bits of encrypted image.



(*a*) (*b*) (*c*)

Fig. 4.5: Process of hiding encrypted image of size 256 × 256 × 3 into cover image of size 512 × 512 × 3, (*a*) Secret image, (*b*) Encrypted secret image and (*c*) Stego image.

4.5 Image Retrieval Algorithm

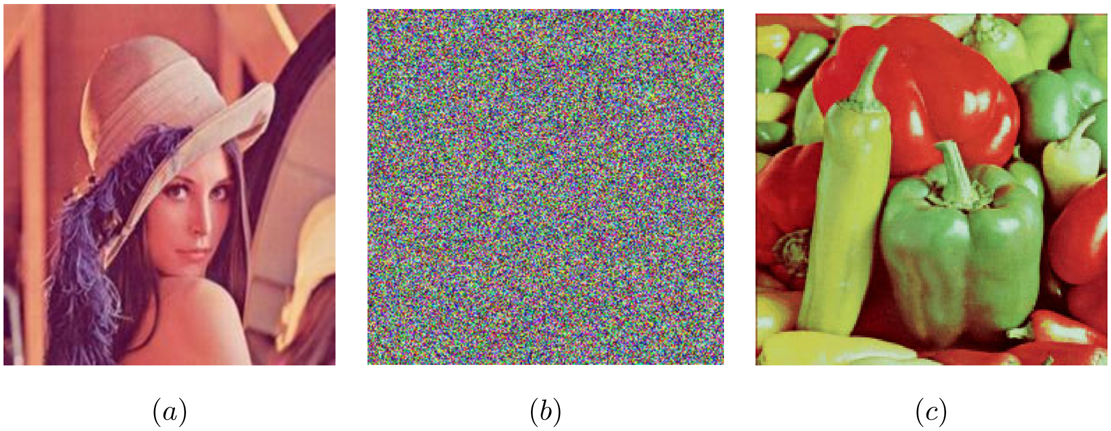
The process of image retrieval consists of two algorithms one for recovery of encrypted or scrambled image and second one is recapturing of secret image from encoded image or encrypted image. These procedures are defined separately in subsequent sections.

4.5.1 Regaining of Scrambled Image

The hided image is recuperated via taking one pixel concurrently from second, third and fourth region. Now with the aid of taking 3 LSB from second vicinity pixel, three LSB from third region pixel and a pair of bits from forth neighborhood pixel types eight bits of first pixel of encrypted picture. Likewise through taking every pixel one at a time from above region forms entire encrypted image.

4.5.2 Regaining of Secrete Image from Scrambled Image

In this phase of the information hiding scheme, we will recover the secret image from our encrypted image. Firstly, we have divided our image into segment of 4×4 pixels having sixteen pixels in each block. Secondly, the address of each block is calculated by compelling first segment of stego image first twelve pixels among 4×4 block are taken and one LSB from these 12 pixels gives 12 bits. These block of twelve bits are inserted to inverse S-box transformation which give the actual address of that block. Each segment from the first part of stego image gives original address of block of that segment into the secret image (see Fig 4.6).



(a) (b) (c)

Fig. 4.6: Process of retrieving secret image from stego image 512 × 512, (a) Stego image, (b) Encrypted secret image and (c) Secret image.

4.6 Analysis of Evaluation Metrics for Steganographic Algorithm

In most sciences, statistical analysis is at the heart of utmost experiments. It is very hard to obtain general theories in these areas that are universally valid. In addition, it is through experiments and surveys that a scientist is able to confirm his theory. In information security different types of statistical metrics were used in order to verify the validity of suggested algorithms. But here we limit ourselves to watermarking performance assessment distortion metrics. The distortion measures the difference between the original cover content and its steganographic version. The stego embedding process introduces some amount of distortion to the original cover image. This distortion can be measured geometrically or perceptually. The measurements which can be used to quantify these distortions are further classified into following most useful categories:

i. Pixel Difference-based measures,

ii. Correlation-based measures,

iii. Human Visual System based measures.

The pixel difference-based measures were derived based on pixel to pixel error such as mean square error(MSE), root mean square error (RMSE), mean absolute error (MAE) and peak signal to noise ratio(PSNR), signal to noise ratio. The correlation based measures includes normalized cross correlation (NCC), structure content (SC) and universal image quality index (UIQI), structural similarity index metric (SSIM) are included in human visual system-based measures. The mathematical expression for each of the above listed statisitcal analyses were already been discussed in previous chapters.

Table 4.5: The results of MSE, PSNR, RMSE, MAE, UIQI, SSIM, SC and NCC of proposed steganographic algorithm for color image.

Proposed Analyses	Color image (cover & stego)	Color image components (cover & steg		
		Red	Green	Blue
MSE	8.8156	10.1537	9.1302	8.8021
PSNR	39.8781	38.5512	37.0159	38.5531
RMSE	2.96910	3.38430	3.18280	3.44860
MAE	2.71580	2.50400	2.33680	2.57840
SC	1.00213	1.00130	1.00070	1.00020
NCC	1.00512	1.00319	1.00100	1.00218
UIQI	0.90360	0.83820	0.85060	0.86110
SSIM	0.93143	0.94470	0.94760	0.94470

4.7 Results and Discussions

The projected scheme is stronger information hiding technique as a result of while not prior data of S-box mapping operate and bits distribution mechanism, the extraction of secrete image from the stego image is impossible. what is more quality of cover image is additionally not degraded due to variation in maximum 3 LSB of 50% of pixel that mirrors solely $zero - eight$ distinction component value and 2 LSB of 25% of component that reflects solely $0-3$ distinction component price and rest having only 1 bit distinction that reflect solely 0-1difference. In addition the projected theme is capable of not simply scrambling knowledge however conjointly changes the intensity of the pixels that contributes to the protection of the secret writing. The degree of distortion of image can be measured by using mean square error (MSE), root mean square error (RMSE), peak signal to noise ratio (PSNR), mean absolute error (MAE). These measures are fundamentally belong from the category of pixel difference based measures. All the pixels of an image are equally important. With the use of PSNR, MSE, RMSE and MAE, gray-value difference between corresponding pixels of the original image and the pixels of stego image are considered. All the pixels of an image are independent of their neighbor pixels. Therefore, pixels at different position have different effect on human visual system (HVS). The values of pixel difference approximation namely MSE, PSNR, RMSE and MAE clearly reflected that our proposed scheme is quite suitable for information hiding of images. Here we not only consider pixel difference based quality measures of an image but also use correlation based and human visual based analyses. The correlation based measures includes structure content (SC) and normalized cross correlation (NCC), and human visual based metrics consists of universal image quality index (UIQI) and structure similarity index measure (SSIM). The correlation based measure namely SC and NCC represent the correlation among the neighboring pixels. The values of SC and NCC (see Table 4.5) close to unity which clearly shows a small disturbance caused by proposed scheme with respect to pixel neighbor. Also the similarity between cover and stego image can be verified through the use of HVS based measures. The HVS based measures is comprises of UIQI and SSIM respectively. The close investigation of the values of UIQI and SSIM (see Table 4.5) which is near to unity reflect that with naked eye it is quite tough to differentiate between cover and stego images.

4.8 Conclusion

The suggested information hiding technique utilize small nonlinear components of block cipher namely S-box that improve the confusion capability of pixels value and address of blocks in encrypted secret image. The present work not only uses small nonlinear components of block ciphers but also combine steganography and cryptography in order to transmit any information through insecure line of communication secretly. With the quick improvement of computerized innovation and web, steganography has propelled a considerable measure over past years. The majority of the current techniques for steganography concentrate on the installing system and lesser thought to the preprocessing stages, for instance encryption of emit picture, as they depend vigorously on the routine encryption algorithms which clearly are not custom-made to steganography applications where flexibility, robustness and security are required. The present steganographic algorithm is mainly depending on double layer security that is cryptography and steganography which is clearly a major refinement is existing technique.

Chapter 5

Optimal Criteria for the Selection of Cryptographically Secure Nonlinear Component

The block ciphers are the most important components due to is applicability in the region of cryptography. The execution of a new cipher relies on upon the quality of the algorithm which is in charge of making confusion in the encryption process. This usefulness is accomplished by the utilization of nonlinear component which is the main segment included in numerous block ciphers [64]. The change in the mathematical and statistical properties of nonlinear component has been a focal point of fascination in the field of encryption. In this chapter, we demonstrate the Balancedness, Nonlinearity, Correlation immunity, Absolute indicator, Sum of square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Number of fixed points, Number of opposite fixed points, Composite algebraic immunity, Robustness to differential cryptanalysis, Delta uniformity, SNR(DPA) and Confusion coefficient variance for existing S- boxes. There are various rising encryption techniques as of late proposed in writing. In spite of the fact that these algorithms have all the earmarks of being promising, there power is not yet settled and they are advancing to wind up models.

Some of these ciphers worth specifying are the general population key cryptosystems in view of chaotic Chebyshev polynomials [61], advanced encryption standard (AES) cryptosystem utilizing the highlights of mosaic picture for to a great degree secure high information rate [54], and picture encryption by means of strategic guide capacity and store tree [57]. The most widely recognized strategies used to break down the measurable quality of nonlinear components of block ciphers are the connection investigation, direct estimate likelihood, differential guess likelihood, and strict torrential slide paradigm and so forth. We have included relationship strategy as a benchmark for the rest of the investigation utilized as a part of this work. Except for connection investigation, the application and utilization of the aftereffects of factual examination, introduced in this section, have not been connected to assess the quality of nonlinear components of block ciphers. The connection investigation, entropy examination, differentiate examination, homogeneity investigation, vitality examination, and mean of outright deviation investigation are performed on AES [56], APA [55], Gray [64], Lui [60], residue prime [53], S_8 AES [59], SKIPJACK [63], and Xyi [62] nonlinear components. The aftereffects of these examinations are broke down by the proposed basis by considering the estimations of all the investigation on various nonlinear components.

The proposed criterion uses the results from Balancedness, Nonlinearity, Correlation immunity, Absolute indicator, Sum of Square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Strict Avalanche Criteria, Number of Fixed Points, Number of opposite Fixed Points, Composite Algebraic Immunity, Robustness to Differential cryptanalysis, Delta Uniformity, SNR(DPA) and Confusion coefficient variance. These analyses are applied to advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S_8-AES, SKIPJACK, and Xyi S- boxes in order to determine the appropriateness of an nonlinear component to multimedia applications.

5.1 Cryptographic Properties

Next we enumerate cryptographic properties of Boolean functions and nonlinear components of block ciphers. With each of the properties we list the references where an interested reader can find definitions and formulas. First block of citations refers to Boolean functions and second one to nonlinear components of block ciphers which we have already discussed in chapter 1. Here in this chapter, we will apply all possible cryptographically strong algebraic properties in order to provide a new scheme for the selection of good nonlinear component of block cipher.

5.2 Algebraic and Statistical Analyses

In this section, we analyze nonlinear components of block ciphers (AES, APA, Gray, Lui J, Residue Prime, S_8 AES, SKIPJACK, and Xyi) used in popular block ciphers. Without the loss of generality, the analysis can be extended to nonlinear components of block ciphers of other sizes. The algebraic and statistical analyses are used to determine the application and appropriateness of an S-box [64]. The strength of an S-box can be evaluated by examining various parameters generated by numerous algebraic and statistical analyses. It is imperative to be familiar with the significance and relationship between the outcomes of different types of analyses. Therefore, we develop a criterion which carefully inspects and scrutinizes the available parameters and makes a decision based on optimum assessment. The procedure begins with the Balancedness, Nonlinearity, Correlation immunity, Absolute indicator, Sum of square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Number of fixed points, Number of opposite fixed points, Composite algebraic immunity, Robustness to differential cryptanalysis, Delta uniformity, SNR(DPA) and Confusion coefficient variance. These analyses, when applied in combination, provide more vivid results and consequently assist in evaluating the performance of nonlinear components of block ciphers. To the best of our knowledge, Balancedness, Nonlinearity, Correlation immunity, Absolute indicator, Sum of square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Number of fixed points, Number of opposite fixed points, Composite algebraic immunity, Robustness to differential cryptanalysis, Delta uniformity, SNR(DPA) and Confusion coefficient variance, have not been extensively analyzed and studied for the evaluation of nonlinear components of block ciphers. The results for the above mentioned analyses for nonlinear components of block ciphers (AES, APA, Gray, Lui J, Residue Prime, S_8-AES, SKIPJACK, and Xyi) are given in table 5.1 and 5.2 respectively. Also the algorithm that classifies the lists of given nonlinear components of block ciphers to be useful for further real world applications is given in next section. Several examples of nonlinear components of block ciphers are given in tables 5.1 and 5.2. These nonlinear components of block ciphers should be regarded as benchmarks. Additionally, we give values for the following cryptographic properties: algebraic degree (deg), correlation immunity (CI), signal to noise ratio (SNR), global avalanche criterion (GAC)-absolute indicator and sum of square indicator, and differential-uniformity.

5.3 Proposed Procedure

The proposed benchmarks for the selection of optimal best nonlinear components of block ciphers for multimedia applications is give as follows:

Algorithm 37 *Let us consider n nonlinear components of block ciphers say $S_1, S_2, ..., S_n$. We can say that S-box S_i is optimal with respect to algebraic analyses than S_j for $j \in \{1, 2, ..., n\} \backslash i$ if*

1. *If the Nonlinearity of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

2. *If Correlation immunity of S_i is less than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

3. *If absolute indicator of S_i is less than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

4. *If the sum of square indicator of S_i is less than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

5. *If algebraic degree of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

6. *If algebraic immunity of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

7. *If transparency order of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

8. *If propagation characteristics of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

9. *If number of fixed points of S_i is less than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

10. *If number of opposite fixed points of S_i is less than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

11. *If composite algebraic immunity of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

12. *If robustness to differential cryptanalysis of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

13. *If delta uniformity of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

14. *If SNR (DPA) of S_i is greater than S_j for $j \in \{1, 2, ..., n\} \backslash i$.*

15. If Confusion coefficient variance of S_i *is less than* S_j *for* $j \in \{1, 2, ..., n\} \setminus i$.

Table 5.1: Comparison of algebraic analyses for AES, APA, Gray and Prime nonlinear components of block

	Existing nonlinear components of block ciphers			
Algebraic Properties	AES	APA	$Gray$	$Prime$
Balanced	Yes	Yes	Yes	Yes
Nonlinearity	112	112	112	112
Correlation immunity	0	0	0	0
Absolute indicator	32	32	32	152
Sum of Square indicator	133120	133120	133120	324736
Algebraic degree	7	7	7	7
Algebraic immunity	4	4	4	4
Transparency order	7.860	7.859	7.860	7.756
Propagation characteristics	0	0	0	0
Number of Fixed Points	0	0	5	2
Number of opposite Fixed Points	0	2	0	0
Composite Algebraic Immunity	4	4	4	4
Robustness to Differential cryptanalysis	0.984	0.984	0.984	0.719
Delta Uniformity	4	4	4	72
SNR (DPA)	9.600	8.910	9.600	9.925
Confusion coefficient variance	0.11304	0.139337	0.111304	0.100074

By analyzing the algebraic characteristics presented in above table, the nonlinearity, algebraic degree, algebraic immunity, propagation characteristics, composite algebraic immunity of AES, APA, Gray, Prime nonlinear components of block ciphers are 112, 7, 4, 0 and 4. The high values of absolute indicator, sum of square indicator, delta uniformity, number of fixed points and low value of robustness to differential cryptanalysis in case of prime S-box does not qualify it for optimally best S-box whereas transparency order, SNR(DPA), confusion coefficient variation is quite comparable properties of prime S-box with AES, APA and Gray nonlinear components of block ciphers respectively.

Table 5.2: Comparison of algebraic analyses for S_8-AES, Skipjack and Xyi nonlinear components of block ci

	Existing nonlinear components of block ciphers		
Algebraic Properties	S_8-AES	Skipjack	Xyi
Balanced	Yes	Yes	Yes
Nonlinearity	110	100	88
Correlation immunity	0	0	0
Absolute indicator	40	96	96
Sum of square indicator	143104	238336	316672
Algebraic degree	8	7	7
Algebraic immunity	4	4	4
Transparency order	7.857	7.821	7.822
Propagation characteristics	0	0	0
Number of fixed points	0	0	1
Number of opposite fixed points	1	0	2
Composite algebraic immunity	4	4	4
Robustness to differential cryptanalysis	0.969	0.953	0.953
Delta uniformity	6	12	12
SNR (DPA)	9.227	8.743	9.448
Confusion coefficient variance	0.123747	0.147139	0.116957

The nonlinearity of S_8-AES S-box is high as compared to Skipjack and Xyi nonlinear components of block ciphers which show that Boolean functions involved in S_8-AES S-box are cryptographically secure. All the nonlinear components of block ciphers enumerated in the tables 5.1 and 5.2 are balanced so we did not write that property in the tables. Also, all the nonlinear components of block ciphers have algebraic degree equal to 7. We omitted correlation immunity property from the table since it must be 0 as evident by Siegenthaler's inequality [9]. Further, none of the nonlinear components of block ciphers satisfy SAC property so we also omitted it from the table. Low nonlinearity value does not ensure low transparency order. In fact, it is easy to find nonlinear components of block ciphers with nonlinearity below 90 and with transparency order comparable to that of AES S-box. Since we could not find any S-box with nonlinearity level the same as in AES case and with significantly lower transparency order, we opted to find nonlinear components of block ciphers with nonlinearity lower than in AES, but also with transparency order significantly lower than in AES case. The lower values of absolute indicator, sum of square indicator and delta uniformity clearly elucidates the effectiveness of S_8-AES nonlinear components of block ciphers in terms of mentioned criteria and also the values of transparency order, robustness to differential cryptanalysis, SNR (DPA) and confusion coefficient variance are quite comparable with Skipjack and Xyi nonlinear components of block ciphers. The number of fixed points and opposite fixed points in case of AES is not found whereas APA, Gray, Prime, S_8-AES and Xyi nonlinear components of block ciphers have fixed and opposite fixed points which clearly reflecting the weakness in these nonlinear components of block ciphers.

5.4 Conclusion

In this work, we are mainly consider some standard nonlinear components of block ciphers likewise AES, APA, Gray, Prime, S_8-AES, Skipjack and Xyi etc., for our proposed optimal criteria. We have analyzed transparency order for the nonlinear components of block ciphers of size 8×8 which is the DPA resistance properties. The properties of balancedness, nonlinearity, correlation immunity, absolute indicator, sum of Square indicator, algebraic degree, algebraic immunity, transparency order, propagation characteristics, number of fixed points, number of opposite fixed points, composite algebraic immunity, robustness to differential cryptanalysis, delta uniformity, SNR(DPA) and confusion coefficient variance were not yet been presented for the classification of AES, APA, Gray, Prime, S_8-AES, Skipjack and Xyi nonlinear components of block ciphers.

Chapter 6

Nonlinearity of Nonbalanced and Nearly Bent Boolean Functions

An important criterion that a Boolean function would satisfy is high nonlinearity to introduce confusion into the secure system. There are several types of famous Boolean functions were introduced in literature in order to food the need of cryptographic applications. Usually in literature available for Boolean functions, authors discussed one property of these functions with respect to other characteristics of a Boolean function. A variety of desirable criteria for Boolean functions with cryptographic application have been identified which includes; balancedness, high nonlinearity, strict avalanche criterion (SAC), correlation immunity (CI) of reasonably high order, low autocorrelation (AC), high algebraic degree (AD), algebraic immunity (AI), transparency order (TO), linear approximation (LA), differential approximation (DA), sum of deviation (SD) and sum of square deviation (SSD) etc. The exchange off between these criteria have gotten a great deal of consideration in Boolean function writing for quite a while. The more criteria that must be considered, the more troublesome it is to produce Boolean functions fulfilling those properties absolutely by useful logarithmic means. Without a doubt, late work has tried to mix development with parts of PC look. A considerable lot of the best functions on little quantities of factors have been gotten along these lines.

The connection between the Walsh-Hadamard change and the autocorrelation capacity of Boolean capacities is utilized to think about propagation attributes of these capacities [79]. The

SAC paradigm and the ideal nonlinearity standard are summed up in a propagation model of degree k. New properties and developments for Boolean bent functions are given and furthermore the augmentation of the definition to odd estimations of n is examined. New properties of functions fulfilling higher order SAC are inferred. At long last a general system is built up to arrange functions as per their propagation attributes if various bits is kept steady.

Nonlinearity criteria for Boolean functions are arranged in perspective of their reasonableness for cryptographic outline. The characterization is set up as far as the biggest change amass leaving a measure invariant. In this regard two criteria end up being of unique intrigue, the separation to linear structures and the separation to affine capacities, which are appeared to be invariant under every single affine change. As to these criteria an ideal class of functions is considered. These functions all the while have most extreme distance to affine functions and greatest distance to linear structures, and additionally least connection to affine functions. The functions with these properties are demonstrated to match with specific functions known in combinatorial hypothesis, where they are called bent functions. They are appeared to have reasonable applications for block and stream ciphers [80]..

The nonlinearity of a function f on the $n-$dimensional vector space V_n, is limited from above by $2^{n-1} - 2^{\frac{n}{2}-1}$. In cryptographic practice, nonlinear functions are normally usefully gotten such that they bolster certain numerical or cryptographic prerequisites. Thus an imperative inquiry is the way to compute the nonlinearity of a function when additional data is accessible. This inquiry is address with regards to auto-relationships, and infer four (two upper and two lower) limits on the nonlinearity of a function. Qualities and shortcomings of each bound are additionally inspected [81].

The importance of nonlinear functions in cryptology is best delineated by the accomplishment of straight cryptanalytic assaults as of late found by Matsui in [105]. Understanding its significance, cryptographers regularly wish to discover the nonlinearity of a cryptographic function, or when the correct esteem isn't effectively possible, a lower and additionally an upper bound on the nonlinearity. A verifiable truth about the upper bound on nonlinearity is $N_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$, where N_f signifies the nonlinearity of f . Conversely, less is thought about the lower bound on nonlinearity, other than some advance made in [11,13] and additionally such paltry certainties as $N_f > 0$ if and only if f is nonlinear.

In cryptographic practice, for example, the outline of a substitution box utilized by a private key encryption calculation or a restricted hashing calculation, or a nonlinear criticism work utilized as a part of a pseudorandom arrangement generator, one as a rule produces a nonlinear capacity such that the capacity would fulfill certain numerical or cryptographic necessities. Two upper and two lower limits on the nonlinearity of a Boolean capacity have been built up. These limits could be especially valuable when certain basic data on a Boolean capacity is accessible. Every one of the limits have been fundamentally in view of the autocorrelation of a capacity under thought. This opens up a conceivable new road for future research, which is to expand the outcomes so they consider different factors, for example, direct structures, logarithmic degree and worldwide torrential slide qualities (GAC) presented in [81].

Boolean functions utilized as a part of cryptographic applications need to fulfill different cryptographic criteria. Despite the fact that the decision of the criteria relies upon the cryptosystem in which they are utilized. There are a few properties (balancedness, nonlinearity, high algebraic degree, correlation immunity, propagation criteria) which a cryptographically solid Boolean function should have. In [82], the previously mentioned properties in the arrangement of every Boolean function (all adjusted Boolean functions) and demonstrate that relatively every Boolean function (relatively every adjusted Boolean function) fulfills all previously mentioned criteria on levels near ideal and along these lines can be thought to be cryptographically solid.

Boolean functions used as a piece of cryptographic applications need to satisfy diverse cryptographic criteria. In spite of the way that the choice of the criteria depends upon the cryptosystem in which they are used. There are a couple of properties (balancedness, nonlinearity, high logarithmic degree, relationship insusceptibility, propagation criteria) which a cryptographically strong Boolean function ought to have. In [82], the already specified properties in the plan of each Boolean function (all balanced Boolean functions) and show that moderately every Boolean function (generally every balanced Boolean function) satisfies all beforehand said criteria on levels close perfect and thus can be believed to be cryptographically strong.

Nonlinear qualities of (Boolean) functions are one of the imperative issues both in the outline and cryptanalysis of (private key) encryption schemes. In [108], examines nonlinear properties of functions from three extraordinary however firmly related viewpoints: maximal odd weighting subspaces, limitations to cosets, and hypergraphs, all related with a function. Primary commitments of this work incorporates: (1) by utilizing a duality property of a function, creators have gotten a few outcomes that are identified with bring down limits on nonlinearity and on the quantity of terms, of the function, (2) the limitation of a function on a coset significantly affects cryptographic properties of the function, (3) creators recognize connections between the nonlinearity of a function and the conveyance of terms in the mathematical ordinary type of the function, (4) Also they have demonstrated that cycles of odd length in the terms, and also quadratic terms, in the arithmetical typical type of a function assume an imperative part in deciding the nonlinearity of the function.

The relationship between the nonlinearity and the order of resiliency of a Boolean function were investigated in [84]. They have proven a sharper version of McEliece theorem for Reed-Muller codes as applied to resilient functions, which also generalizes the well-known Xiao-Massey characterization. As a consequence, a nontrivial upper bound on the nonlinearity of resilient functions is obtained. In addition to that these functions achieving the best possible trade-off which can be constructed by the Maiorana-McFarland like technique.

The connection between the nonlinearity and the request of flexibility of a Boolean function were examined in [84]. They have demonstrated a more keen adaptation of McEliece hypothesis for Reed-Muller codes as connected to versatile functions, which likewise sums up the notable Xiao-Massey portrayal. As an outcome, a nontrivial upper bound on the nonlinearity of strong functions is gotten. Notwithstanding that these functions accomplishing the most ideal exchange off which can be developed by the Maiorana-McFarland like strategy.

The connection between the nonlinearity of a Boolean function and its propagation attributes were researched in [86]. They got a totally new class of Boolean function with high nonlinearity and great propagation measure. On the other hand, any Boolean function fulfilling the propagation measure as for a direct subspace of codimension 1 or 2 has a high nonlinearity. We additionally call attention to that most exceptionally nonlinear functions with a three-esteemed Walsh range can be changed into $1-$resilient functions.

The plan of ordinary cryptographic frameworks depends on two basic standards presented by Shannon [2]: disarray and dissemination. Disarray goes for disguising any algebraic structure in the framework. Dispersion comprises in spreading out the impact of a minor change of the info information over all yields. Most ordinary natives are worried about these basic standards: mystery key figures (square figures and stream figures) and additionally hash functions. Disarray and dispersion can be measured by a few properties of the Boolean functions portraying the framework. Disarray relates to the nonlinearity of the included functions, i.e., to their Hamming separations to the arrangement of affine functions. Dispersion is identified with the propagation attributes of the considered Boolean function. The important cryptographic amounts are the predispositions of the yield likelihood disseminations of the subsidiaries moderately to the uniform dispersion; they are estimated by the auto-relationship coefficients of the function.

Dispersion is along these lines assessed by integral pointers: propagation paradigm, separation to the arrangement of every single Boolean function with a straight structure and sum-of-squares marker. Every one of these amounts will be here considered in a brought together approach.

A noteworthy connection amongst dispersion and perplexity criteria was brought up by Meier and Stafelbach [80]. They demonstrated that maximal nonlinearity and impeccable propagation qualities are equal necessities for Boolean functions with a significantly number of factors. Tragically those functions which accomplish culminate dispersion and immaculate perplexity (called bowed functions) are not adjusted; that implies that they don't have a uniform yield conveyance. The development of adjusted Boolean functions having a high nonlinearity and great propagation attributes at that point remains an open issue albeit such functions are basic segments of cryptographic natives and, further research the connection amongst dispersion and perplexity criteria for Boolean functions and demonstrated that profoundly nonlinear functions more often than not match with the functions having amazing propagation qualities. In this unique situation, they bring up the significant pretended by the exceptionally nonlinear functions whose Walsh range takes three esteems. They display general developments of such functions and demonstrate that it can without much of a stretch be changed into adjusted first-arrange connection safe functions. They are hence appropriate joining functions for pseudo-irregular generators since they guarantee a high protection from quick connection assaults.

Dispersion is in this way evaluated by reciprocal markers: propagation rule, separation to the arrangement of every single Boolean function with a direct structure and entirety of-squares pointer. Every one of these amounts will be here considered in a bound together approach.

As of late, weight detachability comes about on resilient and correlation immune Boolean functions have gotten a great deal of consideration. These outcomes have coordinate results towards the upper bound on nonlinearity of resilient and correlation immune Boolean functions of certain request. Presently the unmistakable prerequisite in the outline of resilient Boolean functions (which improves Siegenthaler's imbalance) is to give comes about which accomplish the upper bound on nonlinearity. Here we build a $7-$variable, $2-$resilient Boolean function with nonlinearity 56. This understands the greatest nonlinearity issue for $7-$variable functions with any request of flexibility. Utilizing this $7-$variable function, we likewise build a 10-variable, 4-resilient Boolean function with nonlinearity 480. Additionally creators finished up with developments of some uneven correlation immune functions of 5 and 6 factors which accomplish the upper bound on nonlinearity [87].

It is realized that Boolean functions utilized as a part of stream and piece figures ought to have great cryptographic properties to oppose mathematical assaults. Up to this point, there have been a few developments of Boolean functions accomplishing ideal arithmetical invulnerability. Nonetheless, the greater part of their nonlinearities are low. Carlet and Feng contemplated a class of Boolean functions with ideal logarithmic resistance and concluded the lower bound of its nonlinearity, which is great, however not high. In addition, the principle pragmatic issue with this development is that it can't be executed effectively. As of late Qichun et. al.,[100], set forward another technique to develop cryptographically noteworthy Boolean functions by utilizing crude polynomials, and build three interminable classes of Boolean functions with great cryptographic properties: balancedness, ideal logarithmic degree, ideal arithmetical resistance, and a high nonlinearity.

As of late, a few development strategies for very nonlinear Boolean functions with generally great mathematical properties were proposed. These methodologies oversee in enhancing the vast majority of the significant cryptographic criteria, however not every one of them in the meantime. Typically, either the nonlinearity limits are somewhat free (however the real nonlinearity is moderately high) or the functions don't give a decent protection from quick logarithmic cryptanalysis. Enes and Yongzhuang built up a hypothetical system for utilizing objects in reasonable projective geometry spaces for development of exceedingly nonlinear Boolean functions. This enables us to set up tight limits on the nonlinearity utilizing straightforward checking contentions, accordingly maintaining a strategic distance from rather convoluted assessments of certain follow aggregates. This technique produces a class of completely advanced functions, that is the functions separated from high nonlinearity additionally have the most extreme mathematical degree and ideal arithmetical insusceptibility. Contrasted with the classes of functions proposed via Carlet and Feng, Wang et. al., and Zeng et al., these proposed Boolean functions in [101], accomplish a somewhat better nonlinearity which is exchanged off against a little more terrible protection against quick arithmetical assaults. Then again, contrasted with the functions by Tang et al. also, Tu and Deng, the nonlinearity in [101], is to some degree lower, however the mathematical properties are somewhat better.

The fundamental aspects of our work here is to concern about the properties and constructions of a new class of S-box namely Boolean functions that attain high nonlinearity, satisfy SAC and remains non-balanced. We presented a novel technique for constructing highly nonlinear non-balanced functions which is based on maximal cyclic subgroup of a Galois ring. It is very interesting to note that these non-balanced functions obtained by using proposed technique, achieve nonlinearity higher than that attainable by any previously known construction method. We also initiate the research into the systematic construction of highly nonlinear non-balanced functions satisfying the SAC and BIC of SAC criterion.

6.1 Fundamental Properties of Galois Rings

We begin with few basic definitions of unitary commutative rings.

Definition 38 *Let R be a commutative ring with identity.*

*1. An element u is a **unit** in R if there exists an element v in R such that $u.v = 1$, where 1 is the identity of R.*

*2. Nonzero element a of ring R is called **zero divisor** if there exist a nonzero element b in R such that $a.b = 0$.*

Definition 39 *A commutative ring R with identity is said to be a **local ring** if and only if its all non unit elements form an additive Abelian group. Alternatively, a commutative ring R*

with identity is local if it has a unique maximal ideal. For instance $\mathbb{Z}_{p^k}$, where p is a prime integer and m is any positive integer, is a local ring.

Definition 40 *Let (R, M) be a local commutative ring with identity having residue field $K(= R/M)$. $\varphi : R \to R/M$ is a canonical epimorphism, defined as $\varphi(a) = \widehat{a} = a + M, a \in R$. An irreducible polynomial $\phi(x) = a_0 + a_1x + \cdots + a_mx^m \in R[x]$ over R is said to be a* ***basic irreducible*** *if $\varphi(\phi(x)) = \overline{\phi(x)} = \widehat{a_0} + \widehat{a_1}x + \cdots + \widehat{a_m}x^m \in K[x]$ is irreducible over K [78]*

Theorem 41 *[148, Theorem 2] There is unique maximal cyclic subgroup of $\mathcal{R}^*$of order relatively prime to p. This cyclic subgroup has order $p^s - 1$.*

The maximal cyclic subgroup G_n is isomorphic to the Galois group $\mathcal{K}^*$.

6.2 Fabriaction of Nonlinear Component over Galois Ring $GR\left(2^3, 8\right)$

In this section, we construct an 8×8 S-box by using the maximal cyclic subgroup G_{255} of group of units of the Galois ring $GR\left(2^3, 8\right)$. The constructed S-box is used in image encryption. For this construction we use the computational techniques of [78] in obtaining the maximal cyclic subgroup G_{255}.

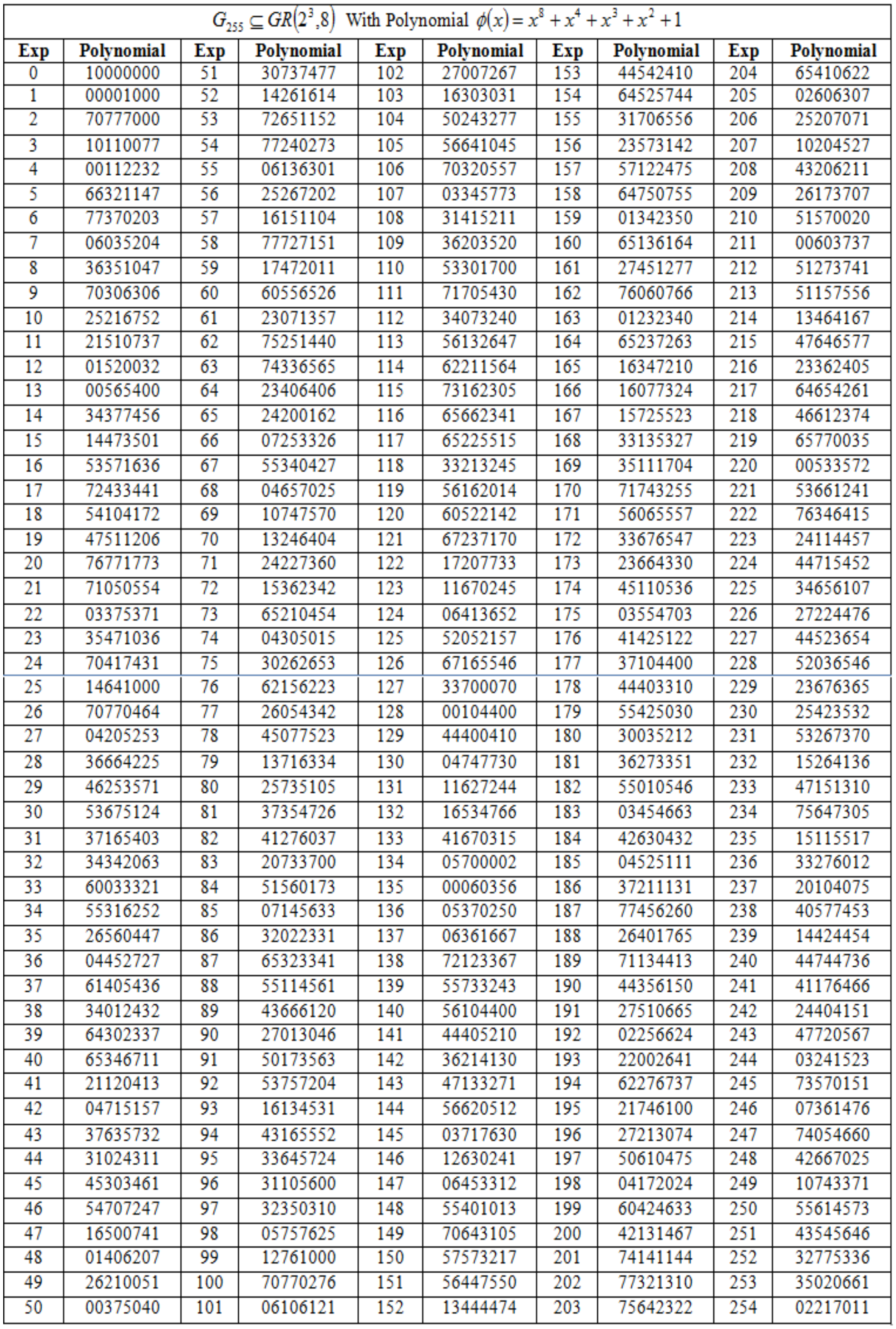
6.2.1 Cyclic Subgroup of Invertible elements of $GR\left(\mathbb{Z}_{2^3}, 8\right)$

For the local ring $\mathbb{Z}_{2^3}$, the binary field $\mathbb{Z}_2$ is its residue field. The polynomial $\phi(x) = x^8 + x^4 + x^3 + x^2 + 1 \in \mathbb{Z}_{2^3}[x]$ is a basic irreducible polynomial. Galois ring $GR\left(\mathbb{Z}_{2^3}, 8\right)$ of order 8^8 is obtained by constructing the factor ring $\frac{\mathbb{Z}_8[x]}{(\phi(x))}$, whose elements are of the form $\{a_0 + a_1x + a_2x^2 + ... + a_6x^6 + a_7x^7 : a_i^{'}s \in \mathbb{Z}_8\}$. The corresponding Galois field $GF(2, 8)$ of order 256 becomes $\frac{\mathbb{Z}_2[x]}{(\overline{\phi(x)})}$ and its elements are obtained by using the identity $u^8 + u^4 + u^3 + u^2 + 1$ modulo 2 and modulo $\overline{\phi(u)}$.

Maximal cyclic subgroup of group of units of $GR\left(\mathbb{Z}_{2^3}, 8\right)$ is obtained by considering u as the root of $\overline{\phi(x)}$ in $\mathbb{Z}_2$. By using the algorithm given in [78], which calculating the successive powers of u modulo 2 and module $\overline{\phi(u)}$, we have $u^{255} = 1$. Hence, the maximal cyclic subgroup of group of units of $GR\left(\mathbb{Z}_{2^3}, 8\right)$ has 255 elements. To find these elements, let α be the root of $\phi(x)$. Then by calculating the consecutive powers of α modulo 8 and modulo $\phi(\alpha)$, we have

$\alpha^{1020} = 1$. Thus, the elements of G_{255} are generated by $\beta = \alpha^4$. These elements are listed in Table 6.1, in which the polynomials are given in increasing powers of α, i.e., the element 77370203 represents the polynomial $7 + 7\alpha + 3\alpha^2 + 7\alpha^3 + 2\alpha^5 + 3\alpha^7$.

Table 6.1 : Elements of maximal cyclic subgroup of group of units of $GR\left(\mathbb{Z}_{2^3}, 8\right)$.



$G_{255} \subseteq GR\left(2^3,8\right)$ With Polynomial $\phi(x) = x^8 + x^4 + x^3 + x^2 + 1$									
Exp	**Polynomial**	**Exp**	**Polynomial**	**Exp**	**Polynomial**	**Exp**	**Polynomial**	**Exp**	**Polynomial**
0	10000000	51	30737477	102	27007267	153	44542410	204	65410622
1	00001000	52	14261614	103	16303031	154	64525744	205	02606307
2	70777000	53	72651152	104	50243277	155	31706556	206	25207071
3	10110077	54	77240273	105	56641045	156	23573142	207	10204527
4	00112232	55	06136301	106	70320557	157	57122475	208	43206211
5	66321147	56	25267202	107	03345773	158	64750755	209	26173707
6	77370203	57	16151104	108	31415211	159	01342350	210	51570020
7	06035204	58	77727151	109	36203520	160	65136164	211	00603737
8	36351047	59	17472011	110	53301700	161	27451277	212	51273741
9	70306306	60	60556526	111	71705430	162	76060766	213	51157556
10	25216752	61	23071357	112	34073240	163	01232340	214	13464167
11	21510737	62	75251440	113	56132647	164	65237263	215	47646577
12	01520032	63	74336565	114	62211564	165	16347210	216	23362405
13	00565400	64	23406406	115	73162305	166	16077324	217	64654261
14	34377456	65	24200162	116	65662341	167	15725523	218	46612374
15	14473501	66	07253326	117	65225515	168	33135327	219	65770035
16	53571636	67	55340427	118	33213245	169	35111704	220	00533572
17	72433441	68	04657025	119	56162014	170	71743255	221	53661241
18	54104172	69	10747570	120	60522142	171	56065557	222	76346415
19	47511206	70	13246404	121	67237170	172	33676547	223	24114457
20	76771773	71	24227360	122	17207733	173	23664330	224	44715452
21	71050554	72	15362342	123	11670245	174	45110536	225	34656107
22	03375371	73	65210454	124	06413652	175	03554703	226	27224476
23	35471036	74	04305015	125	52052157	176	41425122	227	44523654
24	70417431	75	30262653	126	67165546	177	37104400	228	52036546
25	14641000	76	62156223	127	33700070	178	44403310	229	23676365
26	70770464	77	26054342	128	00104400	179	55425030	230	25423532
27	04205253	78	45077523	129	44400410	180	30035212	231	53267370
28	36664225	79	13716334	130	04747730	181	36273351	232	15264136
29	46253571	80	25735105	131	11627244	182	55010546	233	47151310
30	53675124	81	37354726	132	16534766	183	03454663	234	75647305
31	37165403	82	41276037	133	41670315	184	42630432	235	15115517
32	34342063	83	20733700	134	05700002	185	04525111	236	33276012
33	60033321	84	51560173	135	00060356	186	37211131	237	20104075
34	55316252	85	07145633	136	05370250	187	77456260	238	40577453
35	26560447	86	32022331	137	06361667	188	26401765	239	14424454
36	04452727	87	65323341	138	72123367	189	71134413	240	44744736
37	61405436	88	55114561	139	55733243	190	44356150	241	41176466
38	34012432	89	43666120	140	56104400	191	27510665	242	24404151
39	64302337	90	27013046	141	44405210	192	02256624	243	47720567
40	65346711	91	50173563	142	36214130	193	22002641	244	03241523
41	21120413	92	53757204	143	47133271	194	62276737	245	73570151
42	04715157	93	16134531	144	56620512	195	21746100	246	07361476
43	37635732	94	43165552	145	03717630	196	27213074	247	74054660
44	31024311	95	33645724	146	12630241	197	50610475	248	42667025
45	45303461	96	31105600	147	06453312	198	04172024	249	10743371
46	54707247	97	32350310	148	55401013	199	60424633	250	55614573
47	16500741	98	05757625	149	70643105	200	42131467	251	43545646
48	01406207	99	12761000	150	57573217	201	74141144	252	32775336
49	26210051	100	70770276	151	56447550	202	77321310	253	35020661
50	00375040	101	06106121	152	13444474	203	75642322	254	02217011

6.2.2 Algorithm for Nonlinear Component Construction

Nonlinear component of block cipher over Galois ring $GR\left(\mathbb{Z}_{2^3}, 8\right)$ is built by defining the following mapping from $G_{255} \cup \{0\}$ to $G_{255} \cup \{0\}$.

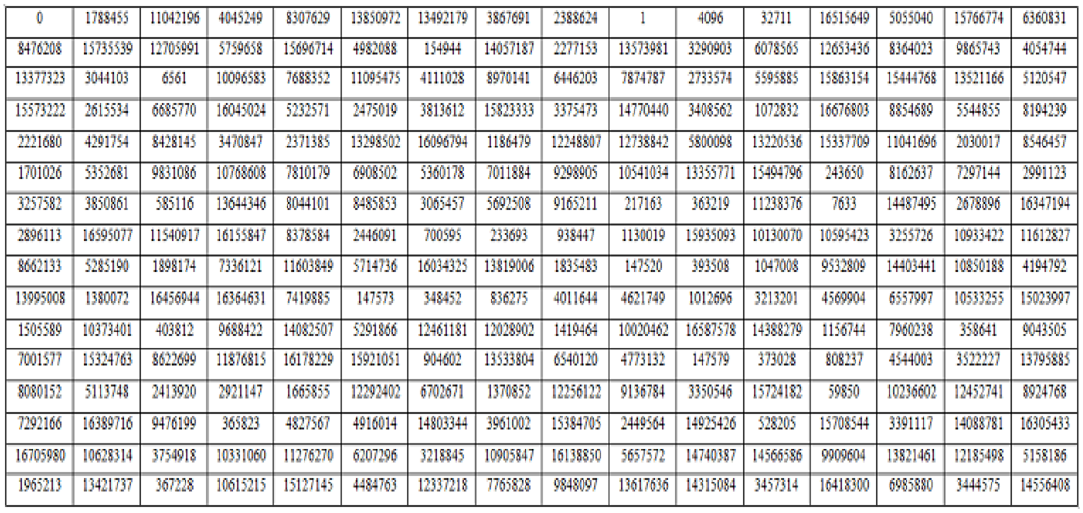
1. The invertibel transformation Inv is defined as $Inv\left(\sigma\right) = \sigma^{-1}$, $\forall\ \sigma \in G_{255}$.

2. The mutiplication map T is defined as $T\left(\sigma\right) = c\sigma$, where c is a fixed element taken from G_{255}.

3. The nonlinear component for block cipher is fabricated by using combination of invertible and scalar transformations as: $Iiv \circ T\left(\sigma\right) = \left(c\sigma\right)^{-1}$.

By selecting different scalars from G_{255}, we can construct 255 different nonlinear components of block ciphers. The S-box given in Table 6.2 is constructed by selecting one particular scalar.

Table 6.2 : S-Box based on $GR\left(\mathbb{Z}_{2^3}, 8\right)$.



0	1788455	11042196	4045249	8307629	13850972	13492179	3867691	2388624	1	4096	32711	16515649	5055040	15766774	6360831
8476208	15735539	12705991	5759658	15696714	4982088	154944	14057187	2277153	13573981	3290903	6078565	12653436	8364023	9865743	4054744
13377323	3044103	6561	10096583	7688352	11095475	4111028	8970141	6446203	7874787	2733574	5595885	15863154	15444768	13521166	5120547
15573222	2615534	6685770	16045024	5232571	2475019	3813612	15823333	3375473	14770440	3408562	1072832	16676803	8854689	5544855	8194239
2221680	4291754	8428145	3470847	2371385	13298502	16096794	1186479	12248807	12738842	5800098	13220536	15337709	11041696	2030017	8546457
1701026	5352681	9831086	10768608	7810179	6908502	5360178	7011884	9298905	10541034	13355771	15494796	243650	8162637	7297144	2991123
3257582	3850861	585116	13644346	8044101	8485853	3065457	5692508	9165211	217163	363219	11238376	7633	14487495	2678896	16347194
2896113	16595077	11540917	16155847	8378584	2446091	700595	233693	938447	1130019	15935093	10130070	10595423	3255726	10933422	11612827
8662133	5285190	1898174	7336121	11603849	5714736	16034325	13819006	1835483	147520	393508	1047008	9532809	14403441	10850188	4194792
13995008	1380072	16456944	16364631	7419885	147573	348452	836275	4011644	4621749	1012696	3213201	4569904	6557997	10533255	15023997
1505589	10373401	403812	9688422	14082507	5291866	12461181	12028902	1419464	10020462	16587578	14388279	1156744	7960238	358641	9043505
7001577	15324763	8622699	11876815	16178229	15921051	904602	13533804	6540120	4773132	147579	373028	808237	4544003	3522227	13795885
8080152	5113748	2413920	2921147	1665855	12292402	6702671	1370852	12256122	9136784	3350546	15724182	59850	10236602	12452741	8924768
7292166	16389716	9476199	365823	4827567	4916014	14803344	3961002	15384705	2449564	14925426	528205	15708544	3391117	14088781	16305433
16705980	10628314	3754918	10331060	11276270	6207296	3218845	10905847	16138850	5657572	14740387	14566586	9909604	13821461	12185498	5158186
1965213	13421737	367228	10615215	15127145	4484763	12337218	7765828	9848097	13617636	14315084	3457314	16418300	6985880	3444575	14556408

The entries of S-box are the decimal representation of elements of G_{255}, by converting these entries into binary form, we can obtain maximum 24 binary bits.

6.3 Analysis for Cryptographically Secure Nonlinear Component

It is vital to assess the performance of the proposed nonlinear component of block cipher in an effort to establish its usefulness in encryption. Several properties are listed in literature, which indicate the strength of any nonlinear component [121]. Among some of the prevailing methods used by cryptanalysis include differential analysis used for the analysis of DES [112] and information theoretic analysis with excerpts from the original concepts presented by Shannon [1]. In this work, we analyze the proposed nonlinear component for five different properties, which includes nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability and differential approximation probability. In order to determine the strength of the proposed nonlinear component, the results of these analyses are prudently analyzed. In the following subsections, we present the details of these analyses and discuss the results pertaining to the strength the S-box under analysis.

6.3.1 Nonlinearity

In the nonlinearity analysis, the constituent Boolean functions are assessed with reference to the behavior of the input/output bit patterns. The set of all affine functions is used to compare the distance from the given Boolean function. Once the initial distance is determined, the bits in the truth table of the Boolean function are modified to approximate to the closest affine function. Number of modifications required to reach the closest affine functions bears useful characteristics in determining the nonlinearity of the transformation used in encryption process. The measure of nonlinearity is bounded by [123],

$$N_g = 2^{m-1}\left(1 - 2^m \max\left|S_g(w)\right|\right). \tag{6.1}$$

The Walsh spectrum $S_g(w)$ is defined as

$$S_g(w) = \sum_{w \in \mathbf{F}_{2^m}} (-1)^{g(x) \otimes \chi . w}. \tag{6.2}$$

Table 6.3: Nonlinearity of non-balanced boolean functions.

Functions	N_g	Functions	N_g	Functions	N_g
g_0	8388586	g_8	8388578	g_{16}	8388580
g_1	8388584	g_9	8388588	g_{17}	8388586
g_2	8388586	g_{10}	8388580	g_{18}	8388582
g_3	8388580	g_{11}	8388582	g_{19}	8388586
g_4	8388580	g_{12}	8388586	g_{20}	8388580
g_5	8388588	g_{13}	8388584	g_{21}	8388586
g_6	8388586	g_{14}	8388582	g_{22}	8388580
g_7	8388582	g_{15}	8388582	g_{23}	8388588

As a rule, cryptographic Boolean capacities ought to fulfill different criteria at the same time, for the most part high nonlinearity, strict avalanche criterion and bit independent criterion. The nonlinearity of a Boolean capacity is characterized as least separation from the capacity to the relative capacities. A cryptosystem that utilizes work with a low nonlinearity is defenseless against numerous cryptanalytic assaults including the linear cryptanalysis found by Matsui (1994). Nonlinearity has been thought to be a critical criterion. Late advances in Linear cryptanalysis set forward by Matsui have made it express that nonlinearity isn't simply vital yet basic to DES like piece encryption calculations. Linear cryptanalysis abuses the low nonlinearity of nonlinear components of block ciphers utilized by a piece figure and it has been effectively connected in assaulting FEAL and DES. It has been demonstrated that to inoculate a S-box against linear cryptanalysis it accomplishment for the Hamming separation between each nonzero linear blend of the segment capacities and each new capacity not to veer off to a long way from n in particular a S box is insusceptible to linear cryptanalysis if the nonlinearity of each nonzero linear mix of its segment capacities is high.

It is notable that bent functions have the most noteworthy nonlinearity and fulfill the propagation criterion as for all non-zero vectors (Dillon, 1972). However two drawbacks of bent functions prohibit their direction application in practice. The first drawback is that they are not balanced, and the second drawback is that they exist only when the number of input coordinates is even. Our proposed S-box consist Boolean functions which are not balanced as a whole and also exist for even number of coordinates. Also our proposed S-box does not follow the existing bound on nonlinearity which is new discovery in the field of cryptographic criteria. The components of proposed S-box namely even number of Boolean functions exhibits characteristics of balancedness and bentness but these Boolean functions doesn't satisfy the nonlinearity bounds as fulfill the by bent Boolean functions. These classes of Boolean functions are more general as compared to the existing Boolean functions. The proposed S-box which is fundamentally based on the non-balanced and non-bent Boolean functions. We have proposed a new bound for nonlinearity of these non-balanced and non-bent Boolean functions. The comparison of among the different bounds are also depicted in Table 6.2.

6.3.2 Comparison with Already Exiting Results in Literature

For simplicity, we suppose

$$N_1 = 2^{n-1} - \frac{2\ln 2}{\pi} n 2^{\frac{n}{2}},\ N_2 = 2^{n-1} - \frac{\ln 2}{2} n 2^{\frac{n}{4}} - 1,\ N_3 = \max\left\{6\left\lfloor\frac{2^{n-1}}{2n}\right\rfloor - 2, 2^{n-1} - \left(\frac{\ln 2}{3}(n-1) + \frac{3}{2}\right)2^{\frac{n}{2}}\right\} \tag{6.3}$$

denote the lower bounds of the nonlinearity of the results in [125], [126], [127], respectively, where $n = 2^t m$ with $gcd(2, m) = 1$. Also the nonlinearity bound available in [128] $N_4 = 2^{n-1} - \sum_{i=0}^{t-1} 2^{\frac{n}{2^{i+1}}} - 2^{\frac{m-1}{2}}$ is much better than N_1, N_2 and N_3. More precisely, by a tedious computation, we can validate that N_4 is larger than N_1, N_2 and N_3 if $n \geq 4$. In [125], [126], and [127], some concrete values of the nonlinearity were given which are denoted by N_1, N_2 and N_3 for convenience which are much better than their bounds. The comparison table is along with our nonlinearity bounds is presented in the following table.

Table 6.4 : Comparison among the nonlinearity bounds of Boolean functions.

Construction	n *even*	N_g
Canteaut et. al., [86]	$n \geq 8$	$2^{n-1} - 2^{\frac{n}{2}}$
Stanica [129]	$n \geq 4$	2^{n-2}
Stanica [129]	$n \geq 8$	$2^{n-1} - 2^{\frac{n}{2}}$
Stanica and Sung [130]	$n \geq 8$	$2^{n-1} - 2^{\frac{n}{2}}$
Maitra [88]	$n \geq 6$	$2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\frac{n}{2}-2}$
Stanica and Sung [131]	$n \geq 4$	$2^{n-1} - 2^{\frac{n}{2}}$
Xiaohu Tang et. al., [128]	$n \geq 10$	$2^{n-1} - 2^{\frac{n}{2}-1} - 2^{\lceil \frac{n}{4} \rceil + 1}$

Table 6.5 : Comparison of the nonlinearity of balanced and nonbalanced Boolean functions (n even).

	Balanced Boolean Functions			Nonbalanced Boolean Functions	
n	$N_1 = N_3$ [125], [127]	N_2 [126]	N_4 [128]	Bent Boolean Functions	Proposed N_F
4	4	4	4	6	-
6	24	24	26	28	-
8	112	116	116	120	124
10	478	490	492	496	-
12	1970	2008	2010	2016	-
14	8036	8118	8120	8128	-
16	32530	32624	32628	32640	32748
18	130442	130792	130800	130816	-
24	-	-	-	8386560	8388588

When compared with the newly proposed Boolean function, which is recorded to have the best nonlinearity among all the known bent Boolean function constructions, our function still has better nonlinearity. This benchmark is through the mixed behavior of our proposed nonlinear components of block ciphers which is mainly at the same time depend on balanced and non-balanced Boolean functions.

6.3.3 Strict Avalanche Criterion Analytically

In strict avalanche criterion (SAC), the behavior of the output bits is analyzed that results from a change at the input bit applied to the nonlinear S-box transformation. It is desired that almost half of the output bits change their value or simply toggle their state in response to a single change at the input. The change in the output bit patterns cause a series of variations in the entire substitution-permutation network (S-P network) and thus causes an avalanche effect. The extent of these changes assists in determining the resistance to cryptanalysis and the strength of the cipher.

Table 6.6: The results of strict avalanche criterion for proposed S-box.

$$SAC = \begin{bmatrix} D_1 & D_2 \\ D_3 & D_4 \\ D_5 & D_6 \\ D_7 & D_8 \end{bmatrix},$$

where

$$D_1 = \left\{ \begin{array}{cccccc} 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \\ 0.5391 & 0.5078 & 0.5156 & 0.5000 & 0.4688 & 0.5000 \end{array} \right\}$$

$$D_2 = \left\{ \begin{array}{cccccc}
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391 \\
0.5000 & 0.5313 & 0.4609 & 0.5234 & 0.4688 & 0.5391
\end{array} \right\}$$

$$D_3 = \left\{ \begin{array}{cccccc}
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547 \\
0.5000 & 0.4688 & 0.5156 & 0.5000 & 0.5234 & 0.5547
\end{array} \right\}$$

$$D_4 = \left\{ \begin{matrix} 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \\ 0.5000 & 0.4531 & 0.5469 & 0.5000 & 0.4922 & 0.5391 \end{matrix} \right\}$$

$$D_5 = \left\{ \begin{matrix} 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4766 \\ 0.5000 & 0.4688 & 0.4922 & 0.5000 & 0.4531 & 0.4609 \end{matrix} \right\}$$

$$D_6 = \left\{ \begin{array}{cccccc}
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688 \\
0.5000 & 0.4453 & 0.4609 & 0.5078 & 0.5000 & 0.4688
\end{array} \right\}$$

$$D_7 = \left\{ \begin{array}{cccccc}
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609 \\
0.5156 & 0.4922 & 0.4922 & 0.5000 & 0.4688 & 0.4609
\end{array} \right\}$$

$$D_8 = \left\{ \begin{array}{cccccc} 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \\ 0.5000 & 0.4453 & 0.5469 & 0.5156 & 0.5156 & 0.4688 \end{array} \right\}.$$

Table 6.7: Comparison of SAC analysis of proposed nonlinear components of block ciphers with chaotic non

nonlinear components of block ciphers	SAC values
Proposed S-box	0.4999
Wang[117]	0.4850
Chen[115]	0.4999
Tang[119]	0.4993
Jakimoski[120]	0.4972

Table 6.8: Comparison of SAC analysis of proposed nonlinear components of block ciphers with some well k

nonlinear components of block ciphers	Min	Max	Avg
Proposed S-box	0.445300	0.539100	0.499
AES	0.453125	0.562500	0.504
APA	0.437500	0.562500	0.437
Gray	0.437500	0.562500	0.499

6.3.4 Bit Independent Criterion

The Bit Independence Criterion (BIC) also relies on the changes at the input bits and the properties exhibited by the independence behavior of pair-wise input/output variables of avalanche vectors [123]. This criterion is analyzed by modifying single input bit from the plaintext.

Table 6.9: Comparison of nonlinearity and SAC of BIC of proposed S-box.

	SAC of BIC		
nonlinear components of block ciphers	Min	Max	Avg.
Proposed	0.487400	0.509200	0.500000
AES	0.480469	0.525391	0.504604
APA	0.472656	0.515625	0.499651
Gray	0.478516	0.515625	0.502581

6.4 Results and Discussions

The comparison of the strong encryption capabilities show that the performance of the proposed S-box is comparable or superior to some prevailing nonlinear components of block ciphers used in the area of cryptography. The nonlinearity analysis depicts that the properties are comparable to the nonlinear components of block ciphers use as a benchmark in this work. The comparison of nonlinearity bounds is listed in table 6.4. The results for each nonlinearity bounds are given in table 6.5. The through investigations of table 6.5, clearly justify the claim of being highly nonlinear Boolean functions are obtained that have yet not been devised in literature which is in fact a central point of the proposed construction technique. The result of SAC is very close 0.5, which assures the acceptability of this S-box to encryption applications. The results are shown in table 6.6. We have also drawn a comparison of SAC among the chaotic and some well known nonlinear components of block ciphers (see table 6.7, 6.8). Our suggested S-box satisfy the SAC and quite comparable with the SAC of already existing nonlinear components of block ciphers. In table 6.9, a comparison of BIC is presented between the proposed S-box and AES, APA, Gray, Prime nonlinear components of block ciphers. The results are in agreement with the desired range. In these tests, it is observed that the performance of the proposed S-box is comparable to the existing well known nonlinear components of block ciphers used as benchmarks in this chapter.

6.5 Conclusion

In this chapter, we mainly provides a novel construction technique for nonlinear component of block cipher namely S-box which is based on maximal cyclic subgroup of Galois ring. Additionally, we have studied the three cryptographic properties of Boolean functions including nonlinearity, SAC and BIC. An innovative technique has been displayed to build nonlinear components of block ciphers that comprise of Boolean functions whose nonlinearity is much higher than accomplished by any beforehand known development. Also comparison with already existing results in literature have been drawn in order to verify the significance of suggested construction scheme. This opens up a conceivable new parkway for advance research that is to develop the outcomes do that they consider other cryptographic components, for example, linear structures, algebraic degree, global avalanche characteristics (GAC), autocorrelation, algebraic immunity, correlation immunity, transparency order, linear and differential approximation probabilities of proposed nonlinear components of block ciphers in order to resist against the linear and differential attacks.

Chapter 7

A Novel Video Encryption Technique and its Statistical Analyses

Security is turning into a heightening worry in an undeniably mixed media characterized world. The current rise of installed interactive media applications, for example, versatile TV, video informing, and telemedicine have expanded the effect of mixed media and its security on our own lives. For instance, a huge increment in the utilization of disseminated video reconnaissance innovation to screen movement and open spots has raised concerns with respect to the protection and security of the focused on subjects. Mixed media content encryption has pulled in an ever-increasing number of scientists and architects attributable to the testing idea of the issue and its interdisciplinary nature in light of difficulties looked with the prerequisites of sight and sound interchanges, mixed media recovery, mixed media pressure, and equipment asset utilization. With the proceeding with improvement of system interchanges (wired and remote), effectively catching recordings and fast advances in Internet innovation and installed figuring frameworks sight and sound information (pictures, recordings, sounds, and so on.) are of significance for utilizing increasingly generally, in applications, for example, video-on-request, video conferencing, broadcasting, and so forth. Presently, it is firmly identified with numerous parts of day by day life, including training, trade, safeguard, diversion, and legislative issues.

With a specific end goal to keep up protection or security, touchy information should be shielded from transmission or dispersion. The progressions in a universal system condition and fast advancements in distributed computing have advanced the quick conveyance of computerized mixed media information to the clients.

Clients are anxious to not just appreciate the accommodation of constant video gushing likewise shares different media data in a fairly modest manner without consciousness of conceivably abusing copyrights. In perspective of these, encryption and watermarking advancements have been perceived as a supportive method for managing the copyright insurance issue in the previous decade. Encryption permits secure end-end correspondence of information while advanced watermarking permitting still faces some trying troubles for viable utilizations; there are no different methods that are prepared to substitute it. Inside the flag preparing and interactive media groups, numerous plans have been proposed for ensuring touchy data while enabling certain genuine activities to be performed. These plans normally do not have a thorough model of security, and their insurance ends up faulty when scaled to huge datasets. The cryptography group has since quite a while ago created thorough protection models and provably secure techniques for information controls. Be that as it may, these systems are essentially intended for non-specific information. Accordingly, they ordinarily prompt an explode in computational expenses and overheads when connected to genuine interactive media applications.

Multimedia data security is getting to be plainly vital with the consistent increment of advanced correspondences on web. With the fast improvement of different mixed media advancements, more interactive media information are created and transmitted in the restorative, business, and military fields, which may incorporate some touchy data which ought not be gotten to by or must be halfway presented to the general clients. The encryption schemes created to secure information which are not reasonable for mixed media application as a result of the huge information size and continuous limitation. In this way, there is an incredible interest for secured information stockpiling and transmission systems. Data security has customarily been guaranteed with information encryption and verification procedures. The introduced work goes for secure video transmission utilizing arbitrariness in encryption designs in view of standard substitution boxes (nonlinear components of block ciphers), accordingly making more disarray to get the first information. For the determination of best S-box for specific video encryption, we have proposed another choice factual foundation. The security of the first figure has been improved by expansion of polluting influences to mislead the cryptanalyst. The proposed work discovers its application in therapeutic imaging frameworks, military picture database correspondence and classified video conferencing, and comparative such application.

7.1 Introduction

With the quick development of interactive media innovation numerous armed forces over the world are utilizing recordings to prepare recently enlisted troops. Such touchy information must be ensured either in transmission or capacity. One conceivable approach to secure interactive media data is to stop unapproved get to. In any case, this approach can't ensure that the mixed media data is physically secure. Another simple approach is to scramble the entire piece stream with a cryptographic calculation, for example, DES or AES. However recordings for the most part have a lot of information and require constant operations. Additionally, on account of the remote portable frameworks, there is restricted preparing force, memory and data transfer capacity, and is seldom ready to deal with the overwhelming encryption handling load. Along these lines, thinking about the particular attributes for asset constrained frameworks, new video encryption calculations should be produced. For certifiable applications, a video encryption calculation needs to consider different parameters like security, computational proficiency, pressure effectiveness et cetera. Distinctive kinds of video applications require diverse levels of security. For instance, for Video on Demand, low security will be fine, though for military purposes or money related data, abnormal state of security is required to totally counteract unapproved get to.

Computational effectiveness implies that the encryption or decoding procedure ought not cause excessively time delay, with the goal that the necessities of ongoing applications are met. Video compression is utilized to lessen the storage room and spare transmission capacity, with the goal that the encryption procedure ought to have minimal effect on the compression proficiency. All things considered, a very much planned video encryption algorithm ought to give adequate security, high computational efficiency impose little effect on the compression effectiveness.

The wide utilization of advanced pictures and recordings in different applications conveys genuine thoughtfulness regarding security and protection issues today. Information encryption is an appropriate strategy to secure information. Till now, different encryption techniques have been proposed and broadly utilized (DES, RSA, IDEA, AES and so on.), a large portion of which are utilized for content and binary data. It is hard to utilize them specifically in video encryption as video information is regularly of extensive volumes and require constant operations. In reasonable applications, for a video encryption technique, security, time productivity, arrange consistence and compression benevolence are extremely essential. Among them, security is the essential prerequisite, which implies that the cost of breaking the encryption algorithm is no littler than the ones purchasing the video's approval. The aim of proposed work is three fold, firstly we design a new algorithm to create huge numbers of nonlinear components of block ciphers, and secondly we developed a novel video encryption technique along with statistical analyses and thirdly suggested a new criterion on the basis of statistical analyses for the selection of best S-box. The analyses are second order texture characteristics which are based on GLCM (Gray level co-occurrence matrices).

7.2 Requirement of Video Encryption

The encryption of multimedia data is important due to the following reasons:

i. For averting undesirable review of transmitted video, for instance from law requirement video reconnaissance being transferred back to a focal survey focus.

ii. To secure the private interactive media messages that is traded over the remote or wired systems.

iii. Video encryption is useful in securing recordings utilized as a part of administrations like video on request (VOD) and video conferencing learning.

iv. For ensuring medicinal recordings which may contain private data of a patient from unapproved access by malignant clients.

This study is based on video encryption based on study of S-box transformation algorithm which is useful in protecting various medical videos that contain private information of patients and requires sharing among various doctors that belongs to different department of hospital. In first part of study I have focused on various prevailing algorithms used for video encryption.

This examination depends on video encryption in view of investigation of S-boxtransformation algorithm which is valuable in ensuring different medicinal recordings that contain private data of patients and requires sharing among different specialists that has a place with various division of doctor's facility. In initial segment of study, we have concentrated on different prevailing algorithms utilized for video encryption.

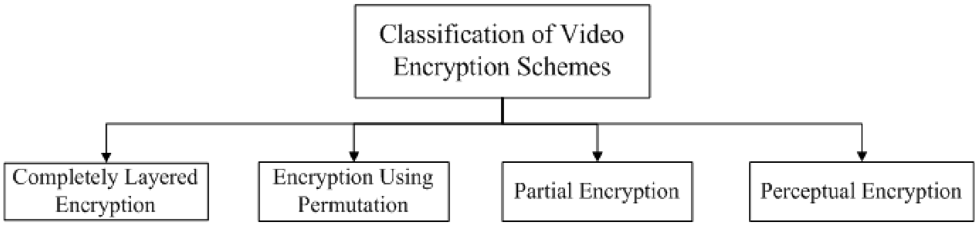

Classification of Video Encryption Schemes
Completely Layered Encryption
Encryption Using Permutation
Partial Encryption
Perceptual Encryption

Fig. 7.1: Classification of video encryption techniques.

7.3 Production of New Nonlinear Components of Block Ciphers

In this correspondence, we have displayed a procedure to orchestrate versatile nonlinear components for the development of substitution box for video encryption that use a multiplicative group of nonzero components of Galois field of order 256 alongside symmetry group S_8. The proposed nonlinear part helps with changing the comprehensible message or plaintext into an enciphered organize by the utilization of exponential map.

7.3.1 Exponential Map

Different types of maps are right now used in cryptography which includes chaotic and non-chaotic maps. A cryptographically sound maps play an important role in the encryption of digital medium. These maps not only create confusion but also diffusion in cryptosystems. In part of chapter is mainly reserve for the development of mathematical expression for exponential map over a finite field of order 256. Let $h : M \to M$ defined as:

$$x \mapsto \begin{cases} h^x \ \text{mod} \ 257 & if \ x < 256, \\ 0 & if \ \ x = 256, \end{cases} \tag{7.1}$$

where $x = h^x \pmod{257}$ and $x \in M = \{0, 1, 2, ..., 255\}$. We select h as a primitive element which generates the multiplicative group of nonzero elements of Galois field of order 256

7.3.2 Mathematical Expression of the Suggested Nonlinear Component

In this section, we are mainly discussed the algebra of proposed S-box. The following are main steps in constructing proposed nonlinear components of block ciphers:

i. First of all select unit elements of finite field $\mathbb{Z}^*_{257}$; with one extra condition that 256 is mapped to 0.

ii. The inverse function $G(x)$ in $\mathbb{Z}^*_{257}$ corresponding to multiplicative unit step is given below:

$$G(x) = \begin{cases} x^{-1} & if \ x < 256, \\ 0 & if \ x = 256. \end{cases} \tag{7.2}$$

The unit element x is equals to x to the power 255 which is can be represented by the expression, $x^{-1} = x^{2^s - 1} = x^{255}$ for $x \neq 0 \in \mathbb{Z}^*_{257}$. Therefore inverse function $G(x)$ becomes

$$G(x) = x^{255}.$$

iii. Let $L_A(x)$ be a linear transformation in $\mathbf{F}_{2^8}$ which can be expressed as follows:

$$y = L_A(x), \tag{7.3}$$

where

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix}, \tag{7.4}$$

iv. We define the nonlinear affine transformation function $K(x)$ in $\mathbf{F}_{2^8}$:

$$K(x) = x \oplus d.$$

The suggested nonlinear component of block cipher is therfore, a combination of three functions namely power function $G(x)$, the linear transformation $L_A(x)$ and the affine transformation $K(x)$:

$$S - box = K \circ L_A \circ G = K(L_A(G)) = L_A(x^{-1}) \oplus d, \tag{7.5}$$

where

$$L_A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}, \ d = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}. \tag{7.6}$$

We now applying action of symmetry group S_8 on Eq. (7.6) to get 40320 new nonlinear components of block ciphers. The mathematical expression for these nonlinear components of block ciphers is given as follows:

$$S_8(S-box) = S_8(K \circ L_A \circ G) = S_8(K(L_A(G)) = S_8(L_A(x^{-1}) \oplus d).$$

One of the proposed S-box is presented in Table 7.1.

Table 7.1: The proposed S-box.

45	103	53	167	51	151	180	155	212	154	204	90	206	106	77	102
226	9	72	62	239	113	133	36	31	248	185	195	18	144	124	221
147	148	156	220	218	202	74	78	110	109	101	37	39	55	183	179
190	235	81	134	44	95	245	169	67	22	176	123	213	162	11	88
69	38	47	119	181	163	19	152	188	219	210	138	76	94	238	105
21	168	59	215	178	139	84	158	236	89	198	42	79	118	173	99
174	107	85	166	43	87	182	171	83	150	172	91	214	170	75	85
120	189	227	17	136	60	223	242	137	68	60	240	121	197	34	15
3	24	192	251	209	130	12	96	254	233	65	6	48	124	245	161
135	52	159	244	153	196	23	208	122	205	98	13	104	61	231	49
164	27	216	186	203	82	142	108	93	230	41	71	54	175	115	149
184	187	211	146	140	92	222	234	73	70	46	111	117	165	35	23
56	191	243	145	132	28	224	250	201	66	14	112	125	229	33	7
207	114	141	100	29	232	57	199	50	143	116	157	228	25	200	58
63	247	177	131	20	160	252	217	194	10	80	126	237	97	5	40
8	64	255	241	129	4	32	0	249	193	2	16	128	253	225	1

7.4 Proposed Video Encryption Algorithm

Various video encryption techniques are proposed to encrypt the videos and used for obtaining highly encrypted videos. Our scheme mainly focuses on the full encryption techniques. The following figures (see Figs. 7.2-7.3) represent the proposed video encryption and decryption algorithm includes following stages:

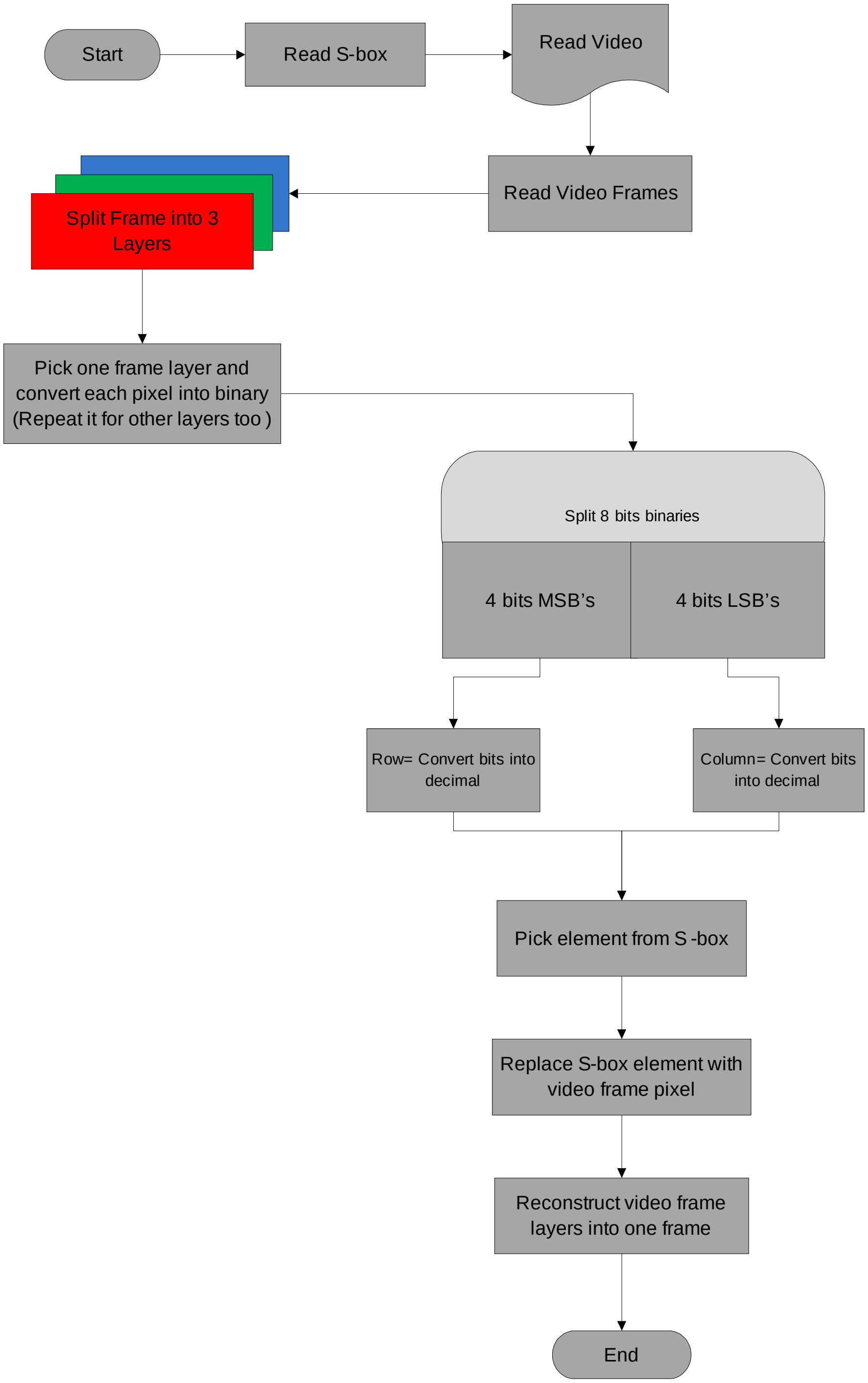

Start
Read S-box
Read Video
Read Video Frames
Split Frame into 3 Layers
Pick one frame layer and convert each pixel into binary (Repeat it for other layers too)
Split 8 bits binaries
4 bits MSB's
4 bits LSB's
Row= Convert bits into decimal
Column= Convert bits into decimal
Pick element from S -box
Replace S-box element with video frame pixel
Reconstruct video frame layers into one frame
End

Fig. 7.2: Video encryption algorithm.

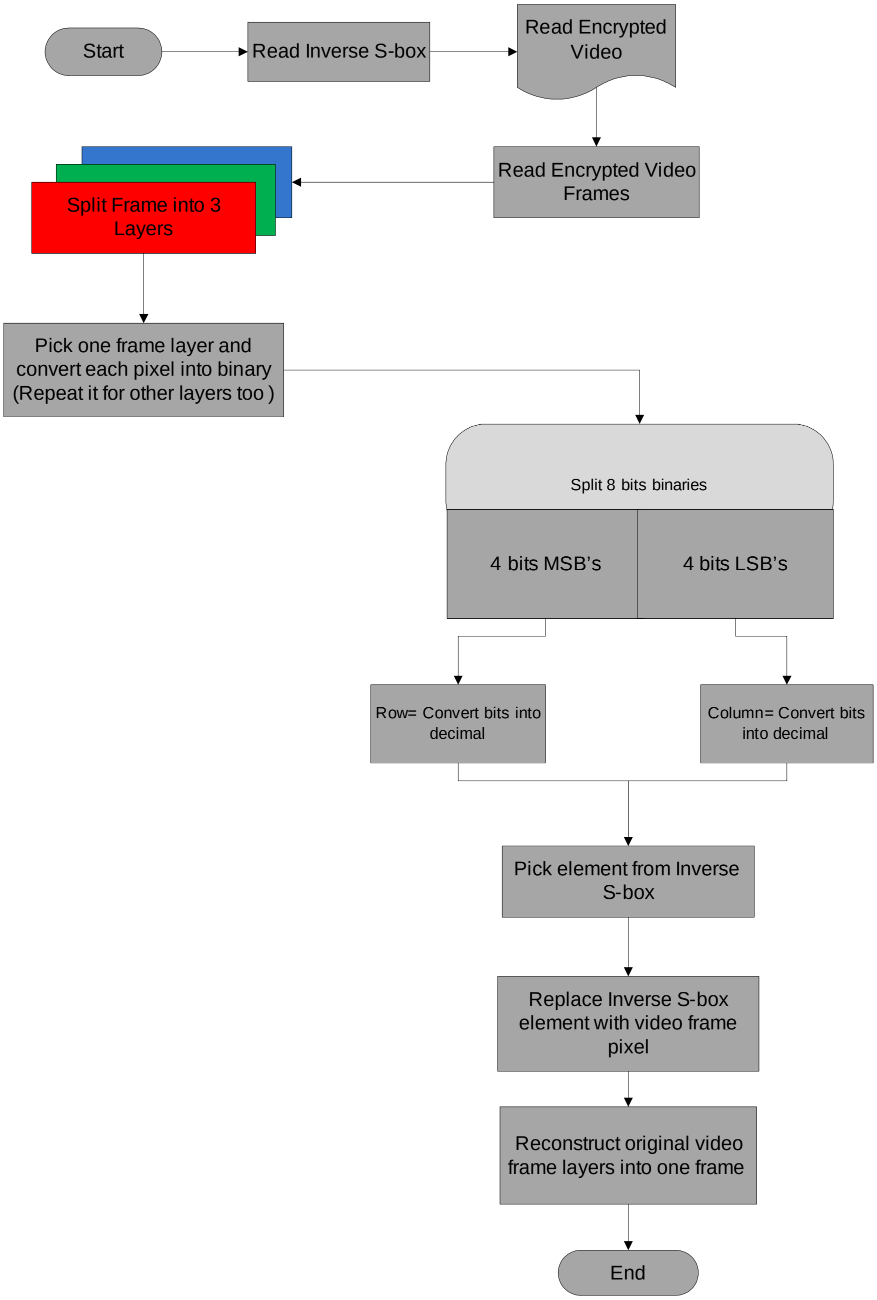

Start
Read Inverse S-box
Read Encrypted Video
Read Encrypted Video Frames
Split Frame into 3 Layers
Pick one frame layer and convert each pixel into binary (Repeat it for other layers too)
Split 8 bits binaries
4 bits MSB's
4 bits LSB's
Row= Convert bits into decimal
Column= Convert bits into decimal
Pick element from Inverse S-box
Replace Inverse S-box element with video frame pixel
Reconstruct original video frame layers into one frame
End

Fig. 7.3: Video decryption algorithm.

7.5 Performance Parameters

A decent encryption method ought to be vigorous against a wide range of cryptanalytic, algebraic, statistical and other well-known security attacks. We have to characterize an arrangement of parameters in light of which we can assess and compare video encryption algorithms. A few parameters recorded underneath are accumulated from writing. Here we examine the security examination of the proposed video encryption plans in view of statistical investigation, for example, correlation, contrast, homogeneity, energy and entropy and so on. In statistical texture examination, texture highlights are computed from the statistical conveyance of observed combinations of intensities at determined positions with respect to each other in the picture. According to the number of intensity points (pixels) in every combination, measurements are characterized into first-arrange, second-arrange and higher-arrange insights. The Gray Level Co-occurrence Matrix (GLCM) strategy is a method for extricating second order statistical texture features. The approach has been utilized as a part of various applications. There are number of measurable strategies used to arrange the data security (encryption, watermarking and steganography) procedures in sight and sound applications.

The five basic textures highlights talked about here are contrast, correlation, energy, homogeneity, and entropy. Contrast is utilized to gauge the nearby varieties, relationship is utilized to quantify likelihood of event for a couple of particular pixels, energy is otherwise called consistency of ASM (angular second moment) which is the whole of squared components from the GLCM, homogeneity is to quantify the dissemination of components in the GLCM as for the corner to corner, and entropy measures the factual arbitrariness. The five regular surfaces highlights are given underneath:

$$Entropy = -\sum_i\sum_j p(x_i, x_j) \ \log_b \ p(x_i, x_j), \tag{7.7}$$

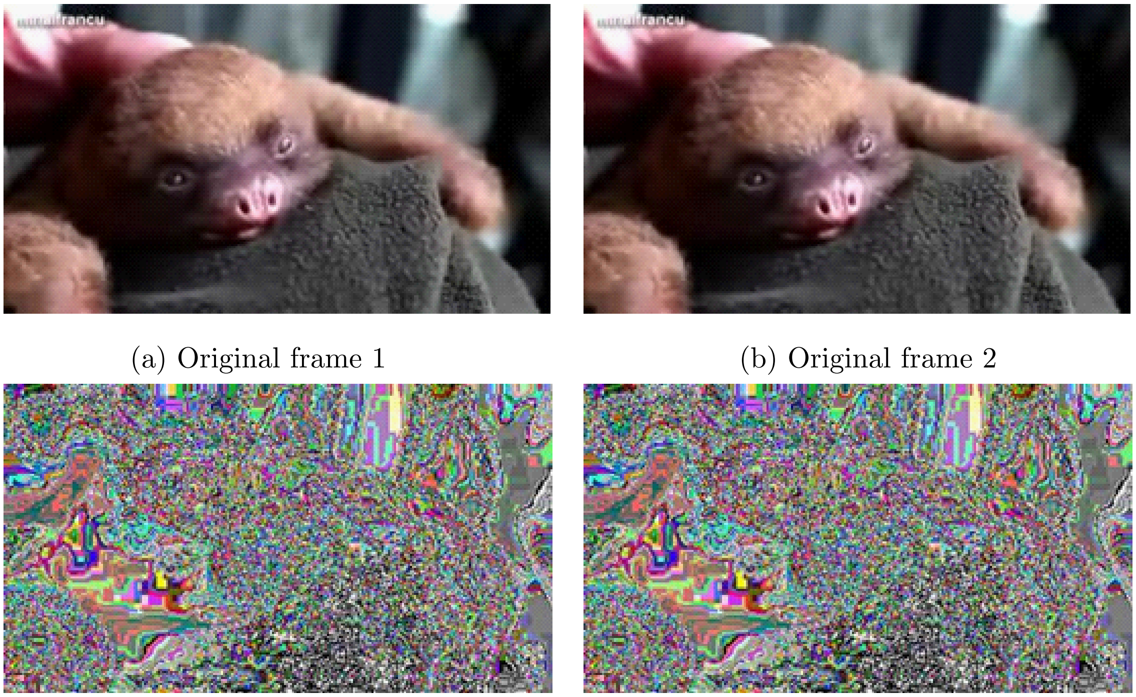
$$Contrast = \sum_i\sum_j |i-j|^2 \ p(i,j), \tag{7.8}$$

$$Homogenity = \sum_i\sum_j \frac{p(i,j)}{1+|i-j|}, \tag{7.9}$$

$$Energy = \sum_{i,j} p(i,j)^2, \tag{7.10}$$

$$Correlation = \sum_i\sum_j \frac{(i-\mu_i)(j-\mu_j)}{\sigma_i\sigma_j} p(i,j), \tag{7.11}$$

where i and j are two different gray levels of the image, p is the number of the co-appearance of gray levels i and j, μ_i, μ_j , are mean of i and j levels of image (a frame of video), σ_i and σ_j are the standard deviations at i and j levels of an image. Entropy is utilized to gauge the substance of a picture with higher esteem demonstrating a picture with wealthier subtle elements. Contrast restores a measure of the power distinction between a pixel and its neighbor over the entire picture. Homogeneity measures the comparability of dim scale levels over the picture. Hence, bigger the adjustments in the dark scale, the higher the GLCM Contrast and lower the homogeneity. GLCM energy measures the general likelihood of having particular dark scale designs in picture. Relationship restores a measure of how associated a pixel is to its neighbor over the entire picture and it gauges the joint likelihood of event of the predefined pixel sets. The exhibitions of these nonlinear components of block ciphers transformation and rely upon the idea of information and their applications. The inquiry emerges how one can verify that one S-box is superior to other? To answer this inquiry, we have examined encourage measurable examinations which are able to answer the above inquiries. We take just two casings from unique video and encode these edges with most famous nonlinear parts of square figure which incorporates Advanced encryption standard (AES), Affine-power-affine (APA), Gray, Lui J, Residue prime, S8 AES, SKIPJACK, Xyi nonlinear components of block ciphers. We use the second order texture analyses on the encrypted frames of given video. The aftereffects of these investigations are additionally analyzed to decide the propriety of an S-box to video encryption applications



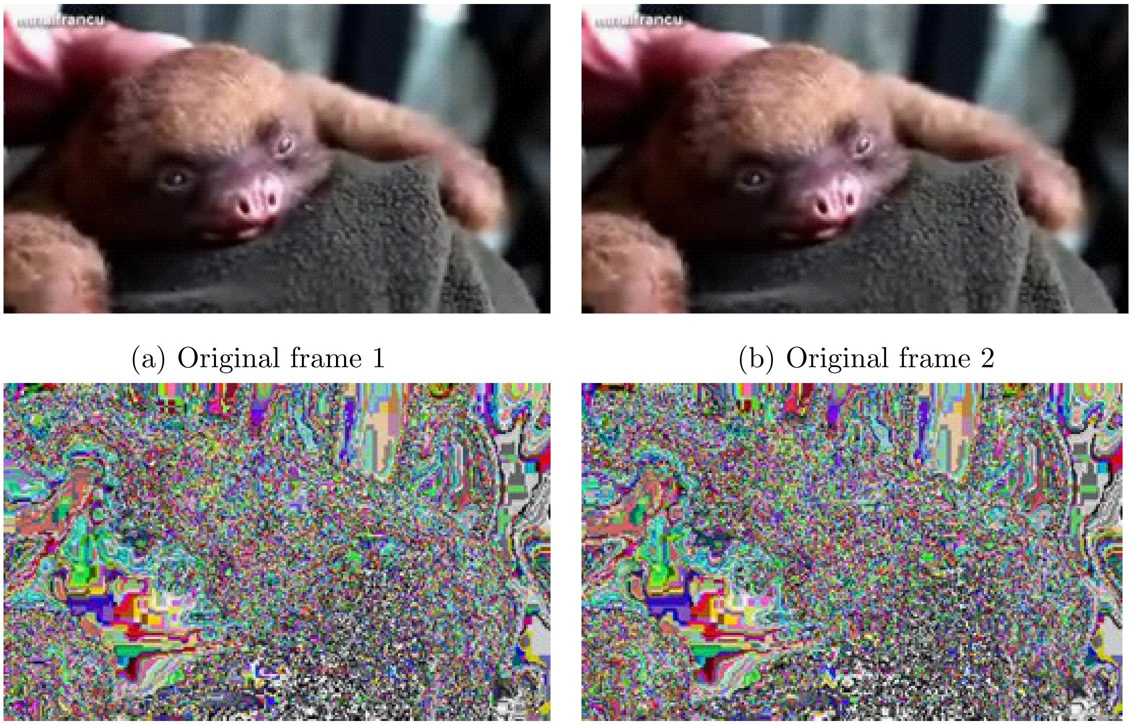
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.4: Encryption of video file through AES S-box.



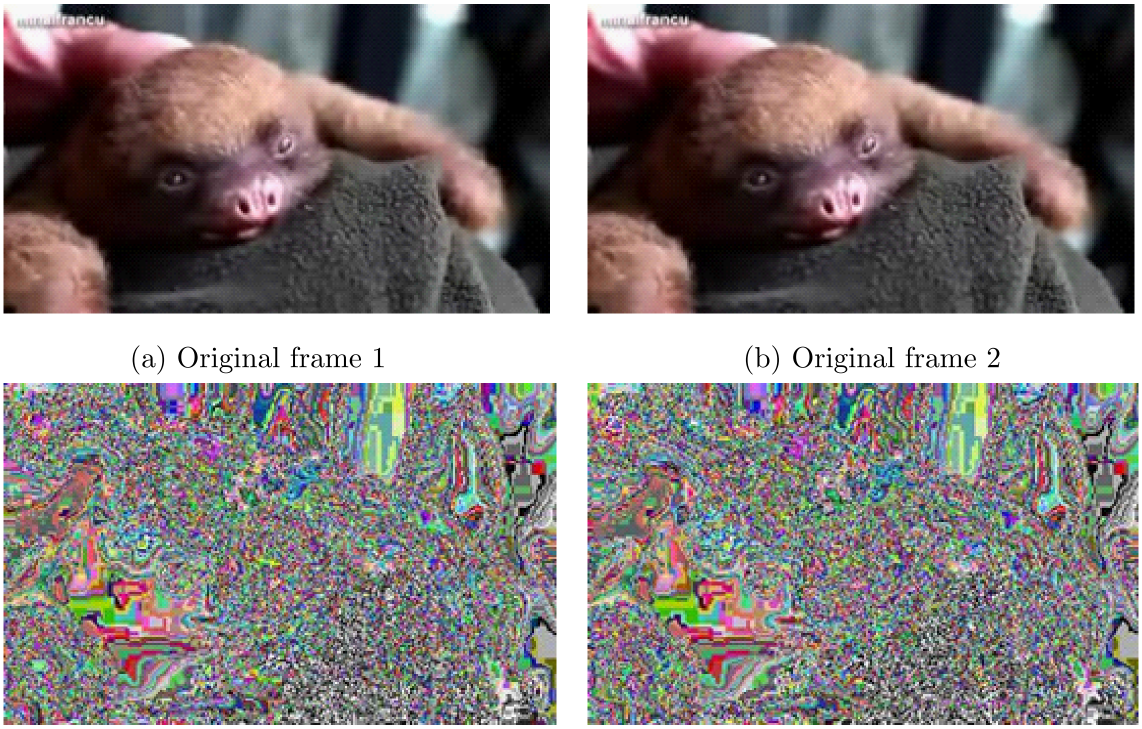
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.5: Encryption of video file through APA S-box.



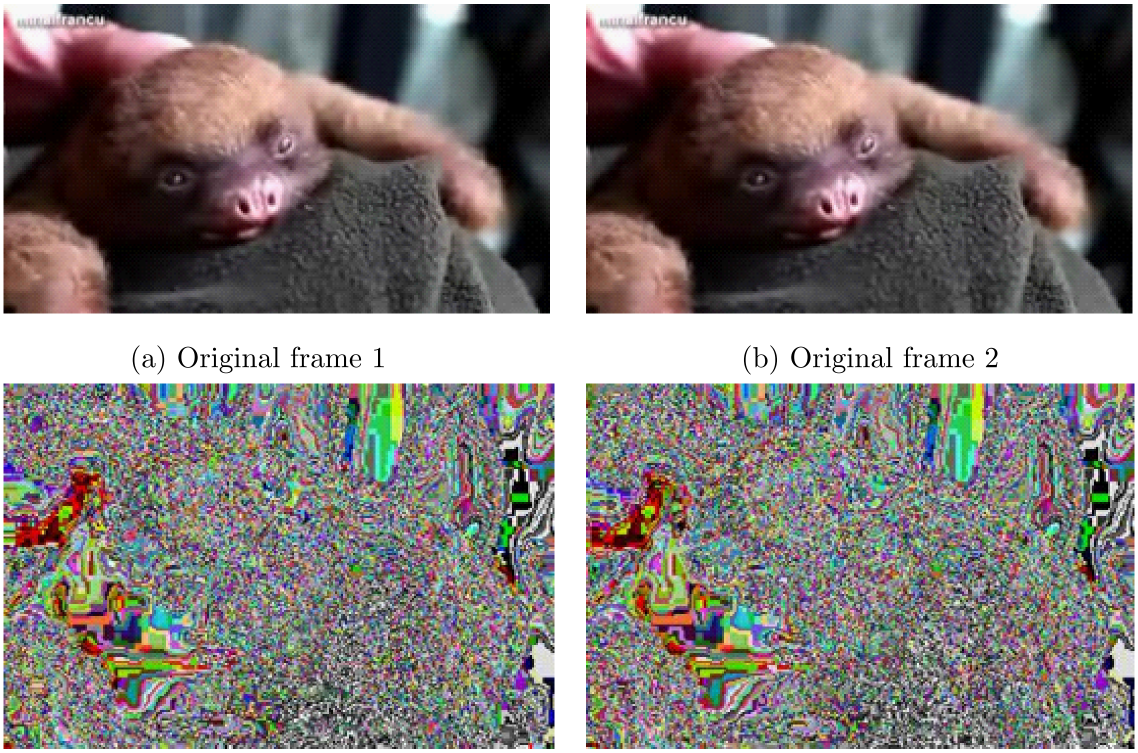
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.6: Encryption of video file through Gray S-box.



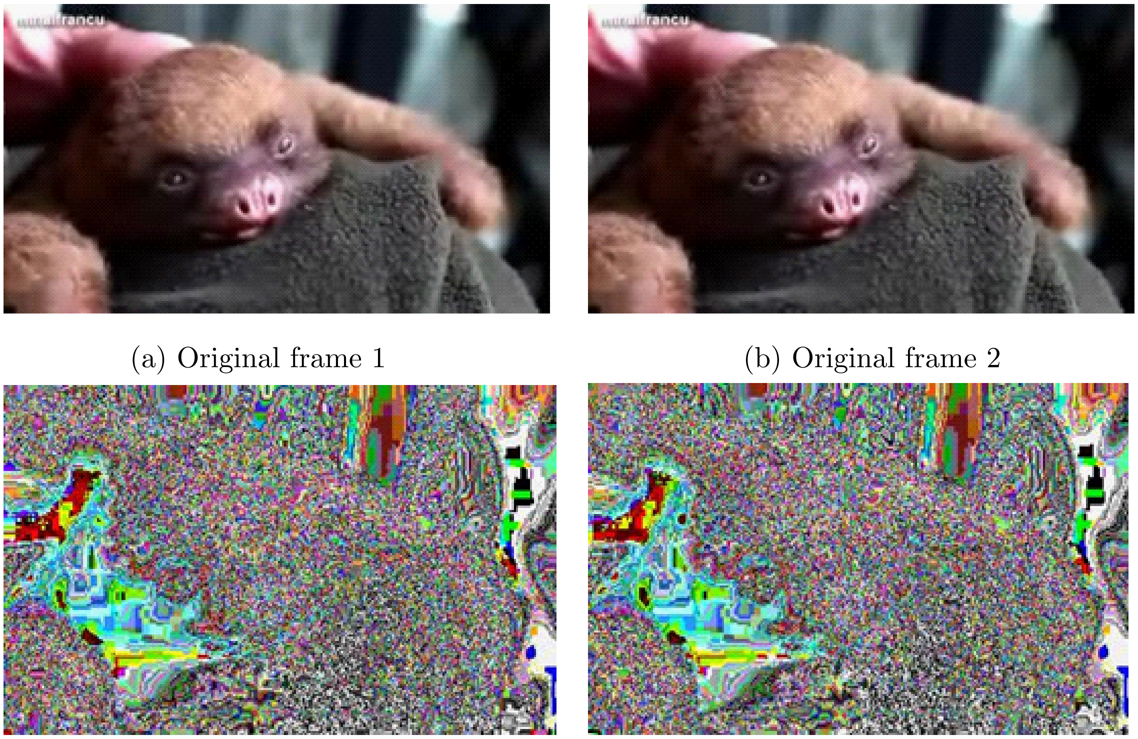
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.7: Encryption of video file through Lui S-box.



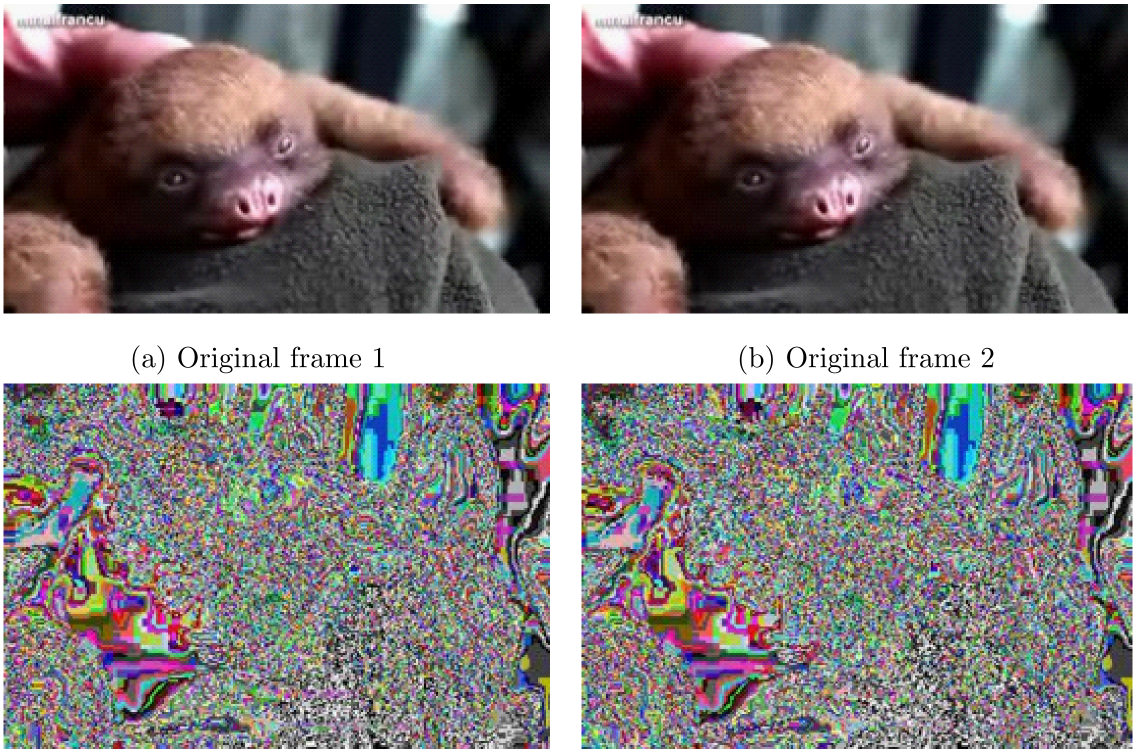
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.8: Encryption of video file through Prime S-box.



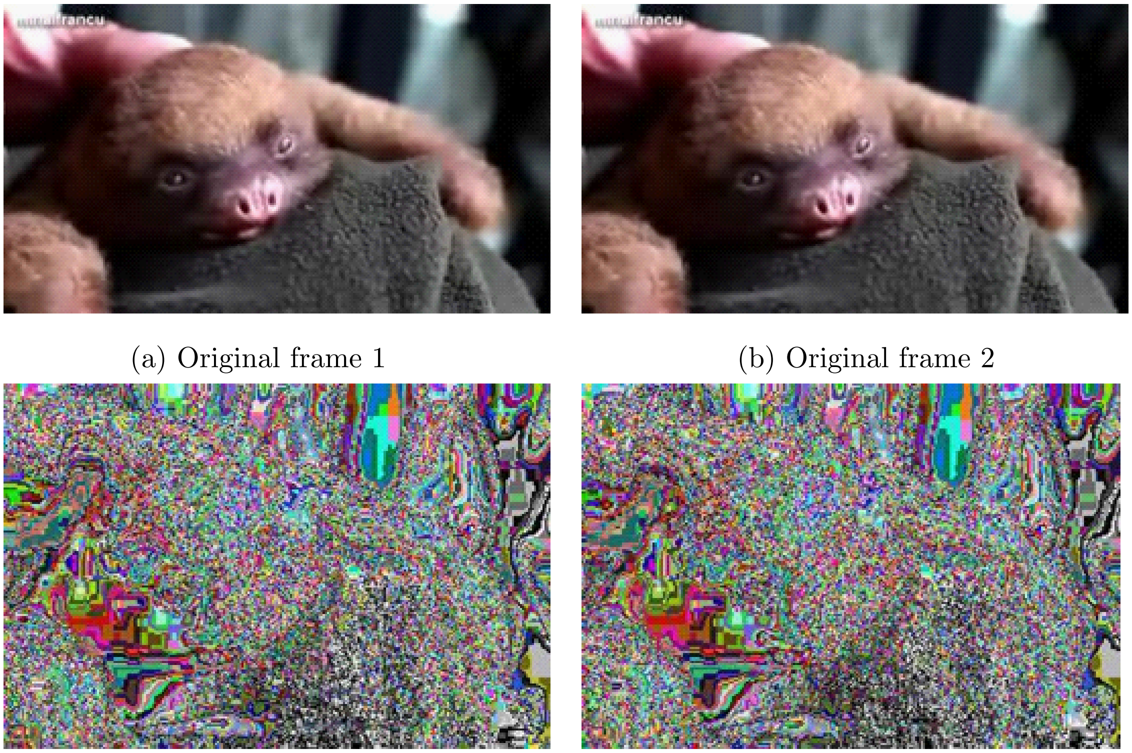
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.9: Encryption of video file through S8-AES S-box.



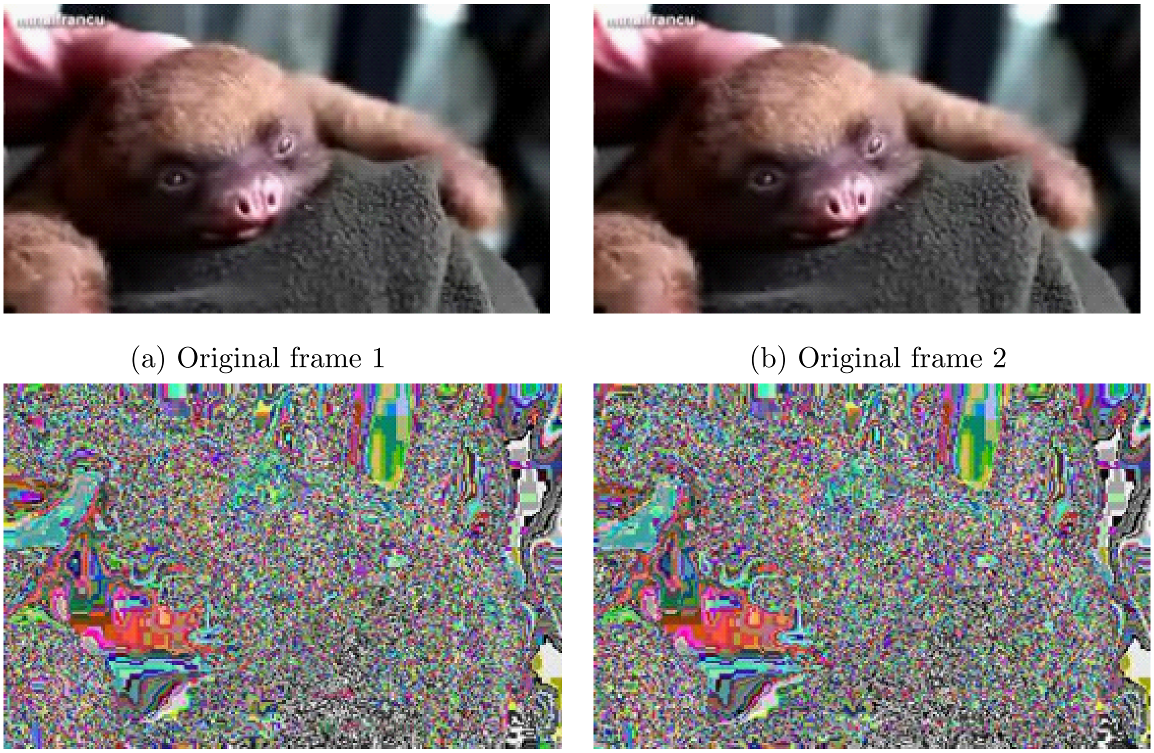
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.10: Encryption of video file through Xyi S-box.



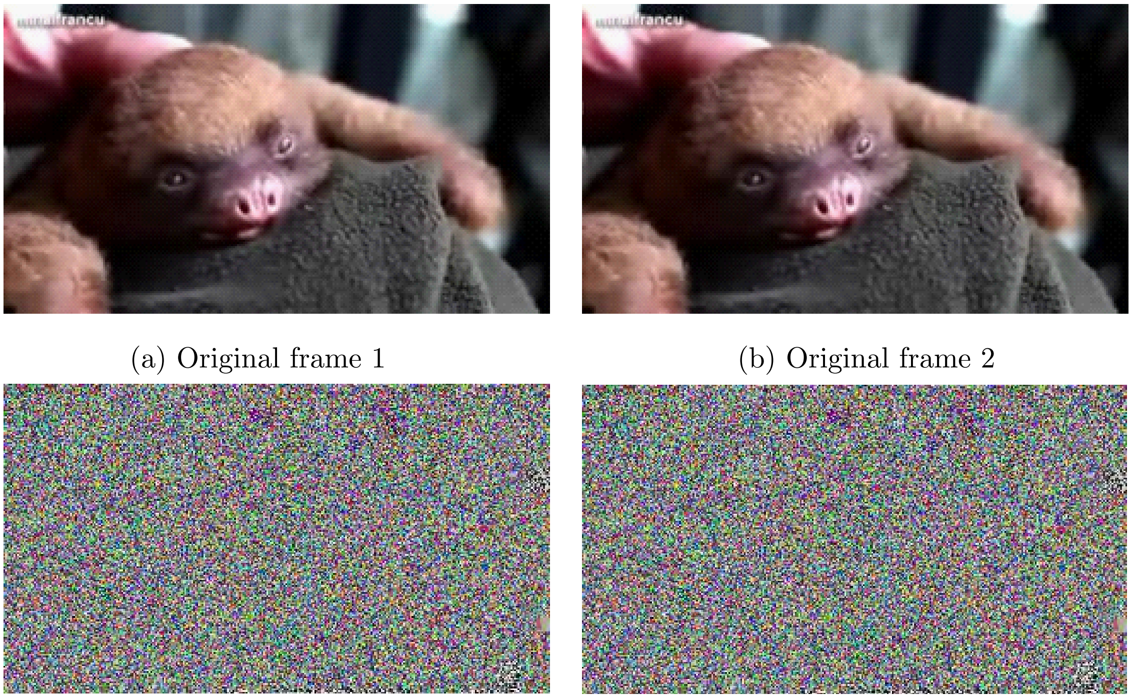
(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.11: Encryption of video file through Skipjack S-box.



(a) Original frame 1

(b) Original frame 2

(c) Encrypted frame 1

(d) Encrypted frame 2

Fig. 7.12: Encryption of video file through proposed S-box.

7.5.1 Statistical Analyses Based Best S-box Selection Algorithm

Here, we are giving a best selection criteria in the list of nonlinear components of block ciphers for video encryption techniques. This criteria fundamentally based on testing number of given nonlinear components of block ciphers for video encryption applications.

Algorithm 42 *Let us consider n nonlinear components of block ciphers say $S_1, S_2, ..., S_n$. We can say that S-box S_i is optimal with respect to statistical analyses than S_j for $j \in \{1, 2, ..., n\}\backslash\{ i\}$ if the following conditions holds:*

i. If the Contrast and Entropy of S_i is greater than S_j for $j \in \{1, 2, ..., n\}\backslash \{i\}$,

ii. If Correlation, Energy and Homogeneity of S_i is less than S_j for $j \in \{1, 2, ..., n\}\backslash \{i\}$.

Table 7.2: Statistical analyses for a gray scale image.

Statistical	Original	Encryption of first frame with nonlinear components of block ciphers							
Properties	frame	*AES*	*APA*	*Gray*	*Lui*	*Prime*	S_8-*AES*	*Skipjaik*	Proposed
Contrast	0.1688	4.8011	4.6630	4.4605	4.5877	4.6841	4.5957	4.5750	4.1867
Homogenity	0.9285	0.4343	0.5307	0.5358	0.5300	0.5289	0.5297	0.5299	0.5395
Entropy	7.6315	7.9282	7.8361	7.7846	7.8140	7.8573	7.8312	7.8062	7.7454
Correlation	0.9759	0.0833	0.2299	0.1770	0.2135	0.2648	0.2229	0.1778	0.1761
Energy	0.1445	0.0158	0.0269	0.0303	0.0279	0.0258	0.0274	0.0291	0.03185

Table 7.3: Statistical analyses for AES S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.814660	4.856900	4.867450
Homogenity	0.927243	0.928763	0.927245	0.437077	0.417827	0.396663
Entropy	7.785210	7.495870	7.487560	7.961220	7.927490	7.940200
Correlation	0.981038	0.973687	0.972199	0.173149	0.115769	0.098270
Energy	0.123563	0.153702	0.150333	0.018441	0.021502	0.017411

Table 7.4: Statistical analyses for APA S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.64397	4.76191	4.56811
Homogenity	0.927243	0.928763	0.927245	0.525618	0.528458	0.524481
Entropy	7.785210	7.495870	7.487560	7.82943	7.85796	7.80127
Correlation	0.981038	0.973687	0.972199	0.305289	0.327557	0.290148
Energy	0.123563	0.153702	0.150333	0.0248075	0.0237682	0.0257022

Table 7.5: Statistical analyses for Gray S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.46005	4.56879	4.44538
Homogenity	0.927243	0.928763	0.927245	0.528096	0.531388	0.527558
Entropy	7.785210	7.495870	7.487560	7.78134	7.80279	7.75448
Correlation	0.981038	0.973687	0.972199	0.274416	0.276426	0.2440
Energy	0.123563	0.153702	0.150333	0.0269791	0.0262526	0.0281263

Table 7.6: Statistical analyses for Lui S-box for color frame image

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.6073	4.70589	4.53046
Homogenity	0.927243	0.928763	0.927245	0.523077	0.526427	0.523965
Entropy	7.785210	7.495870	7.487560	7.80182	7.83796	7.78305
Correlation	0.981038	0.973687	0.972199	0.274219	0.312519	0.302507
Energy	0.123563	0.153702	0.150333	0.0256633	0.0241991	0.0254364

Table 7.7: Statistical analyses for Prime S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	0.46772	4.79047	4.56216
Homogenity	0.927243	0.928763	0.927245	0.522392	0.52806	0.524674
Entropy	7.785210	7.495870	7.487560	7.8282	7.89079	7.83554
Correlation	0.981038	0.973687	0.972199	0.310132	0.370774	0.371136
Energy	0.123563	0.153702	0.150333	0.0248877	0.0228422	0.0235903

Table 7.8: Statistical analyses for S_8-AES S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.56799	4.72119	4.552
Homogenity	0.927243	0.928763	0.927245	0.524465	0.524465	0.523927
Entropy	7.785210	7.495870	7.487560	7.82253	7.84331	7.80726
Correlation	0.981038	0.973687	0.972199	0.31173	0.325783	0.304344
Energy	0.123563	0.153702	0.150333	0.024802	0.0239544	0.025042

Table 7.9: Statistical analyses for Skipjack S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.5651	4.67912	4.54009
Homogenity	0.927243	0.928763	0.927245	0.523372	0.525459	0.522016
Entropy	7.785210	7.495870	7.487560	7.8045	7.8144	7.78273
Correlation	0.981038	0.973687	0.972199	0.285098	0.279685	0.262988
Energy	0.123563	0.153702	0.150333	0.0256217	0.0251742	0.0263711

Table 7.10: Statistical analyses for Xyi S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.45472	4.57534	4.42644
Homogenity	0.927243	0.928763	0.927245	0.524562	0.52732	0.522999
Entropy	7.785210	7.495870	7.487560	7.81467	7.85229	7.80984
Correlation	0.981038	0.973687	0.972199	0.323574	0.344926	0.335634
Energy	0.123563	0.153702	0.150333	0.0250035	0.0237999	0.0247389

Table 7.11: Statistical analyses for proposed S-box for color frame image.

Statistical properties	Color components of original frame			Color components of encrypted frame		
	Red	*Green*	*Blue*	*Red*	*Green*	*Blue*
Contrast	0.168844	0.168391	0.171648	4.83686	4.871580	4.866630
Homogenity	0.927243	0.928763	0.927245	0.53130	0.535748	0.531762
Entropy	7.785210	7.495870	7.487560	7.84411	7.854680	7.782900
Correlation	0.981038	0.973687	0.972199	0.25098	0.262701	0.273437
Energy	0.123563	0.153702	0.150333	0.02879	0.028085	0.028427

The proposed criteria is justify for AES nonlinear components of block ciphers as it is quite evident from the tabulated values of contrast, homogeneity, correlation, energy and entropy of an encrypted frame through AES nonlinear components of block ciphers (see Tables 7.2-7.11). Applying the proposed algorithm for the selection of best S-box among eight, we have the following results:

a. Contrast and entropy encrypted frames through proposed algorithm and AES S-box is higher than other nonlinear components of block ciphers.

b. Correlation, homogeneity and energy of encrypted frames through suggested and AES nonlinear components of block cipher are less than the other existing nonlinear components of block ciphers.

The investigations talked about in this exchange for video encryption applications in conjunction with the proposed novel criteria to pick the best S-box, additionally encourages the client in deciding the ideal S-box for video encryption (see Tables 7.2-7.11). While the proposed standard in this work relates to video encryption applications, this rule and investigations can be adjusted for other imperative encryption applications, for example, voice, video conferencing and watermarking. The investigation of the proposed foundation for various encryption applications is the subject of enthusiasm for future work.

7.6 Conclusion

In this chapter, we have developed a new algorithm for video encryption that is based on substitution boxes. We have encrypted a video file (number of frames) through well-known nonlinear components of block ciphers, i-e., AES, APA, Gray, Prime, S_8-AES, Skipjack, Xyi and Lui. Also we have verified the strength of all encrypted frames through our proposed statistical criteria which is based on second order texture features of an image developed by Haralick et. al., [67]. Such an analyses and technique is yet not available in existing literature.

Chapter 8

Cryptosystems and Key Exchange Alforithms Based on Commutaitve Subgroups of $GL_2(\mathbb{Z}_{p^n})$, $GL_2(\mathbb{Z}_{p^n})$ and $GL_2(GF(p^n))$

Security is the most essential perspective in the field of web and system application. It is a vital errand to secure data over the system. To secure data, cryptography can be utilized. Cryptography can be separated into two sections that are "symmetric key cryptography" and "asymmetric key cryptography. In this part, we will primarily talk about public key cryptography.

The idea of "public key cryptography" (PKC) was presented by Whitfield Diffie and Martin Hellman in 1976 [132]. After that numerous executions of it have been proposed, and a significant number of these cryptographic applications construct their security with respect to the unmanageability of hard scientific issues, to be specific the limited field discrete logarithm problem (DLP) [139] and integer factorization problem (IFP) [133]−[138]. To take care of these issues, sub-exponential time schemes have been produced throughout the years. Subsequently, key sizes developed to in excess of 1000 bits, in order to accomplish a sensible level of security. In the conditions where transfer speed, registering force and capacity are constrained, doing thousand-piece tasks turns into a doubtful approach for giving adequate security. This is most obvious close by held gadgets, for example, the cell phones, PDAs, and pagers that have the extremely constrained preparing force and battery life.

The idea of PKC advanced from an endeavor to assault two of the most troublesome issue related with symmetric encryption. The principal issue is that of key circulation under symmetric encryption requires either: (1) that two communicants as of now share a key, which has been conveyed some way or another to them; or (2) the utilization of key dispersion focus. The general public key cryptography process is portrayed in first chapter with the definition; it is clear that public key techniques depend on one key for encryption and an alternate yet numerically related key for unscrambling. These schemes have the accompanying critical attributes.

Because of quick advancements in points of confinement and conceivable outcomes of interchanges and data transmissions, there is a developing interest of cryptographic methods, which has prodded a lot of escalated examine exercises in the investigation of cryptography. A speculation of the discrete logarithms design schemes of secure information communication is the elliptic curve (EC) algorithms. Different new techniques were developed in literature by using EC along with already existing techniques for symmetric and asymmetric key cryptography, like EC-Diffie algorithm, EC-RSA, EC-Elgamal and EC-digital signatures schemes [140]−[141]. Note that every one of the three families can be utilized to give the fundamental public key systems of the key foundation, nonrepudiation through computerized marks and encryption information. In this chapter, we have developed a novel public-key cryptosystem that uses large commutative subgroup of general linear group of units of local ring of degree 2. Moreover this chapter, depicts a key trade calculation that depends on Chebyshev polynomials. The primary extent of this chapter is to supplant the monomial with the Chebyshev polynomials $T_n(x)$, $U_n(x)$ and supplant lattices in the contentions of Chebyshev polynomial in the Diffie-Hellman (DH) algorithms. As we know that Chebyshev polynomials fulfill the semi-group characteristic on the set of real field R, they additionally have semi-group stuff over the set of integers $\mathbb{Z}$. At that point, we can additionally expand the prescribed definition over finite field and also define Chebyshev polynomials of first and second kinds denoted by $T_n(x)$ and $U_n(x)$ over a finite field $\mathbb{Z}_p$. Different properties of chebyshev polynomails were defined in therein references [150]−[154].

8.1 Commutative Subgroup of $GL_2(\mathbb{Z}_{p^n})$

Let $H_2(\mathbb{Z}_{p^n})$ be the subgroup of $GL_2(\mathbb{Z}_{p^n})$, which is given as follows:

$$H_2(\mathbb{Z}_{p^n}) = \left\{ \left(\begin{array}{cc} a_1 & b_1 \\ b_1 & a_1 \end{array} \right) \middle| \; a_1, b_1 \in \mathbb{Z}_{p^n} \text{ and } a_1^2 - b_1^2 \neq 0 \right\}, \tag{8.1}$$

which shows that elements of subgroup $H_2(\mathbb{Z}_{p^n})$ are belong to unit group of residue ring $\mathbb{Z}_{p^n}$ that is $\mathbb{Z}_{p^n}^*$. The subgroup $H_2(\mathbb{Z}_{p^n})$ is an abelian subgroup $GL_2(\mathbb{Z}_{p^n})$.

8.2 Cryptosystems Established on Commutative Subgroups of $GL_2(\mathbb{Z}_{p^n})$

In this section, we are mainly discussed definition of cryptosystem, correspondence between messages and rings; and proposed cryptosystem one which are based subgroup of $GL_2(\mathbb{Z}_{p^n})$ defined in section 2. We will discussed and explain in detail about the about the key generation, encryption and decryption algorithms of our proposed novel schemes.

Definition 43 *A cryptosystem consists of quintuplet (A, R, γ, E, D), where an alphabet A that contains all characters that can be used in messages, commutative ring R, one-one and onto transformations $\gamma : A \rightarrow R$, $E : P \rightarrow C$ and $D : C \rightarrow E$.*

The main concepts which will be utilized in this chapter is that we define a correspondence α between element of alphabets set A and ring R that maps original message to the elements in R. The second step is to apply encryption function E that maps plaintext to cipher text C. We will apply the reverse procedure in order to recover the plaintext.

In this chapter, we will use the following mapping which maps alphabets to a ring. We suppose that all messages are written in the alphabet $A = \{A_1, A_2, A_3, A_4\}$. We will take $R = \mathbb{Z}_4$ and let $\gamma_1 : A_1 \rightarrow R$ be given by $\gamma_1(A) = 0, \gamma_1(B) = 1, \gamma_1(C) = 3$ and $\gamma_1(D) = 4$. For reference,we list the correspondence for γ_1 below [149]:

Table 8.1: List of correspondence for γ_1.

A_1	A	B	C	D
$\mathbb{Z}_4$	0	1	2	3

Now we will take $R = \mathbb{Z}_8$ and let $\gamma_2 : A_2 \to R$ be given by $\gamma_2(A) = 0, \gamma_2(B) = 1, \gamma_2(C) = 2, ..., \gamma_2(H) = 7$. For reference,we list the correspondence for γ_2 below:

Table 8.2: List of correspondence for γ_2.

L_2	A	B	C	D	E	F	G	H
$\mathbb{Z}_8$	0	1	2	3	4	5	6	7

Similarly for other rings, we have list the correspondence for γ_3 and γ_4 given as follows:

Table 8.3: List of correspondence for γ_3.

L_3	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
$\mathbb{Z}_{16}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Table 8.4: List of correspondence for γ_4.

L_4	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
$\mathbb{Z}_{32}$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
L_4	Q	R	S	T	U	V	W	X	Y	Z	$-$	!	#	.	&	*
$\mathbb{Z}_{32}$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

where $-$ represent blank space.

Galois Field (3^2)

Suppose $f(x) = x^2 + 2x + 2$ be irreducible and primitive polynomial for GF(3^2). Let α be the root of this polynomial then $f(\alpha) = 0$, *i.e.*,

$$\alpha^2 + 2\alpha + 2 = 0$$

$$\alpha^2 = -2\alpha - 2$$

$$\alpha^2 = -2\alpha - 2 + 3\alpha + 3 \qquad \therefore 3 \bmod 3 = 0$$

$$\alpha^2 = \alpha + 1,$$

and

$$\text{Since } \alpha^{p^n - 1} = 1, \Rightarrow \alpha^{3^2 - 1} = \alpha^8 = 1$$

$$\begin{aligned} \alpha^3 &= 2\alpha + 1, \\ \alpha^4 &= 2, \\ \alpha^5 &= 2\alpha, \\ \alpha^6 &= 2\alpha + 2, \\ \alpha^7 &= \alpha + 2, \\ \alpha^8 &= 1. \end{aligned}$$

$$\begin{aligned} Gf(3^2) &= \left\{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7\right\}, \\ &= \{0, 1, \alpha, \alpha + 1, 2\alpha + 1, 2, 2\alpha, 2\alpha + 2, \alpha + 2\}. \end{aligned}$$

Galois Field (3^3)

Suppose $f(x) = x^3 + 2x^2 + 1$ be irreducible and primitive polynomial for GF(3^3).

Let α be the root of this polynomial therefore

$$\alpha^3 + 2\alpha^2 + 1 = 0$$

$$\begin{aligned}\alpha^3 &= -2\alpha^2 - 1,\\ &= -2\alpha^2 - 1 + 3\alpha + 3,\\ &= \alpha^2 + 2,\end{aligned}$$

$\therefore 3 \bmod 3 = 0$

and $\alpha^{p^n-1} = 1$

$\Rightarrow \alpha^{3^3-1} = \alpha^{26} = 1$

$$\alpha^3 = \alpha^2 + 2,$$

$$\begin{aligned}\alpha^4 &= \alpha^2 + 2\alpha + 2,\\ \alpha^5 &= 2\alpha + 2,\\ \alpha^6 &= 2\alpha^2 + 2\alpha,\\ \alpha^7 &= \alpha^2 + 1,\\ \alpha^8 &= \alpha^2 + \alpha + 2,\\ \alpha^9 &= 2\alpha^2 + 2\alpha + 2,\\ \alpha^{10} &= \alpha^2 + 2\alpha + 1,\\ &\vdots\\ \alpha^{26} &= 1.\end{aligned}$$

$$\begin{aligned}Gf(3^3) &= \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}, \alpha^{12}, \alpha^{13},\\ &\quad \alpha^{14}, \alpha^{15}, \alpha^{16}, \alpha^{17}, \alpha^{18}, \alpha^{19}, \alpha^{20}, \alpha^{21}, \alpha^{22}, \alpha^{23}, \alpha^{24}, \alpha^{25}\},\end{aligned}$$

$$\begin{aligned}Gf(3^3) &= \{0, 1, \alpha, \alpha^2, \alpha^2 + 2, \alpha^2 + 2\alpha + 2, 2\alpha + 2, 2\alpha^2 + 2, \alpha^2 + 1, \alpha^2 + \alpha + 2,\\ &\quad 2\alpha^2 + 2\alpha + 2, \alpha^2 + 2\alpha + 1, \alpha + 2, 2\alpha + \alpha^2, 2, 2\alpha, 2\alpha^2, 2\alpha^2 + 1, 2\alpha^2 + \alpha + 1,\\ &\quad \alpha + 1, \alpha^2 + \alpha, 2\alpha^2 + 2, 2\alpha^2 + 2\alpha + 1, \alpha^2 + \alpha + 1, 2\alpha^2 + \alpha + 2, 1 + 2\alpha, 2\alpha^2 + \alpha\}.\end{aligned}$$

8.3 Projected Data Security System Established on Commutative Subgroups

8.3.1 Cryptosystem I

Process of Key Generation

Since in public key cryptography, the owner of public and private keys are receiver, therefore, at receiving end, user apply the steps given below in order to generate a keys:

1. Choose a prime number p and computes $i = p^n$ with $n \geq 2$

2. Choose a matrix arbitrary $A \in GL_2(\mathbb{Z}_{p^n})$

3. Calculate the following matrices:

$$B = A^2,\ D = A^3,\ B^2D \ \text{ and } BD^2. \tag{8.2}$$

4. Choose a matrix $F \in GL_2(\mathbb{Z}_{p^n})$. We now define the automorphism

$$\Theta \ : \ W \rightarrow (B^2D)^{-1}W(B^2D), \tag{8.3}$$

$$\Omega \ : \ W \rightarrow (BD^2)^{-1}W(BD^2), \tag{8.4}$$

$\forall\ W \in M_2(\mathbb{Z}_{p^n})$. The automorphisms Θ and Ω commute with each other.

5. Calcuate the following matrices:

$$BD\ , \Theta(F), \quad \Omega(F^{-1}). \tag{8.5}$$

6. Receiver public keys are:

$$\left(n, BD\ , \Theta(F), \quad \Omega(F^{-1})\right), \tag{8.6}$$

and receiver private keys are:

$$(B, D). \tag{8.7}$$

Process of Encryption

At the sending end, sender will do the following tasks:

1. We can represents the original messgae P as a array of 2×2 matrices over residue ring $\mathbb{Z}_{p^n}$:

$$P^{(1)}, P^{(2)}, P^{(3)}, ..., P^{(k)}. \tag{8.8}$$

2. Choose a arbitrary integer k_i computes matrix:

$$Y^{(i)} = (BD)^{k_i}. \tag{8.9}$$

$\forall\ P^{(i)}\ (i = 1, 2, ..., k)$.

3. The automorphisms for $\forall\ i = 1, 2, ..., k$ are given below:

$$\Im^{(i)} : W \to (Y^{(i)})^{-1} W (Y^{(i)}), \tag{8.10}$$

$\forall\ W \in GL_2(\mathbb{Z}_{p^n})$.

4. Computes $\forall\ i = 1, 2, ..., k$ matrices $\Im^{(i)}(\Theta(N))$, $\Im^{(i)}(\Omega(N^{-1}))$ and $m^{(i)}\Im^{(i)}(\Omega(N))$.

5. Choose $\forall\ i = 1, 2, ..., k$ a arbitrary invertible elements $\mu \in Z_n^*$ and find the ciphertext:

$$\begin{aligned} C &= \left(C^{(1)}, C^{(2)}, ..., C^{(k)}\right), & C^{(i)} &= (C_1^{(i)}, C_2^{(i)}), & (8.11)\\ C_1^{(i)} &= \lambda_i^{-1}\Im^{(i)}(\Omega(F^{-1})), & C_2^{(i)} &= \lambda_i P^{(i)} \Im^{(i)}(\Theta(F)),\ i = 1, 2, ..., k. & (8.12)\end{aligned}$$

Process of Decryption

At the receiving end, receiver will perform the following steps in order to deciphering enciphered message:

1. Computes $\forall\ i = 1, 2, ..., k$ using the private key:

$$d^{(i)} = \chi^{-1}\delta(C_1^{(i)}) = \chi^{-1}\delta(\lambda_i^{-1}\Im^{(i)}(\Omega(F^{-1}))). \tag{8.13}$$

2. Computes $\forall\ i = 1, 2, ..., k$ matrices:

$$P^{(i)} = C_2^{(i)} d^{(i)}. \tag{8.14}$$

3. In a final step, receiver can easily get back the original message i.e., plaintext P, as a string of sequences $P^{(1)}, P^{(2)}, P^{(3)}, ..., P^{(i)}$.

8.3.2 Cryptosystem II

Process of Key Generation

The process of key is generation is given below which will be peformed at receivers end:

1. Choose a arbitrary prime number p

2. Consider the general linear group $GL_n(\mathbb{Z}_p) = \{A \in M_n(\mathbb{Z}_p) | \det(A) \neq 0\}$ and take $H \subset GL_n(\mathbb{Z}_p)$

3. Choose matrices $A, B \in GL_n(\mathbb{Z}_p)$

$$A = \begin{bmatrix} x_1 & y_1 \\ y_1 & x_1 \end{bmatrix}, B = \begin{bmatrix} x_2 & y_2 \\ y_2 & x_2 \end{bmatrix}.$$

where $x_1, x_2, y_1, y_2 \in \mathbb{Z}_p$.

4. Now check $A,\ B \in H$, if not then repeat step and choose those matrices which belong to H

5. Choose two polynomials of the form

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0, \\ g(y) &= b_n y^n + b_{n-1} y^{n-1} + ... + b_1 y + b_0. \end{aligned}$$

where $a_i, b_i \in \mathbb{Z}_p\ \forall\ 0 \leq i \leq n$.

6. Find $f(A),\ g(B)$ such that $\det(f(A)) \neq 0,\ \ \det(g(B)) \neq 0$

7. Define two commutative automorphisms of $GL_n(\mathbb{Z}_p)$

$$\eta : K \to (f(A))^{-1}K(f(A)),\ \xi : K \to (g(B))^{-1}K(g(B))$$

for $A, B \in GL_n(\mathbb{Z}_p)$. As the matrices A and B belongs to H therefore the automorphisms η and ξ.

8. Now define the following automorphisms of $GL_n(\mathbb{Z}_p)$

$$\alpha : K \to (f(A)^2 g(B))^{-1}K(f(A)^2 g(B)),$$

$$\beta : K \to (f(A)g(B)^2)^{-1}K(f(A)g(B)^2),$$

such that

$$\alpha = \eta^2\xi,\ \beta = \eta\xi^2.$$

The automorphisms α and β comutes therefore,

$$\alpha = \eta\xi^{-1}\beta,\ \beta = \eta^{-1}\xi\alpha$$

9. Choose an arbitrary matrix $D \in GL_n(\mathbb{Z}_p)$ such that $D \notin H$

10. Find the following matrices $D^{-1},\ \alpha(D),\ \beta(D^{-1})$

11. Public key for encryption is

$$(p, \alpha(D),\ \beta(D^{-1})),$$

and private key for decryption is

$$(f(A), g(B)).$$

Process of Encryption

For encryption following steps are performed

1. Consider the matrices of plaintext be

$$m_{(1)}, m_{(2)}, m_{(3)}, ...m_{(k)} \in GL_n(\mathbb{Z}_p).$$

2. For every plaintext matrix $m_{(i)}$ $(0 \leq i \leq k)$, choose a random matrix $N_{(i)} \in H$

3. Define automorphism for every $0 \leq i \leq k$

$$\zeta_{(i)} : D \rightarrow (N_{(i)})^{-1} D(N_{(i)}).$$

for every $D \in GL_n(\mathbb{Z}_p)$.

4. For every $0 \leq i \leq k$ compute the following matrices

$$\zeta_{(i)}(\beta(D^{-1})),\ \zeta_{(i)}(\alpha(D)), m_{(i)}\zeta_{(i)}(\alpha(D)).$$

5. Select a random unit $\lambda \in \mathbb{Z}_p$ and calucate the ciphertext

$$C = (C_{(1)}, C_{(2)}, ..., C_{(k)}),\ C_{(i)} = (C_{1(i)},\ C_{2(i)}),$$

$$C_{1(i)} = \lambda_i^{-1}\zeta_{(i)}(\beta(D^{-1})),\ C_{2(i)} = m_{(i)}\zeta_{(i)}(\alpha(D)),\ \ 0 \leq i \leq k\ .$$

Process of Decryption

Now follow the given steps below to decipher the encrypted messaage:

1. By using the private key for $0 \leq i \leq k$ comupte

$$d_{(i)} = \alpha^{-1}\beta(C_{1(i)}) = \alpha^{-1}\beta(\lambda^{-1}\zeta_{(i)}(\beta(D^{-1}))).$$

2. Calculate the following matrices for $0 \leq i \leq k$

$$m_{(i)} = C_{2(i)}d_{(i)} = (\lambda_i m_{(i)}\zeta_{(i)}(\alpha(D)))d_{(i)}.$$

3. Finally, deciphered message matrices are

$$m_{(1)},\ m_{(2)},\ m_{(3)}, ..., m_{(k)}.$$

8.3.3 Cryptosystem III

Process of Key Generation

1. Consider a Galois field of order p^n, i.e. $GF(p^n)$

2. Choose two elements $A,\ B \in GF(p^n)$

3. Now choose an arbitrary element $K \in GF(p^n)$

4. Define the following automorphisms of $GF(p^n)$

$$\alpha : K \rightarrow (A^2B)^{-1}K(A^2B),$$

$$\beta : K \rightarrow (AB^2)^{-1}K(AB^2),$$

such that

$$\alpha = \eta^2\xi,\ \beta = \eta\xi^2.$$

The automorphisms α and β comutes therefore,

$$\alpha = \eta\xi^{-1}\beta,\ \beta = \eta^{-1}\xi\alpha.$$

5. Choose an arbitrary elements $D \in GF(p^n)$

6. Find the following elements $D^{-1},\ \alpha(D),\ \beta(D^{-1})$

7. Public key for encryption is

$$(p, \alpha(D),\ \beta(D^{-1})),$$

and private key for decryption is

$$(A, B).$$

Process of Encryption

For encryption following steps are performed

1. Consider the plaintext be

$$m_{(1)}, m_{(2)}, m_{(3)}, ...m_{(k)} \in GF(p^n).$$

2. For every plaintext $m_{(i)}$ $(0 \leq i \leq k)$, choose a random element $N_{(i)} \in GF(p^n)$

3. Define automorphism for every $0 \leq i \leq k$

$$\zeta_{(i)} : D \to (N_{(i)})^{-1}D(N_{(i)}).$$

for every $D \in GF(p^n)$.

4. For every $0 \leq i \leq k$ compute the following elements

$$\zeta_{(i)}(\beta(D^{-1})),\ \zeta_{(i)}(\alpha(D)).$$

5. Select a random unit $\lambda \in GF(p^n)$ and calucate the ciphertext

$$C = (C_{(1)}, C_{(2)}, ..., C_{(k)}),\ C_{(i)} = (C_{1(i)},\ C_{2(i)}),$$

$$C_{1(i)} = \lambda_i^{-1}\zeta_{(i)}(\beta(D^{-1})),\ C_{2(i)} = \lambda_i m_{(i)}\zeta_{(i)}(\alpha(D)),\ \ 0 \leq i \leq k\ .$$

Process of Decryption

Now follow the given steps below to decipher the encrypted messaage:

1. By using the private key for $0 \leq i \leq k$ compute

$$d_{(i)} = \alpha^{-1}\beta(C_{1(i)}) = \alpha^{-1}\beta(\lambda^{-1}\zeta_{(i)}(\beta(D^{-1}))).$$

2. Calculate the following elements for $0 \leq i \leq k$

$$m_{(i)} = C_{2(i)}d_{(i)} = (\lambda_i m_{(i)}\zeta_{(i)}(\alpha(D)))d_{(i)}.$$

3. Finally, deciphered messages are

$$m_{(1)},\ m_{(2)},\ m_{(3)}, ..., m_{(k)}.$$

8.4 New Extension of DH-Algorithm

In this section, we are mainly discussed the extension of DH algorithm over general linear group (which is already discussed in detail in previous chapter) chebyshev polynomials of first and second kind over prime residue field $\mathbb{Z}_p$.

8.4.1 Extension of DH Algorithm based on $T_n(x)$ and $GL(2, \mathbb{Z}_p)$

In this section, we are mainly discussed DH key exchange algorithm for first order chebyshev polynomial of first kind along with general linear group of degree 2 over finite field. The key agreement algorithm using $T_n(x)$ based on prime residue field and $GL(2, \mathbb{Z}_p)$ is given as follows:

1. Sender generates a matrix $h \in GL(2, \mathbb{Z}_p)$ and prime p,
2. Sender selects a private number i which is degree of polynomial with constrain $0 < i < p$,
3. Sender computes $e = T_i(h) \mod p \in GL(2, \mathbb{Z}_p)$,
4. Transmitter sends p, h and e and to receiver,
5. Receiver selects a private number j with condition $0 < j < p$,
6. Receiver computes $f = T_j(h) \mod p \in GL(2, \mathbb{Z}_p)$,
7. Receiver then sends an emails f to sender,
8. Sender calculates the private key $k_1 = g$ with $g = T_i(f) \mod p$,
9. Receiver calculates the private key $k_1 = l$ with $l = T_j(e) \mod p$.

The integer g for sender and integer l for receiver establish the shared secret key k_1 as both have calculated $T_{i*j}(h) \mod p$.

8.4.2 Extension of DH Key Exchange Algorithm based on $U_n(x)$ and $GL(2, \mathbb{Z}_p)$

We are now presenting a DH key agreement algorithm by using Chebyshev polynomials of second kind $U_n(x)$:

1. Sender generates a matrix $h \in GL(2, \mathbb{Z}_p)$ and prime p,
2. Sender selects a private integer i and j with a condition $0 < i, j < p$,
3. Sender computes $e = T_j(h) \mod p$,
4. Sender emails p, h and e to receiver,
5. Receiver takes a secret integer j with constrain that $0 < j < p$,
6. Receiver computes $f = U_{ij-1}(h) \mod p$,
7. Receiver sends f to sender,
8. Sender finds the private key $k_1 = g$ with $g = U_{i-1}(T_j(h))U_{j-1}(h) \mod p$,

9. Receiver finds the private key $k_1 = l$ with $d = U_{ij-1}(h) \mod p$.

The integer g for sender and the integer l for receivers which establish the mutual secret key k_1.

8.5 Case Study

We have discussed in detail the examination of our proposed schemes in this section of chapter in order to authenticate our suggested techniques.

8.5.1 Example

Process of Key Generation

Since in public key encryption process, receiver at receiving end, will have to perform the following procedure to generate public and private keys:

1. Choose a prime number say $p = 2$ (due to local ring) and calculate $n = p^2 = 4$.

2. Choose an arbitrary matrix

$$A = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \in H_2(\mathbb{Z}_4). \tag{8.15}$$

3. Computes matrices

$$B = A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad D = A^3 = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}, B^2D = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}, BD^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \tag{8.16}$$

4. Receiver, choose an arbitrary invertible matrix $F \in GL_2(\mathbb{Z}_4)$:

$$F = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} . \tag{8.17}$$

5. Defines automorphisms of the ring $GL_2(\mathbb{Z}_4)$:

$$\chi : W \to B^{-1}WB, \qquad \delta : W \to D^{-1}WD, \tag{8.18}$$

$\forall\ W \in GL_2(\mathbb{Z}_4)$. Now computes the automorphisms

$$\begin{aligned} \Theta &= \chi^2\delta, & \Omega &= \chi\delta^2, \qquad (8.19)\\ \Theta &: W \to (B^2D)^{-1}W(B^2D), & \Omega &: W \to (BD^2)^{-1}W(BD^2). \qquad (8.20)\end{aligned}$$

6. Calculating the following matrices:

$$BD = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix},\ \Theta(F) = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix},\ \ \Omega(F^{-1}) = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}. \tag{8.21}$$

7. User A public key is

$$\left(n = 4, \Theta(F) = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix},\ \ \Omega(F^{-1}) = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix},\ \ BD = \begin{pmatrix} 26 & 15 \\ 17 & 11 \end{pmatrix}\right), \tag{8.22}$$

and private key

$$\left(B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \ D = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right). \tag{8.23}$$

Process of Encryption

Sender at message sending end, will do the following sequence of steps:

1. Presents the plaintext "**BDAC**" as a matrix $P \in GL_2(\mathbb{Z}_4)$:

$$P = \begin{pmatrix} 3 & 1 \\ 0 & 2 \end{pmatrix} \in GL_2(\mathbb{Z}_4), \tag{8.24}$$

2. Select the random integer k for instance $k = 3$, and computes the matrix:

$$Y = (BD)^3 = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}. \tag{8.25}$$

3. Define automorphism ϑ of the ring $GL_2(\mathbb{Z}_4)$:

$$\Im : W \to Y^{-1}WY, \tag{8.26}$$

for every $W \in GL_2(\mathbb{Z}_4)$.

4. Compute the matrices:

$$\Im(\Theta(F)) = Y^{-1}\Theta(F)Y = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \tag{8.27}$$

$$\Im(\Omega(F^{-1})) = Y^{-1}\Omega(F^{-1})Y = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}. \tag{8.28}$$

5. Now choose an invertible element of $\mathbb{Z}_4$ arbitrarily:

$$\lambda = 3,\ \lambda^{-1} = 1. \tag{8.29}$$

6. Computes the ciphertext

$$C = (C_1, C_2). \tag{8.30}$$

$$C_1 = \lambda^{-1}\Im(\Omega(F^{-1})) = \begin{pmatrix} 1 & 2 \\ 2 & 3 \end{pmatrix}, \tag{8.31}$$

$$C_2 = \lambda P\Im(\Theta(F)) = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}. \tag{8.32}$$

Process of Decryption

Receiver, will do the following steps in order to recover original message:

1. Calculates the matrix d, using the private key:

$$d = \chi\delta^{-1}(C_1) = (BD^{-1})^{-1}C_1(BD^{-1}) = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}.$$

2. The following matrix manipulations is use to get the original message:

$$P = C_2 d = \begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}. \tag{8.33}$$

8.5.2 Example

Process of Key Generation

1. Select a prime number $p = 23$

2. Consider a group $GL_2(\mathbb{Z}_{23})$ and $H \subset GL_2(\mathbb{Z}_{23})$

3. Choose two matrices $A,\ B \in GL_2(\mathbb{Z}_{23})$

$$A = \begin{bmatrix} 5 & 4 \\ 5 & 5 \end{bmatrix}, B = \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix} \tag{8.34}$$

4. Now check that $A,\ B \in H$, if not then repeat step 2 and choose those matrices which belongs to H

5. Choose two polynomials

$$f(x) = 3x^3 + 4x^2 + 5x + 6, \tag{8.35}$$

$$g(x) = x^4 + 5x^3 + 2x + 1, \tag{8.36}$$

6. Determine $f(A)$ and $g(B)$, i.e.

$$f(A) = \begin{bmatrix} 2 & 7 \\ 7 & 2 \end{bmatrix},\ g(B) = \begin{bmatrix} 5 & 9 \\ 9 & 5 \end{bmatrix}, \tag{8.37}$$

and $\det(f(A)),\ \det(g(B)) \neq 0$.

7. Define two commutative automorphisms of $GL_2(\mathbb{Z}_{23})$.

$$\eta : K \to (f(A))^{-1}K(f(A)),\ \xi : K \to (g(B))^{-1}K(g(B)), \tag{8.38}$$

for $A, B \in GL_{2\times 2}(\mathbb{Z}_{23})$. As the matrices A and B belongs to H therefore the automorphisms η and ξ.

8. Now define the following automorphisms of $GL_{2\times 2}(\mathbb{Z}_{23})$

$$\alpha : K \to (f(A)^2 g(B))^{-1} K (f(A)^2 g(B)),$$

$$\beta : K \to (f(A) g(B)^2)^{-1} K (f(A) g(B)^2),$$

such that

$$\alpha = \eta^2 \xi, \ \beta = \eta \xi^2. \tag{8.39}$$

Automorphisms α and β commutes therefore,

$$\alpha = \eta \xi^{-1} \beta, \ \beta = \eta^{-1} \xi \alpha. \tag{8.40}$$

9. Select a random matrix

$$D = \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \in GL_{n\times n}(\mathbb{Z}_p), \tag{8.41}$$

$$D^{-1} = \begin{bmatrix} 18 & 2 \\ 3 & 22 \end{bmatrix} \tag{8.42}$$

such that $D \notin H$.

10. Find the following matrices

$$D^{-1} = \begin{bmatrix} 18 & 2 \\ 3 & 22 \end{bmatrix} \tag{8.43}$$

$$\alpha(D) = \begin{bmatrix} 7 & 22 \\ 6 & 22 \end{bmatrix} \tag{8.44}$$

$$\beta(D^{-1}) = \begin{bmatrix} 20 & 9 \\ 19 & 20 \end{bmatrix} \tag{8.45}$$

11. Public key for encryption is

$$\left(p = 23, \alpha(D) = \begin{bmatrix} 7 & 22 \\ 6 & 22 \end{bmatrix}, \ \beta(D^{-1}) = \begin{bmatrix} 20 & 9 \\ 19 & 20 \end{bmatrix} \right), \tag{8.46}$$

and private key for decryption is

$$\left(f(A) = \begin{bmatrix} 2 & 7 \\ 7 & 2 \end{bmatrix}, \ g(B) = \begin{bmatrix} 5 & 9 \\ 9 & 5 \end{bmatrix} \right). \tag{8.47}$$

Process of Encryption

For encryption following steps are performed

1. Consider the matrix of plaintext be

$$m = \begin{bmatrix} 10 & 1 \\ 3 & 1 \end{bmatrix} \in GL_2(\mathbb{Z}_{23}). \tag{8.48}$$

2. Choose a random matrix

$$N = \begin{bmatrix} 4 & 1 \\ 1 & 4 \end{bmatrix} \in H \text{ and its inverse } N^{-1} = \begin{bmatrix} 11 & 3 \\ 3 & 11 \end{bmatrix}$$

3. Define automorphism of $GL_2(\mathbb{Z}_{23})$ for every $0 \leq i \leq k$

$$\zeta_{(i)} : D \to (N_{(i)})^{-1} D (N_{(i)}). \tag{8.49}$$

for every $D \in GL_2(\mathbb{Z}_{23})$.

4. Compute the following matrices

$$\zeta(\alpha(D)) = N^{-1}\alpha(D)N = \begin{bmatrix} 21 & 16 \\ 12 & 8 \end{bmatrix}, \tag{8.50}$$

$$\zeta(\ \beta(D^{-1})) = N^{-1}\beta(D^{-1})N = \begin{bmatrix} 2 & 16 \\ 12 & 15 \end{bmatrix}. \tag{8.51}$$

5. Now select a unit element of $\mathbb{Z}_{23}$ randomly:

$$\lambda = 3, \quad \lambda^{-1} = 8. \tag{8.52}$$

6. Compute the ciphertext

$$C = (C_1, C_2), \tag{8.53}$$

$$C_1 = \lambda^{-1}\zeta(\ \beta(D^{-1})) = \begin{bmatrix} 16 & 13 \\ 4 & 5 \end{bmatrix}, \tag{8.54}$$

$$C_2 = \lambda m \zeta(\alpha(D)) = \begin{bmatrix} 22 & 21 \\ 18 & 7 \end{bmatrix}. \tag{8.55}$$

Process of Decryption

Now follow the given steps below to decipher the encrypted message:

1. By using the private key for $0 \leq i \leq k$ compute

$$d = \alpha^{-1}\beta(C_1) = \alpha^{-1}\beta(\lambda^{-1}\zeta(\beta(D^{-1}))) = \begin{bmatrix} 5 & 13 \\ 4 & 16 \end{bmatrix}. \tag{8.56}$$

2. Calculate the following matrices for $0 \leq i \leq k$

$$m = C_2 d = (\lambda m\zeta(\alpha(D)))d = \begin{bmatrix} 10 & 1 \\ 3 & 1 \end{bmatrix}. \tag{8.57}$$

3. Finally, deciphered matrix is

$$m = \begin{bmatrix} 10 & 1 \\ 3 & 1 \end{bmatrix}. \tag{8.58}$$

8.5.3 Example

Process of Key Generation

1. Consider a Galois field of order 3^2,i.e. $GF(3^2)$.

2. Select two elements $A,\ B \in GF(3^2)$

$$A = 2\alpha + 2,\ B = 2\alpha, \tag{8.59}$$

3. Define the following automorphisms of $GF(p^n)$

$$\alpha : K \to (A^2B)^{-1}K(A^2B), \tag{8.60}$$

$$\beta : K \to (AB^2)^{-1}K(AB^2). \tag{8.61}$$

4. Let $D = 2\alpha + 1$ be any random element of $GF(3^2)$ and $D^{-1} = 2\alpha$

5. Compute the following elements $D^{-1} = 2\alpha,\ \alpha(D) = 2\alpha + 1,\ \beta(D^{-1}) = 2\alpha.$

6. Public key for encryption is

$$(p=3, \alpha(D)=2\alpha+1,\ \beta(D^{-1})=2\alpha), \tag{8.62}$$

and private key for decryption is

$$(A=2\alpha+2,\ B=2\alpha). \tag{8.63}$$

Process of Encryption

For encryption following steps are performed

1. Consider the plaintext be

$$m=2\alpha+2\in GF(3^2). \tag{8.64}$$

2. For plaintext $P=2\alpha+2$, choose a random element $N=2\alpha\in GF(p^n)$ and $N^{-1}=2\alpha+1$

3. Define automorphism

$$\zeta : D\rightarrow (N)^{-1}D(N), \tag{8.65}$$

for every $D\in GF(3^2)$.

4. Compute the following elements

$$\zeta(\beta(D^{-1})) = 2\alpha, \tag{8.66}$$

$$\zeta(\alpha(D)) = 2\alpha+1. \tag{8.67}$$

5. Select a random unit $\lambda=\alpha+2\in GF(p^n), \lambda^{-1}=\alpha$ and calculate the ciphertext

$$C=(C_1,\ C_2), \tag{8.68}$$

$$\begin{aligned} C_1 &= \lambda^{-1}\zeta(\beta(D^{-1}) = 2\alpha+1, && (8.69)\\ C_2 &= \lambda m\zeta(\alpha(D)) = 1. && (8.70)\end{aligned}$$

Process of Decryption

Now follow the given steps below to decipher the encrypted message:

1. By using the private key compute

$$d = \alpha^{-1}(\beta(C_1)) = \alpha^{-1}(\beta(\lambda^{-1}\zeta(\beta(D^{-1})))) = 2\alpha+2. \tag{8.71}$$

2. Calculate the following elements for $0 \leq i \leq k$

$$m = C_2 d = (\lambda m\zeta(\alpha(D)))d = 2\alpha+2. \tag{8.72}$$

3. Finally, deciphered message is

$$m = 2\alpha+2. \tag{8.73}$$

8.5.4 Example

We are now start with a very small example in order to understand the above mechanism for general linear group over prime residue field. We have taken $i = 2$ and $j = 3$ and calculate $T_2(x) = 2x^2-1$, $T_3(x) = 4x^3-3x$ and $T_6(x) = 32x^6-48x^4-18x^2-1$.

1. Transmitter selects $p = 7$ and $h = \begin{bmatrix} 6 & 2 \\ 3 & 4 \end{bmatrix} \in GL(2, \mathbb{Z}_7)$,
2. Transmitter selects $i = 2$,
3. Sender calculates the following values $e = T_2(h) \mod 7 = \begin{bmatrix} 6 & 5 \\ 4 & 1 \end{bmatrix}$,

4. Sender then emails receiver $p = 7$, h and e,

5. Receiver at the receiving end selects $j = 3$,

6. Receiver calculates $f = T_3(h) \mod 7 = \begin{bmatrix} 5 & 6 \\ 2 & 6 \end{bmatrix}$,

7. Receiver emails f,

8. Sender/Transmitter calculates $g = T_2(f) \mod 7 = \begin{bmatrix} 3 & 6 \\ 2 & 4 \end{bmatrix}$,

9. Receiver find $l = T_3(e) \mod 7 = \begin{bmatrix} 3 & 6 \\ 2 & 4 \end{bmatrix}$.

8.5.5 Example

We pick same integers in order to generate the first and second order Chebyshev polynomials. We select $i = 2$ and $j = 3$ and compute $T_2(x) = 2x^2-1$, $T_3(x) = 4x^3-3x$, $U_2(x) = 4x^2-1$, $U_3(x) = 8x^3-4x$ an $U_5(x) = 4x^5+3x^3+6x$. The steps for DH key exchange algortihms based on Chebyshev polynomails of second kind and $GL(2, \mathbb{Z}_7)$ are given below:

1. Transmitter selects $p = 7$ and $h = \begin{bmatrix} 5 & 1 \\ 3 & 4 \end{bmatrix} \in GL(2, \mathbb{Z}_7)$,

2. Transmitter selects $i = 2$,

3. Sender calculates the following values $e = T_2(h) \mod 7 = \begin{bmatrix} 6 & 5 \\ 4 & 1 \end{bmatrix}$,

4. Sender then communicates receiver $p = 7$, h and $e = U_1(T_3(h))U_2(h) \mod 7 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$,

5. Receiver at the receiving end selects $j = 3$,

6. Receiver finds $f = U_{j-1}(h) \mod 7 = \begin{bmatrix} 6 & 4 \\ 5 & 2 \end{bmatrix}$,

7. Receiver emails f,

8. Sender/Transmitter calculates $g = U_1(e)f \mod 7 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$,

9. Receiver calculates $l = U_{ij-1}(h) \mod 7 = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$.

Similarly we can easily develop two more cases for chebyshev polynomials of second kind over local ring and simple ring. The idea of non-commutative structures along with orthogonal polynomials is utilized efficiently in order to improve the DH exchange algorithm. With this improve scheme, we can easily use this design technique in modern cryptosystems while exchange key.

8.6 Conclusion

The principal aim of this part of thesis is to device three innovative cryptosystems based on $GL_2(\mathbb{Z}_{p^n})$, $GL_2(\mathbb{Z}_p)$ and $GL_2(GF(p^n))$. We have design all three cryptosystems independently using three different structures inside general linear group. First, cryptosystem uses $GL_2(\mathbb{Z}_{p^n})$. Second, cryptosystem uses $GL_2(\mathbb{Z}_p)$ and third cryptosystem based on $GL_2(GF(p^n))$. The key generation section in cryptosystem III, is based on polynomial extension instead of matrices elements. This modification can easily be used in different multimedia applications. The key exchange issue is the means by which to trade whatever keys or other data are required with the goal that nobody else can get a duplicate. Generally, this required put stock in messengers, discretionary sacks, or some other secure channel. With the appearance of asymmetric/secret key algorithms, the scrambling key (general public/asymmetric key which is in pair) could be made public, since nobody without the decoding key could unscramble the message. Our objective here is to include greater many-sided quality in existing key trade algorithms keeping in mind the end goal to stop interloper to approach the private key. We have supplanted numbers with networks and one term articulation with polynomial of degree n. This change can extremely upgrade the current public key cryptosystems.

Chapter 9

Conclusions

The basic distinction amongst feeling and reason is that feeling prompts activity, while reason prompts conclusions (by Donald Calne). When one thing closes, something else starts. At times finishing something harms, yet a fresh start is constantly worth and agony. To finish up this thesis, we abridge its principle commitments and recommend various headings for additionally look into.

9.1 Impacts of Present Thesis

With the help of present thesis, we have examined distinctive parts of symmetric and asymmetric algorithms. After a short talk of the primary standards of symmetric and asymmetric encryption conspire, and a clarification of the method of reasoning behind various sorts of encryption algorithms are examined in first section. We have focused on various subjects which are altogether associated by one focal topic: the significance of nonlinear segment in particular nonlinear components of block ciphers in symmetric cryptography, watermarking and steganography. We have planned new nonlinear components of block ciphers in view of various algebraic structures. The subject of present theory is three crease, one with improvement of mathematical structures for differing interactive media applications, second to use these for advanced medium which incorporates content, picture, sound and video; and last one to approve the proposed algorithms through statistical examinations. The particular commitments made in this thesis are examined underneath:

- In chapters $2, 3$ and 4, we have developed new nonlinear components of block ciphers based on finite Galois fields $GF(2^4)$, symmetric group S_4 and logarithmic permutations. We have not only designed small nonlinear components of block ciphers but also use these proposed nonlinear components of block ciphers for copyright protection and information hiding schemes. We have utilized $3D$ histogram to analyze the similarities in original and watermarked images. Various types of pixel difference and correlation based statistical analyses as well as algebraic analyses were used to testify the proposed copyright protection and information hiding techniques.

- The trust of new algebraic and statistical analyses plays a vital role in cryptographic algorithms. Several new and modified versions of algebraic and statistical analyses like nonlinearity, strict avalanche criterion, bit independent criterion, linear and differential approximation probabilities, pixel differencing analyses, correlation based analyses and, human vision system based analyses were suggested in order to test the strength of nonlinear component of block cipher. In this sequel, we have proposed new algebraic analyses which include balancedness, nonlinearity, correlation immunity, absolute indicator, sum of square indicator, algebraic degree, algebraic immunity, transparency order, propagation characteristics, strict avalanche criteria, number of fixed points, number of opposite fixed points, composite algebraic immunity, robustness to differential cryptanalysis, delta uniformity, SNR(DPA) and confusion coefficient variance which is main philosophy of chapter 5.

- There is always room of improvement in every science and technology area. Same happened in cryptographic algorithms, where improvements are going by each instant of time. The algorithms development is very interesting task in information security, where we need different algebraic structures and statistical analyses in order to improve the later one and, validate new algorithms. In this respect, the idea of Galois ring based nonlinear components of block ciphers were projected in chapter 6 which is completely new dimension of developing cryptographically secure new class of Boolean functions having high nonlinearity as compared to existing one.

- One look is worth a thousand words and images speak louder than words therefore we are in the era of live streaming where video play a significant role. The importance of video in today's world can't be denied by anyone. The video fundamentally comprises of number of frames which means video can speaks millions and billions of worlds. Due to its importance in daily usage, protection of illegal access to video is also an emerging issue in today digital sphere of information age. In this regard, we have developed new nonlinear components of block ciphers which is based on $\mathbb{Z}_{257}$ and action of symmetric group S_8 which is responsible to generate a large number of nonlinear components of block ciphers. The idea of video encryption based on mention structure is presented in chapter 7.

- The idea of public key cryptography is to use two different keys for encryption and decryption which arouse a new height in cryptography where we utilizing prime factorization and discrete log based algorithms most famous are RSA and Elgamal cryptosystems. Their extensions were developed based on matrix algebra which adds more complexity in simple public key algorithms to cryptanalysis. The idea of subgroup of general linear group based on units of local ring is use to develop a new cryptosystems in chapter 8. Also, we have extended the Diffie Hellman key exchange algorithm which is based on polynomails and general linear group of order 2 over prime residue field which is given in chapter 8. The Diffie Hellman key exchange algorithm proposed in chapter 8, have a high level of complexity as compared to standard algorithm which is based on discrete log property.

9.2 Future Research

The research work of science and art shows people new directions and thinks of the future. Similarly efforts are not enough without purpose and future directions. Finally, we suggest some directions for further research.

- Idea of watermarking with small nonlinear components of block ciphers will further utilize in steganogrphy of audio and also usefulness of these nonlinear components of block ciphers in frequency domains. The combination of encryption and watermarking scheme will be developed in future to provide more privacy in cryptosystems.
- Extending the algebraic analyses of chapter 5 to nonlinear components of block ciphers

based on Galois ring which classifying larger nonlinear components of block ciphers.

- The idea of small nonlinear components of block ciphers with large number of bits is central point of chapter 6. This theory can easily be extended to other class of finite chain ring and apply these nonlinear components of block ciphers in digital multimedia applications.

- We apply proposed nonlinear components of block ciphers based on residue prime field $\mathbb{Z}_{257}$ and symmetric groups S_8 of order 8! which create confusion capability and apply second order texture analyses. We can also add diffusion layer through any discrete and continuous chaotic systems and, also add some more statistical analyses to confirm the authentication of proposed algorithm.

- Finally, the theory of general linear group based algorithm can also be implemented on digital medium. We extend this idea to develop digital signature scheme based on subgroup of general linear group of unit of local ring.

Bibliography

[1] C. E. Shannon, A mathematical theory of communication, Bell Labs. Tech. J., 27 (1948) 379–423.

[2] C. E. Shannon, Communication theory of secrecy systems, Bell Labs. Tech. J., 28 (1949) 656–715.

[3] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, (2010) 257-397.

[4] C. Carlet, Partially-bent functions, Design Codes Cryptogr., 3(2) (1993) 135-145.

[5] M. Matsui, Linear cryptoanalysis method for DES cipher, Lect. Notes. Comput. Sc., 765 (1994) 386-397.

[6] R. L. McFarland, A discrete fourier theory for binary functions, R41 Technical paper, 1971.

[7] P. K. Menon, On difference sets whose parameters satisfy a certain relation, Proc. Amer. Math. Soc., 13 (1962) 739-745.

[8] O. S. Rothaus, On bent functions, J. Combin. Theory Ser. A., 20 (1976) 300-305.

[9] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inf. Theory., 30(5) (1984) 776-780.

[10] J. Christian, M. Hortmann and G. Leander, Boolean Functions, PhD thesis, (2012).

[11] Jean-Pierre Flori. Boolean functions, algebraic curves and complex multiplication, Télécom ParisTech, 2012.

[12] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, Lect. Notes. Comput. Sc., 1008 (1994) 61-74.

[13] Thomas Cusick, Pantelimon Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2009.

[14] C. Carlet, A construction of bent functions, Finite Fields Th. App. 233 (4) (1996) 47-58.

[15] S. Chee, S. Lee and K. Kim, Semi-bent functions, Lect. Notes. Comput. Sc., 917 (1995) 107-118.

[16] Y. Zheng, X. M. Zhang, Plateaued functions, Lect. Notes. Comput. Sc., 1726 (1999) 284-300.

[17] C. Carlet, E. Prouf, On plateaued functions and their constructions, Lect. Notes. Comput. Sc., 2887 (2003) 54-73.

[18] A. Menezes, P. van Oorschot, S. Vanstone, Applied Cryptography. CRC, Boca Raton, 1996.

[19] Seitz J (2005) Digital watermarking for digital media. Idea Group Publishing, Hershey, PA. doi:10.4018/978-1-59140-518-4.ch001

[20] Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T (2008) Digital watermarking and steganography, 2nd edn. Morgan Kaufmann Publisher, San Francisco, CA

[21] Ruanaidh JJKO, Dowling WJ, Boland FM (1996) Watermarking digital images for copyright protection. In: IEEE ProcVis. Image Signal Process, vol 143, No 4, pp 250–254

[22] Cox IJ, Kilian J, Leighton T, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687

[23] Alghoniemy M, Tewfik AH (2004) Geometric invariance in image watermarking. IEEE Trans Image Process 13(2):145–153.

[24] Yang Z, Campisi P, Kundur D (2004) Dual domain watermarking for authentication and compression of cultural heritage images. IEEE Trans Image Process 13(3):430–448

[25] Ruanaidh JJKO, Pereira S (1998) A secure robust digital image watermark. In: Proceedings of SPIE 3409, Electronic imaging: processing, printing, and publishing in color, 150. doi:10.1117/ 12.324106

[26] Venkatesan R, Jakubowski M (2000) Image watermarking with better resilience. In: Proceeds ICIP 2000

[27] Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixelwise masking. IEEE Trans Image Process 10: 783–791

[28] Tefas A, Nikolaidis A, Nikolaidis N, Solachidis V, Tsekeridou S, Pitas I (2001) Statistical analysis of markov chaotic sequences for watermarking applications. In: Proceedings of IEEE international

symposium on circuits and systems (ISCAS2001)

[29] Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. J Pattern Recognit Soc 37:469–474

[30] Bamatraf A, Ibrahim R, Salleh M, Mohd N (2011) A new digital watermarking algorithm using combination of least significant bit (LSB) and inverse bit. J Comput 3:1–8

[31] Nikolaidis S, Pitas I (2008) Comparison of different chaotic maps with application to image watermarking. In: Proceedings of IEEE international symposium on circuits and system cryptography

based on chaotic random maps with position dependent weighting probabilities Chaos, Solitons & Fractals 35 pp 362–369

[32] Giovanardi A, Mazzini G (2001) Frequency domain chaotic watermarking. In: Proceedings of IEEE Symposium Circuits and System, Sydney, vol 2, pp 521–524

[33] Sujatha SS, Sathik MM (2012) A novel DWT based blind watermarking for image authentication. Int J Netw Secur 14(4) : 223–228

[34] Hsu CT, Wu JL (1998) DCT-based watermarking for video. IEEE Trans Consum Electron 44(1):206–216

[35] Cox IJ, Miller ML, Bloom JA (2001) Digital watermarking, 1st edn. Morgan Kaufmann Publisher, San Fransisco

[36] Kutter M, Jordan F, Digital watermarking technology. AlpVision, Switzerland, pp 1–4

[37] Morimoto Norishige (1999) Digital watermarking technology with practical applications. Inf Sci 2:107–111

[38] Luo H, Chu SH, LuZM(2008) Self-embeddingwatermarking using half toning technique. Circuits Syst Signal Process 27:155–170

[39] Lee YK, Bell G, Huang SY, Wang RZ, Shyu SJ (2009) An advanced least-significant-bit embedding scheme for steganographic encoding. Springer, Berlin

[40] Rashi Singh and Gaurav Chawla, A Review on Image Steganography, International Journal of Advanced Research in Computer Science and Software Engineering, 4 (5) (2014) 686-689.

[41] Archana.O.Vyas, Sanjay.V. Dudul, An Overview of Image Steganographic Techniques, International Journal of Advanced Research in Computer Science, 6 (2015) 67-72.

[42] Z. Wang and A. C. Bovik, A universal image quality index, IEEE Signal Processing letters, vol. 9, no.3, pp. 81-84, March 2002

[43] Chandrasekharappa TGS, Prema KV, Shama K (2011) nonlinear components of block ciphers generated using affine transformation giving maximum avalanche effect. Int J Comput Sci Eng 3:3185–3193

[44] Cid Carlos, Murphy Sean, Robshaw Matthew (2006) Algebraic Aspects of the advanced encryption standard. Springer, US

[45] Khan M, Shah T (2014) A novel statistical analysis of chaotic S-box in image encryption. 3D Res 5:16. doi:10.1007/s13319-014-0016-5

[46] A. Piva, F. Bartolini, M. Barni , Managing copyright in open networks, IEEE Trans. Internet Comput., 6(3) (2002) 18-26.

[47] C. Lu, S. Huang, C. Sze, H. Y. M. Liao , Cocktail watermarking for digital image protection, IEEE Trans. Multimedia., 2(4) (2000) 209-224.

[48] M. M. Latha, G. M. Pillai, K. A. Sheela, Watermarking based content Security and Multimedia Indexing in digital Libraries, International Conference on Semantic Web and Digital Libraries, (2007).

[49] W. Bender, D. Gruhi, N. Morimota, A. Lu, Techniques for Data Hiding, IBM. Syst. J., 35 (3-4) (1996) 313 - 336.

[50] Majid Khan, Tariq Shah and Syeda Iram Batool, A color image watermarking scheme based on affine transformation and S4 permutation, Neural Comput & Applic, Springer, (2014) 25:2037–2045.

[51] Ingemar J. Cox, Matt L. Miller and Jeffrey A. Bloom, Watermarking applications and their properties, Int. Conf. on Information Technology'2000, Las Vegas, 2000

[52] Majid Khan, Tariq Shah, An efficient construction of substitution box with fractional chaotic system, Signal, Image and Video Processing, DOI 10.1007/s11760-013-0577-4.

[53] Abuelyman ES, Alsehibani AAS (2008). An optimized implementation of the S-Box using residue of prime numbers. Int. J. Comput. Sci. Ntwk. Secur., 8(4): 304-309.

[54] Alam GM, Mat Kiah ML, Zaidan BB, Zaidan AA, Alanazi HO (2010). Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Int. J. Phys. Sci., 5(21): 3254-3260.

[55] Cui L, Cao Y (2007). A new S-box structure named Affine- PowerAffine. Int. J. Innov. Comput. I., 3(3): 45-53.

[56] Daemen J, Rijmen V (1999). AES Proposal: Rijndael. AES Algorithm Submission, Available: http://csrc.nist.gov/archive/aes/rijndael/ Rijndael-ammended.pdf.

[57] Enayatifar R (2011). Image encryption via logistic map function and heap tree. Int. J. Phys. Sci., 6(2): 221:228.

[58] Gadelmawla ES (2004). A vision system for surface roughness characterization using the gray level co-occurrence matrix. NDT & E. Int., 37(7): 577-588.

[59] Hussain I, Shah T, Mehmood H (2010). A New Algorithm to Construct Secure Keys for AES. Int. J. Cont. Math. Sci., 5(26): 1263-1270.

[60] Lui J, Wai B, Cheng X, Wang X (2005). An AES S-box to increase complexity and cryptgraphic analysis. Int. Conf. Infor. Network. Appl.,1: 724-728.

[61] Prasadh K, Ramar K, Gnanajeyaraman R (2009). Public key cryptosystems based on chaotic Chebyshev polynomials. Int. J. Phys. Sci., 1(7): 122-128.

[62] Shi XY, Xiao Hu You XC, Lam KY (2002). A Method for Obtaining Cryptographically Strong 8×8 nonlinear components of block ciphers. Int. Conf. Infor. Network. Appl., 2(3): 14-20.

[63] SKIPJACK (1998). KEA Algorithm. Specifications version, 2(29): 1-23.

[64] Tran MT, Bui DK, Doung AD (2008). Gray S-box for Advanced Encryption Standard. Int. Conf. Comp. Intel. Secur., 253-256.

[65] J.M.H. du Buf, M. Kardan and M. Spann,“Texture Feature Performance of Image Segmentation”, Pattern Recognition, Vol. 23, pp. 291-309, 1990.

[66] JC.C. Gotlieb and H.E. Kreyszig,“Texture Descriptors based on Co-ocurrence Matrices”,Computer Vision, Graphics, and Image Processing, Vol. 51, pp. 70-86, 1990.

[67] R.M. Haralick, K. Shanmugam, and I. Dinstein,”Textural Features for Image Classification”, IEEE Trans. on Systems, Man and Cybernetics, Vol. SMC-3, pp. 610-621, 1973.

[68] R.M. Haralick and K. Shanmugam, ”Computer Classification of Reservoir Sandstones”, IEEE Trans. on Geo. Eng., Vol. GE-11, pp. 171-177, 1973.

[69] D.C. He, L.Wang, and J. Juibert, ”Texture Feature Extraction”, Pattern Recognition Letters, Vol. 6, pp. 269-273, 1987.

[70] M. Iizulca, "Quantitative evaluation of similar images with quasi-gray levels", Computer Vision, Graphics, and Image Processing, Vol. 38, pp. 342-360, 1987.

[71] S. Peckinpaugh,"An Improved Method for Computing Gray-Level Coocurrence Matrix Based Texture Measures", Computer Vision, Graphics, and Image Processing; Graphical Models and Image Processing, Vol. 53, pp. 574-580, 1991.

[72] L.H. Siew, R.H. Hodgson, and E.J. Wood, "Texture Measures for Carpet Wear Asessment", IEEE Trans. on Pattern Analysis and Machine Intell., Vol. PAMI-10, pp. 92-105, 1988.

[73] L.H. Siew, R.H. Hodgson, and E.J. Wood, "Texture Measures for Carpet Wear Asessment", IEEE Trans. on Pattern Analysis and Machine Intell., Vol. PAMI-10, pp. 92-105, 1988.

[74] M.M. Trivedi, R.M. Haralick, R.W. Conners, and S. Goh, "Object Detection based on Gray Level Coocurrence", Computer Vision, Graphics, and Image Processing, Vol. 28, pp. 199-219, 1984. Albregtsen : Texture Measures Computed from GLCM-Matrices 14

[75] M Unser, "Sum and Difference Histograms for Texture Classification", IEEE Trans. on Pattern Analysis and Machine Intell., Vol. PAMI-8, pp. 118-125, 1986.

[76] J.S. Weszka, C.R. Dyer, and A. Rosenfeld, "A comparative Study of Texture Measures for Terrain Classification", IEEE Trans. on Systems, Man and Cybernetics, Vol. SMC-6, pp. 269-285, 1976.

[77] JC-M. Wu, and Y-C. Chen, "Statistical Feature Matrix for Texture Analysis", Computer Vision, Graphics, and Image Processing; Graphical Models and Image Processing, Vol. 54, pp. 407-419, 1992.

[78] T. Shah, N. Mehmood, A.A. Andrade and R. Palazzo Jr., Maximal cyclic subgroups of the groups of units of Galois rings: A computational approach, Computational and Applied Mathematics- (40314/CAM) DOI 10.1007/s40314-015-0281-9

[79] Bart Preneel', Werner Van Leekwijck, Luc Van Linden, Rem Govaerts and Joos Vandewalle, Propagation characteristics of Boolean functions, Advances in Cryptology - EUROCRYPT '90, LNCS

473, pp. 161-173, 1991. 0 Springer-Verlag Berlin Heidelberg 1991.

[80] W. Meier, Othmar Staffelbach, Nonlinearity criteria for cryptographic functions, Advances in Cryptology — EUROCRYPT '89, Volume 434 of the series Lecture Notes in Computer Science pp 549-562.

[81] X.-M. Zhang and Y. Zheng. Auto-correlations and new bounds on the nonlinearity of Boolean functions. Advances in Cryptology – EUROCRYPT, 96, no. 1070 in Lecture Notes in Computer Science, Springer-Verlag, pp. 294-306, 1996.

[82] D. Olejar and M. Stanek. On cryptographic properties of random Boolean functions." Journal of Universal Computer Science, vol. 4, No.8, pp. 705-717, 1998.

[83] Y. Zheng, X.-M. Zhang, and H. Imai. Restriction, terms and nonlinearity of Boolean functions. Theoretical Computer Science, 226(1-2),pp. 207-223, 1999.

[84] P. Sarkar and S. Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. CRYPTO 2000, LNCS, vol. 1880, ed. Mihir Bellare, pp. 515-532, 2000.

[85] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. Advances in Cryptology - EUROCRYPT 2000, no. 1807 in Lecture Notes in Computer Science, Springer Verlag, pp. 485-506, 2000.

[86] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. Proceedings of EUROCRYPT'2000, Advances in Cryptology, Lecture Notes in Computer Science n 187, pp. 507-522 (2000).

[87] E. Pasalic, T. Johansson, S. Maitra and P. Sarkar. New constructions of resilient and correlation immune Boolean functions achieving upper bounds on nonlinearity. Proceedings of the Workshop on Coding and Cryptography 2001, published by Electronic Notes in Discrete Mathematics, Elsevier, vo. 6, pp. 425-434, 2001.

[88] S. Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property. Proceedings of the Workshop on Coding and Cryptography 2001 published by Electronic Notes in Discrete Mathematics, Elsevier, vo. 6, pp. 355-364, 2001.

[89] J. Clark, J. Jacob, S. Stepney, S. Maitra, W. Millan, Evolving Boolean functions satisfying multiple criteria, in: INDOCRYPT 2002, Lecture Notes in Computer Science, vol. 2551, Springer, Berlin, 2002, pp. 246–259.

[90] C. Carlet. A larger Class of Cryptographic Boolean Functions via a Study of the Maiorana-McFarland Construction. Advances in Cryptology - CRYPT0 2002, no. 2442 in Lecture Notes in Computer Science, pp. 549-564, 2002.

[91] P. Charpin. Normal Boolean functions, Journal of Complexity 20, pp. 245-265, 2004.

[92] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science 1008, pp.61-74, 1995.

[93] A. Canteaut and M. Videau. Symmetric Boolean functions. IEEE Transactions on Information Theory 51(8), pp. 2791-2811, 2005.

[94] D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Significant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. Fast Software Encryption 2005, Lecture Notes in Computer Science 3557, pp. 98-111, 2005.

[95] A. Braeken and B. Preneel, On the algebraic immunity of symmetric Boolean functions, in INDOCRYPT 2005, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 2005, pp. 35-48.

[96] C. Carlet, D. Dalai, K. Gupta and S. Maitra. Algebraic Immunity for Cryptographically Significant Boolean Functions: Analysis and Construction. IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 3105-3121, July 2006.

[97] Li, N., Qi, W.-Q.: Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 84–98. Springer, Heidelberg (2006).

[98] Sihem Mesnager, Improving the Lower Bound on the Higher Order Nonlinearity of Boolean Functions With Prescribed Algebraic Immunity, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 54, NO. 8, AUGUST 2008,

[99] Wei Guo Zhang, Member, IEEE, and GuoZhen Xiao, Constructions of Almost Optimal Resilient Boolean Functions on Large Even Number of Variables, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 55, NO. 12, DECEMBER 2009

[100] Qichun Wang, Jie Peng, Haibin Kan, Member, Constructions of Cryptographically Significant Boolean Functions Using Primitive Polynomials, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 6, JUNE 2010.

[101] Enes Pasalic and Yongzhuang Wei, On the Construction of Cryptographically Significant Boolean Functions Using Objects in Projective Geometry Spaces, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 58, NO. 10, OCTOBER 2012 6681

[102] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich, and R. Smolensky, The bit extraction problem or $t-$resilient functions, In Foundations of Computer Science, 1985, 26th Annual Symposium, 396-407.

[103] J. F. Dillon, A survey of bent functions, The NSA technical journal, (1972) 191-215.

[104] R. Forre, The strict avalanche criterion: Spectral properties of boolean functions and an extended definition, Lect. Notes. Comput. Sc., 403 (1990) 450-468.

[105] M. Matsui, Linear cryptoanalysis method for DES cipher, Lect. Notes. Comput. Sc., 765 (1994) 386-397.

[106] Preneel, V. Leekwijk, V. Linden, Govaerts and Vandewalle, Propagation characteristics of boolean functions, Lect. Notes. Comput. Sc., 473 (1991) 161-173.

[107] A. F. Webster and S. E. Tavares. On the design of nonlinear components of block ciphers, Lect. Notes. Comput. Sc., 218 (1986) 523-534.

[108] Y. Zheng, X. M. Zhang, Plateaued functions, Lect. Notes. Comput. Sc., 1726 (1999) 284-300.

[109] Y. Zheng, M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, Lect. Notes. Comput. Sc., 2012 (2001) 262-274.

[110] M. Matsui, The first experimental cryptanalysis of the Data Encryption Standard, Lect. Notes. Comput. Sc., 839 (1994) 1–11.

[111] H. M. Heys, A tutorial on linear and differential cryptanalysis, Technical Report CORR 2001-17, Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, March 2001.

[112] E. Biham, A. Shamir, Differential cryptanalysis of DES like cryptosystems, Lect. Notes. Comput. Sc., 537 (1991) 2–21.

[113] T. Siegenthaler, Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications, IEEE Transactions on Information Theory 30 (5) (1984) 776–780.

[114] L. L. Bartosov, Linear and differential cryptanalysis of reduced-round AES, Tatra Mt. Math. Publ., 50(1) (2011) 51-61.

[115] G. Chen, Y. Chen, X. Liao, An extended method for obtaining nonlinear components of block ciphers based on three-dimensional chaotic Baker maps, Chaos Solitons Fract., 31(3) (2007) 571–577.

[116] F. Özkaynak, A. B. Özer, A method for designing strong nonlinear components of block ciphers based on chaotic Lorenz system, Phys. Lett. A., 374(36) (2010) 3733–3738.

[117] Y. Wang, K. W. Wong, X. Liao, T. Xiang, A block cipher with dynamic nonlinear components of block ciphers based on tent map, Commun. Nonlinear Sci. Numer. Simul., 14(7) (2009) 3089-3099.

[118] Y. G. Chen, X. Liao, An extended method for obtaining nonlinear components of block ciphers based on three-dimensional chaotic Baker maps, Chaos Solitons Fract., 31(3) (2007) 571-577.

[119] T. Guoping, L. Xiaofeng, C. Yong, A novel method for designing nonlinear components of block ciphers based on chaotic maps, Chaos Solitons Fract., 23(2) (2005) 413-419.

[120] G. Jakimoski, L. Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, IEEE Trans. Circuits Syst., 48(2) (2001) 163-170.

[121] C. Adams, S. Tavares, Good nonlinear components of block ciphers are easy to find, Lect. Notes. Comput. Sc., 89 (1989) 612–615.

[122] A. F. Webster, S. Tavares, On the design of nonlinear components of block ciphers, Lect. Notes. Comput. Sc., 85 (1986) 523–534.

[123] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, An efficient method for the construction of block cipher with multi-chaotic systems, Nonlinear Dynam., 71(3) (2013) 489–492.

[124] J. P. Pieprzyk, Non-linearity of Exponent Permutations, Lect. Notes. Comput. Sc., 434 (1990) 80-92.

[125] C. Carlet and K. Feng, An infinite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in Advances in Cryptology-ASIACRYPT 2008 (Lecture Notes in Computer Science), Springer-Verlag, 2008, vol. 5350, pp. 425-440.

[126] Z. Tu and Y. Deng, \A conjecture on binary string and its applications on constructing boolean functions of optimal algebraic immunity," Designs, Codes Cryptogr., 2010. Online First Articles. DOI 10.1007/s10623-010-9413-9.

[127] Q. Wang, J. Peng, H. Kan, and X. Xue, Constructions of cryptographically significant Boolean functions using primitive polynomials," IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 3048-3053, 2010.

[128] Xiaohu Tang, Deng Tang, Xiangyong Zeng and Lei Hu, Balanced Boolean Functions with (Almost) Optimal Algebraic Immunity and Very High Nonlinearity.

[129] P. Stanica, Nonlinearity, local and global avalanche characteristics of balanced Boolean functions, Discr. Math., vol. 248, pp. 181-193, 2002.

[130] P. Stanica, S. H. Sung, Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics, Inf. Process. Lett., vol. 79, pp. 167-172, 2001.

[131] P. Stanica, S. H. Sung, Boolean functions with five controllable cryptographic properties, Des., Codes Cryptogr., vol. 31, no. 2, pp. 147-157, 2004.

[132] W. Diffie and M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644-654.

[133] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (1978), pp. 120-126.

[134] H.C. Williams, A Modification of the RSA Public-Key Encryption Procedure, IEEE Transactions on Information Theory, IT No.6 (26), 1980, pp. 726-729. 1.1

[135] Z. Cao, Conic analog of RSA cryptosystem and some improved RSA cryptosystems, Journal of Natrual Science of Heilongjiang University, 16 (4), 1999. 1.1

[136] Z. Cao, The multi-dimension RSA and its low exponent security, Science in China (E Series), 43 (4): 349-354, 2000.

[137] M.O. Rabin, Digitized signatures and public-key functions as intractible as factorization, MIT Laboratory for Computer Science Technical Report, LCS/TR-212 (1979).

[138] P. Smith and M. Lennon, LUC: A newpublic key system, Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec 93, 103-117, North-Holland, 1993.

[139] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory, 31 (1985), pp. 469-472.

[140] K. Komaya, U. Maurer, T. Okamoto and S. Vanston, New public-key schemes bases on elliptic curves over the ring Z_n, Int. J. Feigenbaum (Ed.): Crypto'91, LNCS 576, Springer-Verlag (1992), pp. 252-266.

[141] P. K. Shau, R. K. Chhotray, Gunamani Jena, S Pattnaik, An Implementation of Elliptic Curve Cryptography, Int. J. Eng. Res. Tech. 2 (2013) 1-8.

[142] C. Cid, S. Murphy, and M.J.B. Robshaw Small Scale Variants of the AES, Proceedings of FSE 2005, LNCS, 2005, 145-162. Springer-Verlag.

[143] Jorge Nakahara Jr, Daniel Santana de Freitas, Mini ciphers: a reliable testbed for cryptanalysis?, "Symmetric Cryptography", Seminar 09031, 2009. Dagstuhl Seminar Proceedings. 1862-4405. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (eds.), Germany.

[144] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher”, The 9th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2007, LNCS 4727, P. Paillier and I. Verbauwhede (eds.), Berlin, Germany: Springer-Verlag, pp. 450-466, 2007.

[145] Mihajloska, H., Gligoroski, D.: Construction of Optimal 4-bit nonlinear components of block ciphers by Quasigroups of Order 4. In: The Sixth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2012, Rome, Italy (2012).

[146] Raphael Chung-Wei Phan; Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students, Published in Cryptologia, XXVI (4), 2002.

[147] Hanem M. El-Sheikh, Omayma A. El-Mohsen, Talaat Elgarf, and Abdelhalim Zekry, A New Approach for Designing Key-Dependent S-Box Defined over $GF(2^4)$ in AES, International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012.

[148] J.C. Interlando, R. Palazzo Jr., M. Elia, On the decoding of Reed-Solomon and BCH codes over integer residue rings, *IEEE Trans. Inform. Theory,* IT-43 (1997) 1013–1021.

[149] Richard Klima, Neil Sigmon, Ernest Stitzinger, Applications of Abstract Algebra with Maple and MATLAB, Chapman and Hall/CRC; 2 edition (July 12, 2006).

[150] Kocarev L., Tasev Z., Public-key encryption based on Chebyshev maps, The 2003 IEEE International Symposium on Circuits and Systems Proceedings, 2003, 28-31.

[151] Pina Bergamo, Paolo D'Arco, Alfredo De Santis, et al., Security of public key cryptosystems based on Chebyshev polynomials, http://citebase.eprints.org, 2004.

[152] D Xiao, X Liao, G Tang, Chuandong Li. Using Chebyshev chaotic map to construct infinite length hash chains, Circuits and Systems, 1 (2004) 11-12.

[153] Xiao Di■ Liao Xiaofeng■ Wong K.W. An efficient entire chaos-based scheme for deniable authentication. Chaos, Solitons and Fractals, 23 (2005) 1327-1331.

[154] Kohda Tohru■ Fujisaki Hirohi. Jacobian elliptic Chebyshev rational maps, Physica D 148 (2001) 242-254.

Turnitin Originality Report

Novel designs of nonlinear component for block ciphers and its applications in diverse security systems by Syed Iram Batool Naqvi

From Thesis Reports (Institutional Repository)

- Processed on 28-Feb-2018 10:35 PKT
- ID: 922708531
- Word Count: 51155

Similarity Index
17%
Similarity by Source

Internet Sources:
12%
Publications:
9%
Student Papers:
5%

sources:

1 1% match (publications)
Majid Khan, Tariq Shah, Syeda Iram Batool. "A new approach for image encryption and watermarking based on substitution box over the classes of chain rings", Multimedia Tools and Applications, 2016

2 1% match (publications)
Khan, Majid, and Tariq Shah. "A copyright protection using watermarking scheme based on nonlinear permutation and its quality metrics", Neural Computing and Applications, 2015.

3 1% match (Internet from 21-Apr-2016)
http://academicjournals.org/journal/IJPS/article-full-text-pdf/E34816025906

4 1% match (publications)
Hussain, Iqtadar, and Tariq Shah. "Literature survey on nonlinear components and chaotic nonlinear components of block ciphers", Nonlinear Dynamics, 2013.

5 1% match (Internet from 27-Oct-2017)
https://link.springer.com/article/10.1007/s00521-014-1800-0

6 < 1% match (publications)
Majid Khan, Tariq Shah. "A Novel Statistical Analysis of Chaotic S-box in Image Encryption", 3D Research, 2014

7 < 1% match (Internet from 02-Mar-2017)
http://crypto.math.uni-bremen.de/Arbeiten/dipljanson.pdf

8 < 1% match (Internet from 14-Apr-2015)
http://airccse.org/journal/ijsptm/papers/3114ijsptm02.pdf

9 < 1% match (Internet from 24-Mar-2016)
http://ijireeice.com/upload/2015/july-15/IJIREEICE%2020.pdf

10 < 1% match (Internet from 01-Apr-2010)
http://www.sis.uncc.edu/~yzheng/publications/files/euroc96-auto-corel-p294.pdf

11 < 1% match (Internet from 10-Nov-2017)
https://link.springer.com/content/pdf/10.1007%2Fs11071-016-3046-0.pdf

12 < 1% match (Internet from 14-Jan-2013)
http://etd.fcla.edu/CF/CFE0000273/Gadkari_Dhanashree_U_200412_MS.pdf

13 < 1% match (Internet from 11-Nov-2013)
http://www.ukessays.com/essays/computer-science/study-on-video-encryption-using-wavelet-transform-computer-science-essay.php

14 < 1% match (student papers from 13-Oct-2017)
Submitted to Campbellsville University on 2017-10-13

15 < 1% match (Internet from 09-Oct-2013) http://www.ijetae.com/files/Volume3Issue4/IJETAE_0413_41.pdf

16 < 1% match (Internet from 04-Jun-2017)
http://eprints.qut.edu.au/16023/1/Linda_Burnett_Thesis.pdf

17 < 1% match (Internet from 15-May-2016)
http://research.ijcaonline.org/volume79/number9/pxc3891620.pdf

18 < 1% match (Internet from 02-May-2016)
http://www.jucs.org/jucs_4_8/on_cryptographic_properties_of

19 < 1% match (Internet from 08-Jul-2015)
http://www.researchgate.net/publication/266489894_Statistical_analysis_of_S-box_in_image_encryption_applications_based_on_majority_logic_criterion

20 < 1% match (Internet from 29-Aug-2015)
http://www.tceic.com/1l5892j53186hikh19k8hhg5.html

21 < 1% match (student papers from 29-Jul-2017)
Submitted to Manipal University on 2017-07-29

22 < 1% match (publications)
Pasalic, E.. "New Constructions of Resilient and Correlation Immune Boolean Functions Achieving Upper Bound on Nonlinearity", Electronic Notes in Discrete Mathematics, 200104

23 < 1% match (Internet from 07-Apr-2009)
http://www.ualr.edu/xxliu/log_SBox.pdf

24 < 1% match (Internet from 20-Sep-2013)
http://eprint.iacr.org/2010/443.pdf

25 < 1% match (Internet from 21-Apr-2010)
http://www.iacr.org/archive/crypto2000/18800516/18800516.pdf

26 < 1% match (Internet from 25-May-2008)
http://www.jucs.org/jucs_2_3/on_the_difficulty_of/Zhang_X.pdf

27 < 1% match (student papers from 21-Jan-2015)
Submitted to Gulf University on 2015-01-21

28 < 1% match (Internet from 03-Dec-2016)
https://pdfs.semanticscholar.org/1e84/e598601a6cc42526bb93aec2dd5b5101ecac.pdf

29 < 1% match (publications)
Khan, Majid, and Tariq Shah. "An efficient chaotic image encryption scheme", Neural Computing and Applications, 2015.

30 < 1% match (Internet from 08-Nov-2003)
http://preterhuman.net/texts/cryptology/NONLINEA.PDF

31 < 1% match (publications)
Hussain, Iqtadar, Tariq Shah, Muhammad Asif Gondal, and Hasan Mahmood. "A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence", Nonlinear Dynamics, 2013.

32 < 1% match (student papers from 31-Jan-2018)
Submitted to Chandigarh University on 2018-01-31

33 < 1% match (Internet from 11-Jun-2009)
http://www.maths.uq.edu.au/courses/MATH3302/files/cryptonotes.pdf

34 < 1% match (publications)
Shah, Tariq, Nasir Mehmood, Antonio Aparecido de Andrade, and Reginaldo Palazzo. "Maximal cyclic subgroups of the groups of units of Galois rings: a computational approach", Computational and Applied Mathematics, 2015.

35 < 1% match (Internet from 14-Oct-2013)
http://www.uio.no/studier/emner/matnat/ifi/INF4300/h08/undervisningsmateriale/glcm.pdf

36 < 1% match (Internet from 21-Mar-2016)
http://jocpr.com/vol6-iss3-2014/JCPR-2014-6-3-90-101.pdf

37 < 1% match (Internet from 22-Mar-2016)
http://www.m-hikari.com/ijcms-2010/25-28-2010/hussainIJCMS25-28-2010.pdf

38 < 1% match (student papers from 16-Feb-2016)
Submitted to Middle Technical University on 2016-02-16

39 < 1% match (publications)
Iqtadar Hussain. "A projective general linear group based algorithm for the construction of substitution box for block ciphers", Neural Computing and Applications, 02/16/2012

40 < 1% match (publications)
Alqahtani, Ali. "An efficient approach to design confusion creating component and its analyses using majority logic criterion", International Journal of Dynamical Systems and Differential Equations, 2016.

41 < 1% match (student papers from 23-Mar-2015)
Submitted to SASTRA University on 2015-03-23

42 < 1% match (student papers from 21-Aug-2016)
Submitted to University of Kufa on 2016-08-21

43 < 1% match (Internet from 07-May-2016)
http://airccse.org/journal/jcsit/4612ijcsit13.pdf

44 < 1% match (Internet from 30-Oct-2013)
http://explorable.com/statistical-analysis

45 < 1% match (publications)
Khan, Majid, Tariq Shah, and Syeda Iram Batool. "Construction of S-box based on chaotic Boolean functions and its application in image encryption", Neural Computing and Applications, 2015.

46 < 1% match (student papers from 24-Dec-2015)
Submitted to Savitribai Phule Pune University on 2015-12-24

47 < 1% match (Internet from 19-Jan-2010)
http://www.inf.teilam.gr/staff/KARKANIS/CPIMB.pdf

48 < 1% match (Internet from 05-Jul-2013)
http://yarrg.chiark.net/RSYNC/OCEAN-Cerulean.db

49 < 1% match (Internet from 26-May-2012)
http://www.ejournal.aessangli.in/ASEEJournals/CE10.doc

50 < 1% match (publications)
Lecture Notes in Computer Science, 2000.

51 < 1% match (student papers from 05-May-2012)
Submitted to Swansea Metropolitan University on 2012-05-05

52 < 1% match (Internet from 10-May-2010)
http://www.cstp.umkc.edu/~dmedhi/papers/hm-tissec-2004.pdf

53 < 1% match (student papers from 29-Nov-2015)
Submitted to ABA-An IB World School on 2015-11-29

54 < 1% match (Internet from 01-Dec-2017)
https://link.springer.com/content/pdf/10.1007%2Fs11071-014-1767-5.pdf

55 < 1% match (publications)
Zeng, Guoping. "A unified definition of mutual information with applications in machine learning.(Research Article)(", Mathematical Problems in Engineering, Annual 2015 Issue

< 1% match (publications)

56 Aliwa, Mehemed Bashir. "A New Novel Fidelity Digital Watermarking Based on Adaptively Pixel-Most-Significant- Bit-6 in Spatial Domain Gray Scale Images and Robust", American Journal of Applied Sciences/15469239, 20100701

57 < 1% match (Internet from 14-Aug-2014)
http://www.slideshare.net/romeo98765/applied-numerical-methods-using-matlab-wiley2005

58 < 1% match (Internet from 09-Sep-2010)
http://www.ieindia.org/publish/et/0104/jan04et5.pdf

59 < 1% match (student papers from 20-Oct-2017)
Submitted to University of the Western Cape on 2017-10-20

60 < 1% match (Internet from 22-Mar-2016)
http://ijarcsse.com/docs/papers/Volume_4/5_May2014/V4I5-0271.pdf

61 < 1% match (Internet from 09-Mar-2016)
http://ethesis.nitrkl.ac.in/5230/1/211EE1143.pdf

62 < 1% match (Internet from 26-Dec-2017)
http://perso.telecom-paristech.fr/~flori/thesis/thesis.pdf

63 < 1% match (student papers from 01-Jul-2017)
Submitted to Thapar University, Patiala on 2017-07-01

64 < 1% match (student papers from 20-Aug-2014)
Submitted to Imperial College of Science, Technology and Medicine on 2014-08-20

65 < 1% match (Internet from 18-Mar-2015)
http://hippocampus.si/ISBN/978-961-6832-92-2.pdf

66 < 1% match (Internet from 18-Nov-2014)
http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-5-167-171.pdf

67 < 1% match (Internet from 08-Jan-2007)
http://www.comm.uqam.ca/~profil/meta/DildoDoll/DilDoll_multi_work%201

68 < 1% match (publications)
Majid Khan, Zeeshan Asghar. "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation", Neural Computing and Applications, 2016

69 < 1% match (publications)
Jamal, Sajjad Shaukat, Muhammad Usman Khan, and Tariq Shah. "A Watermarking Technique with Chaotic Fractional S-Box Transformation", Wireless Personal Communications, 2016.

70 < 1% match (publications)
Belazi, Akram, Ahmed A. Abd El-Latif, Adrian-Viorel Diaconu, Rhouma Rhouma, and Safya Belghith. "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms", Optics and Lasers in Engineering, 2017.

71 < 1% match (student papers from 11-Oct-2016)
Submitted to Heriot-Watt University on 2016-10-11

72 < 1% match (Internet from 22-Mar-2016)
http://ijarcsse.com/docs/papers/Volume_4/1_January2014/V4I1-0302.pdf

73 < 1% match (Internet from 10-Mar-2016)
http://archive.mu.ac.in/myweb_test/S.Y.B.Sc.IT.%20%28Sem%20-%20III%29%20Logic%20and%20Discrete%20Mathematics.pdf

74 < 1% match (Internet from 12-Dec-2007)
http://en.wikipedia.org/wiki/Rijndael_S-box

75 < 1% match (publications)
Anees, Amir, and Muhammad Asif Gondal. "Construction of Nonlinear Component for Block Cipher Based on One-Dimensional Chaotic Map", 3D Research, 2015.

76 < 1% match (student papers from 30-Sep-2016)
Submitted to Pacific University on 2016-09-30

77 < 1% match (Internet from 22-Sep-2017)
https://springerplus.springeropen.com/articles/10.1186/s40064-016-3298-7

78 < 1% match (Internet from 16-Jun-2015)
http://www.nbhkdz.com/read/0bff02583ae581c21e7a5bd3.html

79 < 1% match (Internet from 13-Jan-2007)
http://www.ce.org/shared_files/div_comm_docs/100_740e_NP.pdf

80 < 1% match (publications)
Iqtadar Hussain. "A group theoretic approach to construct cryptographically strong substitution boxes", Neural Computing and Applications, 04/06/2012

81 < 1% match (Internet from 05-Nov-2017)
http://www.math.univ-paris13.fr/~carlet/pubs.html

82 < 1% match (Internet from 03-Dec-2015)
http://deepblue.lib.umich.edu/bitstream/handle/2027.42/97857/pgarias_1.pdf?sequence=1

83 < 1% match (Internet from 14-Jun-2013)
http://iosrjournals.org/iosr-jce/papers/Vol6-Issue1/F0613641.pdf

84 < 1% match (publications)
"Soft Computing: Theories and Applications", Springer Nature, 2018

85 < 1% match (Internet from 06-Sep-2017)
http://www.canberra.edu.au/researchrepository/file/374a96ec-6d48-45d7-8dac-8516e361f504/1/full_text.pdf

86 < 1% match (Internet from 15-Jul-2017)
http://mobile.repository.ubn.ru.nl/bitstream/handle/2066/141872/141872.pdf?sequence=1

87 < 1% match ()
http://numerik.math.uni-duisburg.de/people/nemitz/diplom/diplomarbeit.pdf

88 < 1% match (publications)
John A. Clark. "Evolving Boolean Functions Satisfying Multiple Criteria", Lecture Notes in Computer Science, 2002

89 < 1% match (publications)
Khan, Majid, and Tariq Shah. "An efficient construction of substitution box with fractional chaotic system", Signal Image and Video Processing, 2015.

90 < 1% match (publications)
Zheng, Y.. "Connections among nonlinearity, avalanche and correlation immunity", Theoretical Computer Science, 20030131

91 < 1% match (Internet from 01-Apr-2010)
http://www.sis.uncc.edu/~yzheng/publications/files/crypto94-pitfalls-p383.pdf

92 < 1% match (Internet from 31-Oct-2016)
https://www.coursehero.com/file/15199308/ChenGongbookApril2012pdf/

93 < 1% match (Internet from 16-Aug-2014)
http://tastyspleen.net/~quake2/baseq2/maps/other.bsp

94 < 1% match (Internet from 25-Aug-2014)
http://jda.noekeon.org/JDA_VRI_Stat_2007.pdf

95 < 1% match (Internet from 03-Nov-2012)
http://www.info.big-tits-teens.info/read/Permutation_matrix

96 < 1% match (student papers from 01-Sep-2013)
Submitted to Institute of Technology, Nirma University on 2013-09-01

97
< 1% match (student papers from 08-May-2015)
Submitted to Univerza v Ljubljani on 2015-05-08

98
< 1% match (Internet from 02-Nov-2017)
http://drops.dagstuhl.de/opus/volltexte/2016/6906/pdf/lipics-vol64-isaac2016-complete.pdf

99
< 1% match ()
http://www.xris.de/Informatik/UniquenessConstraints.pdf

100
< 1% match (Internet from 29-Jan-2016)
http://eprints.uthm.edu.my/6932/1/ABDULLAHI_MOHAMUD_HASSAN.pdf

101
< 1% match (Internet from 22-Mar-2016)
http://www.m-hikari.com/ces/ces2015/ces29-32-2015/p/deviCES29-32-2015.pdf

102
< 1% match (publications)
Maitra, S.. "Highly Nonlinear Balanced Boolean Functions with Very Good Autocorrelation Property", Electronic Notes in Discrete Mathematics, 200104

103
< 1% match (publications)
E. Pasalic. "Maiorana–McFarland Class: Degree Optimization and Algebraic Properties", IEEE Transactions on Information Theory, 10/2006

104
< 1% match (student papers from 21-Mar-2016)
Submitted to The University of Buckingham on 2016-03-21

105
< 1% match (Internet from 05-May-2016)
http://www.arpnjournals.com/jeas/research_papers/rp_2015/jeas_0615_2186.pdf

106
< 1% match (Internet from 12-Feb-2014)
http://www.aam.org.in/site/st_material/ebook.pdf

107
< 1% match (Internet from 08-Jan-2015)
http://vanilla47.com/PDFs/Cryptography/Cryptography/HANDBOOK_of_APPLIED_CRYPTOGRAPHY.pdf

108
< 1% match (Internet from 24-Jun-2016)
https://linknovate.com/publication/statistical-analysis-of-s-box-in-image-encryption-applications-based-on-majority-logic-criterion-3029491/

109
< 1% match (Internet from 07-Sep-2017)
http://openaccess.city.ac.uk/15498/1/ICC2016.pdf

110
< 1% match (Internet from 30-Jan-2004)
http://www.cand-merc.dk/staff/hzh/hzh_phd.pdf

111
< 1% match (student papers from 03-Aug-2016)
Submitted to The University of Buckingham on 2016-08-03

112
< 1% match (student papers from 31-Aug-2015)
Submitted to University of South Alabama on 2015-08-31

113
< 1% match (Internet from 26-Nov-2016)
https://zenodo.org/record/32256/files/ImageDeNoisingTechnique.pdf

114
< 1% match (Internet from 04-Mar-2017)
http://sciencepublishinggroup.com/journal/paperinfo?doi=10.11648%2Fj.es.20160101.12&journalid=619

115
< 1% match (Internet from 03-Apr-2017)
http://www-users.cs.york.ac.uk/~jac/PublishedPapers/COIN04-Clark-Maitra-Stanica.pdf

116
< 1% match (student papers from 15-Jun-2010)
Submitted to De Montfort University on 2010-06-15

117
< 1% match (publications)

Lecture Notes in Computer Science, 2003.

118 < 1% match (publications)
T. G. S., Chandrasekharappa. "S-boxes generated using Affine Transformation giving Maximum Avalanche Effect", International Journal on Computer Science & Engineering/09753397, 20110901

119 < 1% match (student papers from 16-Jan-2017)
Submitted to Universiti Teknologi MARA on 2017-01-16

120 < 1% match (student papers from 01-Jun-2017)
Submitted to Government College of Engineering Aurangabad, Maharashtra State, India on 2017-06-01

121 < 1% match (student papers from 11-May-2017)
Submitted to Wittenborg University on 2017-05-11

122 < 1% match (Internet from 15-Mar-2014)
http://cmsim.org/images/1_ProceedingsCHAOS2013_S-T_pp_583-694.pdf

123 < 1% match (Internet from 19-Mar-2010)
http://www.sis.uncc.edu/~yzheng/publications/files/crypt93-nl-p49.pdf

124 < 1% match (Internet from 07-Feb-2017)
http://spectrum.library.concordia.ca/976237/1/MR63241.pdf

125 < 1% match (publications)
Communications in Computer and Information Science, 2013.

126 < 1% match (publications)
Hussain, Iqtadar, Muhammad Asif Gondal, and Azkar Hussain. "Construction of Substitution Box Based on Piecewise Linear Chaotic Map and S8 Group", 3D Research, 2015.

127 < 1% match (student papers from 16-Jun-2014)
Submitted to Indian Institute of Technology, Kharagpure on 2014-06-16

128 < 1% match (student papers from 11-Feb-2015)
Submitted to iGroup on 2015-02-11

129 < 1% match (student papers from 08-Jun-2015)
Submitted to Gunn High School on 2015-06-08

130 < 1% match (Internet from 28-Sep-2016)
https://www.scribd.com/document/281641706/Handbook-of-Finite-Fields

131 < 1% match (Internet from 23-Dec-2014)
http://www.ecti-thailand.org/assets/papers/242_pub_17.pdf

132 < 1% match (Internet from 04-Jun-2017)
http://eprints.qut.edu.au/15828/1/Joanne_Fuller_Thesis.pdf

133 < 1% match (Internet from 12-Nov-2017)
https://link.springer.com/content/pdf/10.1007%2Fs11227-009-0304-7.pdf

134 < 1% match (publications)
Hussain, Iqtadar, Tariq Shah, Muhammad Asif Gondal, and Hasan Mahmood. "A novel image encryption algorithm based on chaotic maps and GF(28) exponent transformation", Nonlinear Dynamics, 2013.

135 < 1% match (student papers from 25-Apr-2008)
Submitted to University of Warwick on 2008-04-25

136 < 1% match (student papers from 30-Apr-2014)
Submitted to Feng Chia University on 2014-04-30

137 < 1% match (student papers from 30-Nov-2012)
Submitted to Universiti Teknologi Malaysia on 2012-11-30

138 < 1% match (student papers from 24-Oct-2017)
Submitted to SASTRA University on 2017-10-24

139 < 1% match (Internet from 16-Mar-2017)
http://www.imedpub.com/articles/utilization-of-edge-position-for-digital-image-watermarking-using-discriminant-analysis.pdf

140 < 1% match (Internet from 10-Sep-2009)
http://www.cns.nyu.edu/~zwang/files/papers/vssim.pdf

141 < 1% match (Internet from 14-Aug-2008)
http://live.ece.utexas.edu/publications/2007/eetimes.pdf

142 < 1% match (Internet from 20-Jun-2017)
http://www.dtic.mil/dtic/tr/fulltext/u2/a574590.pdf

143 < 1% match (Internet from 12-Mar-2016)
http://eprints.maynoothuniversity.ie/736/1/paperOI.pdf

144 < 1% match (Internet from 12-Jan-2015)
http://195.144.0.229/content/equations-theory-of/239300

145 < 1% match (Internet from 01-Oct-2003)
http://ads.texmate.com/pdf/144/UM-35P_(UM09)L9-10-03.pdf

146 < 1% match (Internet from 21-Apr-2003)
http://www-ma2.upc.es/~cripto/Q1-01-02/des+aes.pdf

147 < 1% match (publications)
Atta Ullah, Sajjad Shaukat Jamal, Tariq Shah. "A novel scheme for image encryption using substitution box and chaotic system", Nonlinear Dynamics, 2017

148 < 1% match (publications)
Ullah, Ehsan . "New Techniques for Polynomial System Solving", Universitätsbibliothek Passau, 2012.

149 < 1% match (publications)
Su, Bai Yun, Gang Xu, Geng Zhao, and Yang Liao. "A Method for Obtaining Chaos-Based S-Box via a PWLCM", Advanced Materials Research, 2013.

150 < 1% match (student papers from 19-Aug-2010)
Submitted to Universiti Kebangsaan Malaysia on 2010-08-19

151 < 1% match (Internet from 05-May-2016)
http://www.rroij.com/open-access/extensive-experimental-analysis-of-image-statistical-measures-for-image-processing-appliances-.pdf

152 < 1% match (Internet from 07-May-2009)
http://www-users.cs.york.ac.uk/~jac/PublishedPapers/ResultsOnROTSFSE2004.pdf

153 < 1% match (Internet from 29-May-2016)
http://nte-serveur.univ-lyon1.fr/nte/immediato/Math/Enseignement/Manuscrits/Quelques%20remarques%20sur%20les%20%E9quations%20de%20r%E9currenc

154 < 1% match ()
http://pastel.paristech.org/archive/00000840/01/Leveiller_these.pdf

155 < 1% match (Internet from 24-Aug-2016)
https://www.coursehero.com/file/9801152/Handbook-of-Applied-Cryptography-A-Menezes-P-VanOorschot-S-Vanstone/

156 < 1% match (Internet from 27-May-2016)
https://data.cms.gov/Medicare/Provider-of-Services-File-OTHER-June-2013/re8s-thbg/alt?page=88

157 < 1% match ()
http://lcawww.epfl.ch/Publications/Vojnovic/TR99_024.pdf

158 < 1% match (Internet from 03-Jul-2003)
http://rockshi.nethome.com.cn/files/nextxzt2.htm

159 < 1% match (publications)
S. Maitra. "Further constructions of resilient Boolean functions with very high nonlinearity", IEEE Transactions on Information Theory, 7/2002

160 < 1% match (Internet from 07-Jun-2016)
http://srd.kku.edu.sa/sites/srd.kku.edu.sa/files/general_files/files/%D9%83%D8%AA%D9%8A%D8%A8%20%D9%8A%D9%88%D9%85%

161 < 1% match (Internet from 23-Feb-2016)
http://dyuthi.cusat.ac.in/xmlui/bitstream/handle/purl/3892/Dyuthi-T1784.pdf?sequence=1

162 < 1% match (Internet from 27-Jan-2016)
http://ojs.academypublisher.com/index.php/jsw/article/download/0507777784/1958

163 < 1% match (Internet from 20-Apr-2010)
http://eprint.iacr.org/2009/134.pdf

164 < 1% match (Internet from 20-Feb-2017)
https://espace.curtin.edu.au/bitstream/handle/20.500.11937/2510/190335_Nordin2011.pdf?isAllowed=y&sequence=2

165 < 1% match (Internet from 06-Oct-2013)
http://ijens.org/1964091%20IJVIPNS.pdf

166 < 1% match (Internet from 05-Feb-2013)
http://welcome.isr.ist.utl.pt/img/pdfs/2653_Tarapore_Alife2012.pdf

167 < 1% match (Internet from 30-Dec-2017)
http://scholarbank.nus.edu.sg/bitstream/10635/122604/1/GuCJ.pdf

168 < 1% match (Internet from 04-Dec-2011)
http://coitweb.uncc.edu/~yzheng/publications/files/dcc2k-1.pdf

169 < 1% match (Internet from 10-Jun-2008)
http://th-www.if.uj.edu.pl/acta/vol32/ps/v32p0669.ps.gz

170 < 1% match (Internet from 18-Jun-2017)
http://www.cs.rug.nl/~petkov/publications/ieee-tip1999.pdf

171 < 1% match (Internet from 04-Jun-2015)
http://nptel.ac.in/courses/IIT-MADRAS/Machine_Design_II/pdf/5_4.pdf

172 < 1% match (publications)
Gulve, Avinash K. Joshi, Madhuri S.. "An image steganography method hiding secret data into coefficients of integer wavelet transform usin", Mathematical Problems in Engineering, Annual 2015 Issue

173 < 1% match (Internet from 15-Dec-2014)
http://www.docstoc.com/docs/10572164/DIGITAL-IMAGE-PROCESSING

174 < 1% match (Internet from 26-Nov-2017)
https://link.springer.com/content/pdf/10.1007%2F978-0-387-09823-4.pdf

175 < 1% match (Internet from 14-Nov-2017)
https://link.springer.com/content/pdf/10.1007%2F978-3-642-34961-4.pdf

176 < 1% match (Internet from 12-Sep-2010)
http://www1.spms.ntu.edu.sg/~kkhoongm/chap-fcts-Bool.pdf

177 < 1% match (Internet from 07-Sep-2017)
https://www.rocq.inria.fr/secret/Pascale.Charpin/encyclopedia-tout.pdf

178 < 1% match (Internet from 19-Jan-2015)
http://pselab.ru/Books/Allen.pdf

179 < 1% match (Internet from 24-Nov-2012)
http://www.ijetae.com/files/Issue1/IJETAE_1111_05.pdf

180 < 1% match (Internet from 24-Oct-2003)
http://buhafiles.net/download/krypto/my_phd.pdf

181 < 1% match (Internet from 06-Jul-2017)
http://academic.odysci.com/article/1010113017217107/gray-image-extraction-using-fuzzy-logic

182 < 1% match (Internet from 29-Jan-2016)
http://www.academypublisher.com/jmm/vol08/no03/jmm0803.pdf

183 < 1% match (Internet from 28-Mar-2012)
http://www.11articles.com/noreg/?g1

184 < 1% match (Internet from 05-Nov-2009)
http://groups.csail.mit.edu/cag/pub/papers/pdf/dann-thesis.pdf

185 < 1% match (Internet from 26-Feb-2015)
http://geo.citg.tudelft.nl/broere/pdf/broere_phdthesis.pdf

186 < 1% match (Internet from 12-Apr-2016)
http://epubl.ltu.se/1402-1617/2007/266/LTU-EX-07266-SE.pdf

187 < 1% match (Internet from 17-Mar-2016)
http://www.ijcaonline.org/volume12/number5/pxc3872252.pdf

188 < 1% match (Internet from 02-Nov-2013)
http://www.ijcncs.org/published/volume1/issue3/p3_1-3.pdf

189 < 1% match (Internet from 27-Jan-2016)
http://autoidlab.cs.adelaide.edu.au/sites/default/files/thesis/matheu_Thesis.pdf

190 < 1% match (Internet from 08-Jun-2015)
http://www.unicode.org/L2/L2001/01106-1923rev.pdf

191 < 1% match (Internet from 27-Jul-2007)
http://www.ecrypt.eu.org/documents/D.STVL.4-1.0.pdf

192 < 1% match (Internet from 23-Jan-2018)
https://hal.archives-ouvertes.fr/tel-01565037v1/html_references

193 < 1% match (Internet from 09-Mar-2010)
http://www.cis.fiu.edu/mipr05/review/papers/19_Potdar_Comparative%20Study%20of%20Binary%20Watermarks.pdf

194 < 1% match (Internet from 10-Feb-2004)
http://www.ii.uib.no/~matthew/ConstaBent2.pdf

195 < 1% match (Internet from 16-Jan-2010)
http://www.stork.eu.org/documents/ENS-D4-1_4.pdf

196 < 1% match (Internet from 25-Jan-2014)
http://www.enggjournals.com/ijcse/doc/IJCSE11-03-09-138.pdf

197 < 1% match (publications)
Pascale Charpin. "On Propagation Characteristics of Resilient Functions", Lecture Notes in Computer Science, 2003

198 < 1% match (publications)
Gang Xu. "The Design of dynamical S-boxes based on discrete chaos map system", 2009 IEEE International Conference on Intelligent Computing and Intelligent Systems, 11/2009

199 < 1% match (publications)

Attaullah, Sajjad Shaukat Jamal, Tariq Shah. "A Novel Algebraic Technique for the Construction of Strong Substitution Box", Wireless Personal Communications, 2017

200 < 1% match (publications)
P.X. Yu, Z.F. Tian, A.Y. Ying, M.A. Abdou. "Stream function-velocity-magnetic induction compact difference method for the 2D steady incompressible full magnetohydrodynamic equations", Computer Physics Communications, 2017

201 < 1% match (publications)
Kuppusamy, Arulmani Iyer, Swaminathan Pi. "Two-key dependent permutation for use in symmetric cryptographic system.(Research Article)(Report)", Mathematical Problems in Engineering, Annual 2014 Issue

202 < 1% match (publications)
C. Carlet. "On the algebraic thickness and non-normality of Boolean functions", Proceedings 2003 IEEE Information Theory Workshop (Cat No 03EX674) ITW-03, 2003

203 < 1% match (student papers from 16-Nov-2017)
Submitted to Savitribai Phule Pune University on 2017-11-16

204 < 1% match (student papers from 14-Nov-2015)
Submitted to Asia Pacific University College of Technology and Innovation (UCTI) on 2015-11-14

205 < 1% match (student papers from 29-May-2012)
Submitted to Acharya Nagarjuna University on 2012-05-29

206 < 1% match (student papers from 18-Jan-2017)
Submitted to Indian Institute of Technology, Madras on 2017-01-18

207 < 1% match (publications)
"Data Engineering and Intelligent Computing", Springer Nature, 2018

208 < 1% match (publications)
Lecture Notes in Computer Science, 2001.

209 < 1% match (publications)
Lecture Notes in Computer Science, 2015.

paper text:

NOVEL DESIGNS OF NONLINEAR COMPONENT FOR BLOCK CIPHERS AND ITS APPLICATIONS IN DIVERSE SECURITY SYSTEMS by Syeda Iram Batool Naqvi

78**Submitted to the Department of Mathematics on** February 28, 2018, **in partial fulfillment of the requirements for the degree of Doctor of Philosophy**

Abstract

The improvement of the web make individuals bit by bit acquainted with transmit computer- ized data through different systems, the data incorporate content, advanced pictures and sight and sound data, and so on. Due to the extensive scale use of sight and sound innovation, advanced pictures turn into a critical method for correspondence. It is frequently evident that an expansive piece of this data is either classified or private. Therefore, extraordinary security procedures have been utilized to give the required insurance. With the headways of media and systems advances, an immense number of computerized pictures now transmitted over the Internet and through remote systems for advantageous getting to and sharing. Sight and sound security, as a rule, is given by a technique or an arrangement of strategies used to ensure the interactive media content. These days, we are living in a time where data is the extremely significant asset to us. Subsequently securing the data turns into all the more important. The correspondence media through which we send information does not give information security, so different techniques for securing information are required. Data hiding/stowing away assumes an exceptionally critical part today. It gave techniques to encoding the data with the goal that it winds up muddled for any unintended client. There are three noteworthy data concealing methods to be specific watermarking, cryptography and steganography. Crypt means “hidden or secret” and graphein means “writing”. The term has been gotten from Greek dialect. Cryptography is a craft of changing information into a mixed up arrange called ciphertext. The recipient at another side, interprets or unscramble the message into plain content. Cryptography gives information secrecy, information uprightness, validation, and non-denial. Secrecy is constraining access or setting the confinement on specific sorts of data. Honesty is keeping up and guaranteeing the exactness of information being conveyed, i.e, the data contains no adjustment, erasure and so forth. Verification guarantees the character of sender and beneficiary of the data. Non-disavowal is the capacity to guarantee that the sender or beneficiary can’t preclude the legitimacy from securing their mark on the sending data that they started. A watermark is a conspicuous picture or example that is inspired onto paper, which gives con…rmation of its validness. Watermark shows up as di¤erent shades of softness/obscurity when seen in transmitted light. Watermarks are regularly observed as security highlights to banknotes, identi…cations, postage stamps and other security papers. Computerized water- marking is an augmentation of this idea in the advanced world. Today there have been such a large amount of information over the web that it has constrained us to utilize systems that can secure responsibility for media. Robbery of computerized data is exceptionally normal, be it pictures, content, sound or video. These can be delivered and circulated e¤ectively. Along these lines, it turns out to be critical to discover who is the proprietor of the report. Computerized watermarking is a standout amongst other answers for avoid illicit duplicating, altering and re-distributing mixed media information. Encryption of sight and sound items keeps an interloper from getting to the substance without a legitimate unscrambling key. Yet, once the informa- tion is unscrambled, it can be copied and dispersed illicitly. Copyright insurance, information veri…cation, secretive correspondence and substance ID can be accomplished by advanced wa- termarking. Computerized watermarking is a system to implant copyright or other data into the fundamental information. The implanted information ought to keep up the nature of the host ‡ag. An advanced watermark is an example of bits embedded into a computerized picture, sound and video record that recognizes the document's copyright data. Watermarking procedures is to give a proof of responsibility for information by inserting copyright articulations into a video or into a computerized picture. Watermarking convey an assortment of procedures how to stow away critical data, in an imperceptible as well as irremov- able route, in a picture sound and video information. Watermarking are principle parts of the quick creating region of data covering up. Watermarking is an entirely unexpected method from cryptography. Cryptography just gives security by encryption and unscrambling. Dissimilar to Cryptography, watermarks can ensure content even after they are decoded. Computerized watermarking has gotten signi…cant consideration as a supplement to cryptography for the security of advanced substance, for example, music, video, and pictures. Cryptography gives a way to secure conveyance of substance to the buyer. True blue shoppers are expressly or certainly given a key to unscramble the substance so as to view or hear it out. Strikingly, steganography receives a substitute methodology disconnected from everything the evidence that even a correspondence is happening. Steganography is changing the photo in a way that selects the sender and the proposed recipient can perceive the message sent through it. It is imperceptible, and in this way, the revelation isn't basic. It is a prevalent technique for sending secret messages than encoded messages or cryptography as it doesn't pull in respect for itself. The information concealed by a watermarking structure is always identi…ed with the propelled question be guaranteed or to its proprietor

56**while steganographic systems** basically cover **any information.** The quality **criteria are** similarly extraordinary **since steganography**

is generally stressed over the revelation of the covered

56**message while watermarking concerns potential** ejec- tion **by a**

privateer. The steganographic exchanges are ordinarily point-to-point (among sender and bene…ciary) while watermarking techniques are regularly one-to-many. This thesis mainly concern about cryptography, watermarking and steganographic tech- niques. The construction of di¤erent techniques in cryptography, watermarking and steganog- raphy is always been open task. Theses construction involves various mathematical structures which includes Boolean functions, …nite Galois …eld and Galois ring. The construction of an important nonlinear component of block cipher namely substitution boxes are based on Boolean functions. The nonlinear component simply provides confusion capability in any information hiding techniques which is a fundamental component while constructing strong block cipher according to the Shannon theory of confusion and di¤usion. Our main concern here is to pro- pose new algorithms for the construction of nonlinear component and utilize these in diverse multimedia applications. The

23**basic cryptographic properties of S-boxes are** discussed **in** chap- ter 1. **The**

construction of new small S-boxes based watermarking and steganographic schemes were designed in chapters 2, 3 and 4 respectively. The cryptographic algebraic analyses play a vital role in order to test the validity of any component of block cipher speci…cally S-boxes. Moreover, there are several cryptographically strong algebraic analyses were developed in liter- ature. Keeping in view the importance of these analyses, we have also tried to design a novel and innovative cryptographic analyses to check the strength of any S-boxes in chapter 5. The idea of Galois …eld is then replaced with Galois ring for the construction of strong S-boxes. The technique of chapter 6 is an innovative in the area of cryptographic algorithms development. The highly nonlinear Boolean functions observed in this construction which break the existing upper bound on nonlinearity of Boolean functions. Moreover, these functions are less balanced and more non balanced which qualify these Boolean functions to be near to bent Boolean func- tions. The idea of symmetric group S8 is applied to S-box based on which consequently generate 8! new S-boxes which surely add confusion capability in each frame of the proposed video en- cryption techniques. This novel and e¢ cient video encryption technique is formally presented in chapter 7. The idea of more than one key is used in public key cryptography where various algorithms were developed already in literature whereas the single key based algorithms use only confusion and di¤usion principles. In this sequel, the novel public-key cryptosystem that uses large abelian subgroup of general linear group of units of local ring of degree 2 is developed for di¤erent set of plaintext i-e., and in chapter 8. Moreover in chapter 8, based on general linear group, we have extended Di¢ e Hellman key exchange algorithm over matrices by incorporating chebyshev polynomials of …rst and second kind. Finally, the conclusions with future directions and recommendation are given in chapter 9. Contents 1 Preliminaries of Boolean Functions and Data Security 12 1.1 Review on

62**Boolean Functions in Cryptography** . . . . 15 **1.1.** 1 **Cryptographic** Desirable Characteristics of **Boolean Functions** . . . . 15 **1.**

2 Nonlinear Component of Block Ciphers (S-Box) . . . . 19 1.2.1 De…nition of Nonlinear Component and Types . . . . 19 1.2.2 Cryptographic Possessions of Nonlinear Components . . . . 20 1.3 Review on Information Security Preliminaries . . . . 24 1.4 Cryptology . . . . 26 1.4.1 Classi…cation of Cryptology . . . . 26 1.4.2 Basics Terminology of Cryptography . . . . 27 1.5 Prime Security Purposes of Cryptography . . . . 29 1.5.1 Con…dentiality . . . . 29 1.5.2 Data Integrity . . . . 29 1.5.3 Authentication . . . . 29 1.5.4 Non-repudiation . . . . 30 1.6 1.7 Cryptographic Essentials . . . . 30 Classi…cation of Cryptographic Algorithms . . . . 31 1.7.1 Private/Secret Key Cryptography . . . . 32 1.7.2 Public Key Cryptography . . . . 32 1.7.3 Hash Function . . . . 32 1.7.4 Di¤usion and Confusion . . . . 33 1.7.5 Digital image processing . . . . 34 1.8 Basics of Watermarking . . . . 35 1.9 Digital Watermarking . . . . 36 1.9.1 Basic Terminologies of Watermarking . . . . 36 1.9.2 Qualities of Computerized Watermarking . . . . 37 1.10 Watermarking Attacks . . . . 38 1.10.1 Elimination Attack . . . . 39 1.10.2 Intrusion Assault . . . . 39 1.10.3 Shapes Attacks . . . . 39 1.10.4 Security Attack . . . . 39 1.10.5 Protocol Attack . . . . 39 1.10.6 Cryptographic Assaults . . . . 40 1.10.7 Dynamic Attacks . . . . 40 1.10.8 Passive Attacks . . . . 40 1.10.9 Collusion Attacks . . . . 40 1.10.10 Digital Image Degradation . . . . 41 1.10.11 Image Augmentation . . . . 41 1.10.12 Image Firmness . . . . 41 1.10.13 Image Alterations . . . . 41 1.11 Watermarking Applications . . . . 42 1.11.1 Secretive Correspondence . . . . 43 1.11.2 Communicate Scrutiny . . . . 43 1.11.3 Proprietor Recognizable Proof . . . . 43 1.11.4 Con…rmation of Possession . . . . 44 1.11.5 Veri…cation . . . . 44 1.11.6 Value-based Watermarks . . . . 45 1.11.7 Reproduction Controller . . . . 46 1.12 Classi…cation of Computerized/Digital Watermarking . . . . 46 1.13 Steganography . . . . 47 1.13.1 Applications of Steganography . . . . 48 1.14 Assessment Factors for a Steganography Schemes . . . . 48 1.14.1 Capacity . . . . 49 1.14.2 Imperceptibility . . . . 49 1.14.3 Robustness . . . . 49 1.14.4 Security . . . . 49 1.14.5 Embedding Rate . . . . 49 1.14.6 Indistinctness or Fidelity . . . . 49 1.14.7 Sort of Pictures Supported . . . . 50 1.14.8 Time Complexity . . . . 50 1.15 Features of Robust Steganography . . . . 50 1.16 Basic Components of Steganography . . . . 51 1.16.1 Secret Message . . . . 51 1.16.2 Cover Image . . . . 51 1.16.3 Stego Image . . . . 51 1.16.4 Key . . . . 51 1.16.5 Embedding Steganography Algorithm . . . . 51 1.16.6 Extracting Steganography Algorithm . . . . 52 1.16.7 Embedding Domain . . . . 52 1.17 Steganographic Models . . . . 52 1.18 Steganographic Protocols . . . . 53 1.18.1 Pure Steganography . . . . 53 1.18.2 Private Steganography . . . . 54 1.18.3 Asymmetric Steganography . . . . 54 1.19 Signi…cance of Cryptography, Steganography and Watermarking . . . . 55 1.20 Some Di¤erences in Information Security Systems . . . . 57 1.20.1 Steganography Versus Watermarking . . . . 57 1.20.2 Cryptography Versus Watermarking . . . . 57 1.20.3 Cryptography Versus Steganography . . . . 57 1.21 Combination of Di¤erent Security Techniqes . . . . 58 1.21.1 Joined Cryptography and Steganography . . . . 58 1.21.2 Joined Watermarking and Steganography . . . . 58 1.22 Cybersecurity vs. Network Security vs. Information Security . . . . 58 1.22.1 Information security . . . . 59 1.22.2 Cybersecurity . . . . 59 1.22.3 Network security . . . . 60 1.23 Conclusion 61 2

2**A Color Image Watermarking Scheme Based on** A¢ ne **Transformation and** S4 **Permutation**

63 2.1 Some Algebraic De…nitions . . . . 66 2.1.1 De…nition . . . . 66 2.1.2 De…nition . . . . 66 2.2 Algebra of New Watermarking Technique . . . . 67 2.2.1 Least Signi…cant Bits . . . . 70 2.2.2 Most Signi…cant Bits 70 2.2.3

Example....................................197 8.6 Conclusion ....198 9 Conclusions 199 9.1 Impacts of Present Thesis . . . . 199 9.2 Future Research . . . . 201 Chapter 1 Preliminaries of Boolean Functions and Data Security As the generation, stockpiling, and trade of data turn out to be broader and imperative in the working of social orders, the issue of shielding the data from unintended and undesired utiliza- tion turns out to be more unpredictable. In current social orders, insurance of data includes numerous associated innovative and approach issues identi…ed with data privacy, integrity, anonymity, and authenticity, utility etc. Data concealing procedures are getting much consideration today. Digital sound, video, and pictures are progressively out…tted with recognizing yet indistinct imprints, which may be consist of concealed copyright marks or some registration number or even help to avoid unapproved replicating straightforwardly. Digital watermarking and steganography may ensure data, cover insider facts, or are utilized as center natives in advanced rights administration plans. There are three noteworthy information concealing methods famously: watermarking, cryptography and steganography. We essentially talk about cryptography in this part because of its signi…cance in Boolean algebra other two writes will be examined in di¤erent areas of this section. Cryptography is the study of giving security to data and assets by utilizing suitable inno- vations. Cryptography makes secure sites and electronic safe transmissions conceivable. For a website to be secure the greater part of the information communicated between the PCs where the information is kept and where it is gotten must be scrambled. Because of the vast number of business exchanges on the web, cryptography is exceptionally entered in guaran- teeing the security of the exchanges. Cryptography enables you to believe in your electronic exchanges.

59**Encryption is utilized as a part of electronic** exchanges **to** secure **information,** for example, **account numbers and exchange sums, computerized marks supplant written by hand marks or** mastercard **approvals, and open key encryption**

gives privacy. Key administration is a vital perspective in encryption that enables you to apply basic encryption approaches over all information on all oversaw gadgets. Cryptography in advanced world o¤ers three center zones that shield you and your infor- mation from endeavor robbery, burglary or an unapproved utilization of your information and conceivable misrepresentation. Cryptography cover these basic authentication, integrity, and privacy. The vocations of cryptography have colossally stretched out in the most recent

7**years, as the** utilization **of the** web **has** detonated. **A** most **basic** motivation behind **cryptography is to** connect with **two** social events **to**

quietly present over an uncertain line of correspondence. This construes any adversary can't recoup the message (additionally

7**called plaintext). The most** comprehensively saw movement **in cryptography is encryption and** unscrambling. **The term encryption** depicts **the** distinction in **the plaintext into the ciphertext.** In **the** event that the **ciphertext is** utilized **as** a commitment to **the** turnaround change, by **then we** recuperate **the plaintext. This** portrays **the** unscrambling **of a ciphertext. We** discuss **symmetric key cryptography if the encryption** change **is** unimportant related **to the** modify deciphering change. **In case the encryption key can be made** open, **we** discuss open **key cryptography. This** headway **came up in the mid** 1970's **when** Di¢ e **and Hellman** issued **their** article **"New Directions in Cryptography". Public key cryptography is** consistently attractive over **symmetric key cryptography** since **it** grants **to**

pass on protected without having e¤ectively normal

7**keys. In the late 1940s, Shannon** [1] displayed **the** vital thoughts **of** disarray **and** dissemination **to achieve security in**

cryptosys- tems. Disarray thinks the association

7**between the key and the ciphertext as** brain boggling **as** would be judicious. **This is** re‡ected **in the nonlinearity of** portions **of the cryptosystem.** Dispersion infers **that the ciphertext depends on** upon **the plaintext in**

an unusual way. In this way, we have scattering while at the same time changing a little piece of plaintext prompts to an immense contrast

7**in the ciphertext. The** inquiry develops **whether there are** capacities **that can be utilized to achieve this. We will** exhibit **that suitable Boolean functions** capacities **easily** give perplexity/ **confusion**

and furthermore di¤usion/ dispersion. Nonlinear parts of block ciphers and Boolean functions have a quite vital system of any data security schemes. These two imperative segments are …rmly connected by direct change. That is, a nonlinear segment is by and large included distinctive exceptional yield Boolean functions, yet in the event that it is changed to only a solitary bits or di¤erent bits, is indistinguishable to a Boolean function. The S-box is a lone nonlinear segment of any block cipher which is capable confusion in any symmetric cryptographic techniques. Boolean mapping are much of the time utilized as a part of the private key stream cre- ation methodology of

4**stream ciphers** algorithms **as these** transformations **are well** proper **for** accepting **bits of**

direct criticism move enrolls as contribution to request to go along with them as emphatically as conceivable to produce the single mystery key stream. Moreover, Boolean transforms have likewise displayed some critical properties, which are fundamental to restrict the great sort of assaults, so these mapping are a vital part in all stream and block ciphers. The nonlinear component for block cipher is one of the vital importance in many block ciphers. It o¤ers a method for making confusion in di¤erent blocks of bits for an absolutely divergent arrangement of yield

4**bits. One thing which is** imperative **is the** utilization **of secure substitution boxes (those which hold** amazing **encryption properties) so the substitution** shows **a**

confounded

16**relationship** amongst info **and** yield **bits of the** substitution **box.** One of **the** fundamental elements **of**

the substitution box, when utilized as a part of

4**iterative round** capacity, **is to** improve **the** exertion **required to** investigate **any** measurable **structure in the**

protected information. The nonlinear segments are talented to give the security of an encryption schemes by having brilliant encryption properties. Creating

4**secure S-boxes to use them in** di¤erent **cryptosystems for**

growing their security is energy investigates issue. This is basically so in light of the way that the cryptanalytic structure winds up being more re…ned and with the di¤erence in PC advancement

4**that contributes** also **supporting and against secure** correspondence. **The** quality **of** nonlinear segment **has a** noteworthy bearing **on secure**

correspondence. Nonetheless, greater capacities generally require extra computational time and exertion keeping in mind the end goal to investigate their imperfections, so we pick up a decent computational multifaceted nature upgrade when attempting to discover extensive capacities with strikingly amazing measures of appealing encryption properties. This incorporates an extra piece of in- tricacy to the examination issue. Consequently, we oversee Boolean transformations and their cryptographic attributes. This chapter of thesis for the most part exhibits a survey of hypothesis pertinent to the investigation of Boolean algebra, cryptography, watermarking and steganography. 1.1 Review on Boolean Functions in Cryptography The investigation of Boolean functions is a boundless and summed up range in itself. This segment displays a little writing review of Boolean functions and their properties. To a speci…c degree, the overview gave in this part is a total association of that which is required for the peruser to totally know about the research displayed in this dissertation. Especially, we have talked about some vital cryptographic properties which are appropriate to this work. 1.1.1 Cryptographic Desirable Characteristics of

7**Boolean Functions The** principle idea **of this** segment **is to** add **some** basic **preliminary** de…nitions **on Boolean functions**

[11]. De…nition 1 [13] "Let Vn2

142be the n dimensional vector space over the …eld of two element say V2. A Boolean function

g(x) : Vn2 ! V2 with the end goal that x = (x1;x2;:::;xn),

132is a mapping from n binary contributions to one yield. We let Bn speak to the arrangement of

every one of the 22n Boolean elements of n factors. Boolean function can be spoken to utilizing a di¤erent distinctive structures, each frame have diverse huge in data security primarily in calculations making and breaking." De…nition 2 [13] "A multi-esteemed or vector Boolean function

94is a change that maps a Boolean vector to another Boolean vector:"

: Vn2 ! Vm2: (1.1) De…nition 3 [11] "A Boolean function g : Vn2 ! V2 is viewed as linear i¤ it

162is a linear function from the vector space V2n to the vector space

V2. This adds up to stating" L (x) = 1x1 2x2 ::: nxn; (1.2) where denotes bitwise XOR operation and i 2 Vn2. De…nition 4 [11] "The arrangement of a¢ ne Boolean

115functions is the arrangement of linear Boolean functions and their complements" A ;c = L (x) c; (1.3) where x 2

Vn2. De…nition 5 [10] "The Hamming-weight wt(g);

176of an n-variable Boolean function is a simple a

function g : Vn2 ! V2 which gives

163number of 1's in the truth table of

g:" De…nition 6 [10] "The

7Hamming-distance as the number of arguments where g and

h have a di¤ erence, that is" d(g; h) = #fx 2 Vn2 j g(x)6 = h(x) g = wt(g h: (1.4) De…nition 7 [113] "The

7correlation value between two Boolean functions g and h is de…ned by" C(g; h) = 1 d(g; h) 2n 1

: De…nition 8 [13] "A Boolean function g 2 Bn

103is said to be a balanced if output column in the truth table contains equal numbers of zeros and one. A function is balanced if

its sequence is balanced that is wt(g) =2n 1:" It is easy to see that there are 2n2n 1 many balanced functions in the

102set of all n variable Boolean functions. Note that the

combining function in any cryptographic system need to be balanced. De…nition 9 [11] "The autocorrelation function rg(a) with a shift a 2 Vn2 is de…ned as" b

4rg(a) = g (x):g(x a):

b (1.5) b b xX2Z2n b b De…nition 10 [10] "The

45**algebraic degree/** order **of a Boolean function g(x); denoted by deg(g); is** de…ned **to be the number of variables in the largest product term of the function’s ANF having a**

non-zero coe¢ cient." De…nition 11 The

20**nonlinearity of a Boolean function** g is **denoted by** Ng and **is de…ned as**

follows Ng = d(g; An) = min d(g;): (1.6) 2An Example 12 Let n = 2; g(x) = x1x2 and ai 2 V2: Then any a¢ ne function can be expressed as i(x) = a0 a1x1 a2x2: By taking all the combinations of a0i s; we can generate all a¢ ne functions for n=2 and they are presented in the table. To …nd the nonlinearity of g, we calculate the distance between g and all a¢ ne functions that are presented in the following table. The minimum Hamming distance is nonlinearity of g. Table 1.1: Distance between g and all a¢ ne functions. A¢ ne functions g 1 2 3 4 5 6 7 8 0 0 0 0 0 1 1 1 1 0 0 1 0 1 1 0 1 0 0 0 0 1 1 1 1 0 0 1 0 1 1 0 1 0 0 1 d(g; Ai) 1 1 1 3 3 3 3 1 dmin = 1) Ng = 1: De…nition 13 [10] "The

7**Walsh transform of a function** g **on** Vn2 **is a map**

: Vn2 ! R de…ned by" (g)(u) = g(x)(1)<u;x>; (1.7) xX2Z2n

7**where < u; x > is the canonical scalar product.**

De…nition 14 [13] "The Walsh

90**-Hadamard matrix of order 2n,** signi…ed **by** W **Hn is** produced **by the recursive** connection" W **Hn** = W **Hn 1** W **Hn 1** 2 W **Hn 1** W **Hn 1**

3 = W H1 W Hn 1; (1.8) 4 5 for n = 1; 2; :::and W H0 = (1): Theorem 15 [13]

149**"The nonlinearity of a Boolean function g can** also **be** controlled **by** utilizing **Walsh**

transform which is given below:" Ng = 2n 1 1 2 u2Z n2 max j (g)(u)j : (1.9) b De…nition 16 [10] "A function g : Vn2 ! Vm2 has the avalanche impact, if a normal of 1/2 of the yield bits change at whatever point a solitary information bit is complemented i.e.," 1 m 2n wt(g(xi) g(x)) = ; f or all i = 1; 2; :::; n: (1.10) uX2Z2n 2 De…nition 17 [10] "A function g : Vn2 ! V2m of n input bits into m yield bits is said to be complete, if each yield bit relies upon each information bits, i.e. change at whatever point a solitary information bit is supplemented i.e." 8

164**i = 1; 2; :::; n; j = 1; 2; :::; m;** 9 **x**

2 V2n with (g(xi))j6 = (g(x))j: (1.11) De…nition 18 [13] "A function g : Vn2 ! Vm2 ful…lls the strict avalanche criterion, if each yield bit changes with a likelihood 1/2 at whatever point a solitary info bit is supplemented i.e."

166**8 i = 1; 2; :::; n; j = 1; 2; :::; m;**

P rob(g(xi))j6 = P rob(g(x))j = 1 2 : (1.12) 1.2 Nonlinear Component of Block Ciphers (S-Box) In this fragment, we by and by turning our trades to the zone of a nonlinear segment of block ciphers. The fundamental implications

16**of S-box theory are** given **to** enable **the** examination to **work performed in this** proposal. **In** like manner in **this**

portion, an overview of huge crypto- graphic properties as associated with S-boxes is given. 1.2.1 De…nition of Nonlinear Component and Types We list beneath a few vital S-box de…nitions,

16**together with a** short depiction **of some S-box** kinds important **to this** exploration. **An** i j **substitution box (S-box) is a mapping from** i **input bits to** j **output bits, S**

: Vi2 ! Vj2: The output vector S(x) = (s1; s2; :::; sj) can be decomposed into m component functions Sk : Vi2 ! V2; k = 1; 2; :::; m: There are 2i inputs and 2j

4**possible outputs for an** i j S **-box. Often considered as a look-up table, an** i j S **-box, S; is** normally symbolized **as a matrix of size** 2i j; **indexed as** Sk **(0** k 2i **1) each an** j **bit entry.**

There are, generally speaking, three types of S-boxes: Straight, compressed and expansion S-boxes. A straight nonlinear component of block cipher number of input and out remains same for instance AES nonlinear component take same number input and produces same outputs. A compressible nonlinear component of block cipher consists of more number of inputs as compared to output, DES S-boxes are the example of compressible nonlinear component of block ciphers. A expansion nonlinear component take less number of input and produce more outputs bits in general. 1.2.2 Cryptographic Possessions of Nonlinear Components While a large number of the Boolean capacity properties examined in past areas have calculated equivalences when connected to nonlinear components, there are principal contrasts in the way by which these properties are inferred. As a nonlinear component, is involved various part Boolean capacities, watch that while

4**considering the cryptographic properties of** a nonlinear component, **it**

isn't adequate

4**to consider the cryptographic** properties **of the** segment **Boolean**

capacities separately. Or maybe, it is likewise important

194**to consider the** cryptographic **prop- erties of** all **the** straight mixes of **the**

part capacities. This is represented in the accompanying choice of applicable nonlinear component of block ciphers properties. A n m nonlinear component of block cipher which is adjusted is one whose part Boolean capacities and their direct mixes are altogether adjusted. In view

16**of this** adjust, **there does not exist an exploitable** inclination **in that the** similarly **likely number of** yield **bits over all** yield **vector** blends guarantees **that an**

aggressor can't inconsequentially estimated the capacities or the yield. The outstanding idea of disarray because of Shannon [1] is depicted as a technique for guar- anteeing that in a …gure framework a mind boggling

16**relationship exists between the ciphertext and the key material. This** thought **has been extrapolated to** imply **that a** noteworthy depen- dence **on some** type **of substitution is required as a** wellspring **of this** perplexity. **The** perplexity **in a** …gure framework **is**

accomplished using nonlinear segments. Not surprisingly, substitution boxes have a tendency to give the principle wellspring of

4**nonlinearity to cryptographic** …gure frameworks. **We now** characterize **the measure of** nonlinearity **for** a **n m**

nonlinear component of block cipher. Since nonlinear component of block cipher is consist of single or multiple values Boolean functions, therefore all the basic properties which were de…ned for Boolean functions can be equally applicable for classi…cation of cryptographically secure nonlinear component for block ciphers. De…nition 19 The bit independence comparing

119**to the** impact **of the ith input** bit **change on the jth and kth bits of**

is ei : Bic(j; k) = 1miaxmjcorr(eji; eki)j: (1.13) The bit independent criterion (BIC) for nonlinear component for block cipher function f is de…ned as follows: Bic(f) = max Bic(j; k); (1.14) 1 j;k m j6=k which indicates how close is ful…lling the BIC [107]. Linear and Di¤erential Cryptanalysis Linear and di¤erential cryptanalysis are connected assaults utilized basically against iterative symmetric key piece …gures. An iterative …gure (additionally called an item …gure) directs di¤erent rounds of encryption utilizing a subkey for each round. Illustrations incorporate the Feistel Network utilized as a part of DES and the State rounds utilized as a part of AES. In the two assaults, a cryptanalyst examine changes to the transitional ciphertext between rounds of encryption. The assaults can be joined, which is called di¤erential linear cryptanalysis. An objective of solid encryption is to deliver ciphertext that seem arbitrary where a little change in a plaintext brings about an irregular change in the subsequent ciphertext [105].

177**Linear Cryptanalysis Linear cryptanalysis is a known plaintext**

assault that expects access to a lot of plaintext and ciphertext sets scrambled with an obscure key. It centers around mea- surable investigation against one round of unscrambling on a lot of ciphertext. The cryptanalyst decodes each …gure content utilizing all conceivable subkeys for one round of encryption and concentrates the subsequent middle …gure content to look for the slightest irregular outcome. A subkey that delivers the minimum arbitrary middle cipher6 for all …gure writings turns into an applicant key (the in all likelihood subkey). Di¤erential Cryptanalysis Di¤erential cryptanalysis is a picked plaintext assault that looks to …nd the connection between ciphertext delivered by two related plaintexts. It centers around measurable examination of two data sources and two yields of a cryptographic calculation. A plaintext combine is made by applying a Boolean restrictive or (XOR) activity to a plain content. For instance, XOR the rehashing twofold string 10000000 to the plaintext. This makes a little contrast (thus the term di¤erential cryptanalysis) between the two. The cryptanalyst at that point encodes the plaintext and its XOR-ed combine utilizing all conceivable subkeys, and it looks for indications of nonrandomness in each moderate ciphertext match. The subkey that makes the minimum irregular example turns into the applicant key [110]. De…nition 20 For a given vector Boolean function g : Vn2 ! V2m it is de…ned the linear approximation table which elements are LATg(a; b) = #fx 2 Zn2ja:x = b:g(x)g 2n 1; (1.15) where a 2 V2n; b 2 Vm2nf0g: De…nition 21 For any given x, y , x, y 2 Vn2 ;the linear and di¤erential approximation probabilities for each vector Boolean function (S-box) are de…ned as: LPSi(y ! x) = 2 #fx 2 V2njx x = Si(x) yg 1 ; 2n (1.16) DPSi(x ! y) = #fx 2 Vn2jSi(x) 2nSi(x x) = yg ; (1.17)

117**where x** x, **denotes the parity (0 or 1) of** the **bitwise product of x and**

x [110], [102], [105], [111]. De…nition 22 The maximum linear and di¤ erential approximation probabilities of vector Boolean function (S-boxes) are de…ned as [112], [114]: p = max max LPSi(y ! x); i x; y q = max max DPSi(x ! y): i x; y (1.18) (1.19) De…nition 23 [87] "An element a 2 Vn2 is a …xed point (opposite …xed point) of g : Vn2 ! Vm2 if g(a) = a (g(a) = a)." De…nition 24 [87]

84**"The resistance of S-boxes** to **DPA**

attacks called

84**transparency order of an S-box S**

= (s1; s2; ::::; sn) on V2n is de…ned as:" TF = max jn 2H W ( )j 1 2Vn2 0 22n 2 n (1)v: WDaS(u;v) (1.20) @ aX2V2n vX2V2n 1 ; A where WDaS(u;v) is the Fourier

86**transform of the** sign function **derivative of** S **with respect to** vector **a**

2 V2n; DaS : x7 ! S(x) S(x a): The

188**Fourier transform of the sign function** derivative of S **is** de…ned **as**

follows WDaS(u;v) = (1)v:fS(x) F Sx a)g u x (1.21) aX2V2n De…nition 25 [87] "For any positive integers n and m, a function S : Vn2 ! V2m is called di¤erentially -uniform if for every a 2 Vn2 nf0g and every b 2 V2m, the equation S(x)+S(x+ a) = b; admits at most solutions." De…nition 26 [87] "The

4**sum of square** indicator, **also derived from the autocorrelation**

func- tion, may be calculated as follows:" = r2(a) a 2 f1; 2; ::::; 2N 1g: (1.22) X De…nition 27 [87] "The

20**Boolean function obtained by the product of the TTs of two Boolean** b **functions f;g by f:g (note that this product is di¤erent from the dot product between two vectors x;y). The algebraic immunity (AI) of a Boolean function f on** Vn2 **is de…ned as the lowest degree of the function g**

: V2n ! V2

> 20**for which f:g = 0 or (f 1):g = 0: The function g for which f:g = 0 is called an annihilator of f . Denote the set of all annihilators of f by An(f)."**

De…nition 28 [87] "Let S = (s1;s2;:::;sn) be an n s nonlinear component of block cipher.

> 26**Denote by L the largest value in the di¤erence distribution table** on **F , and by N the number of nonzero entries in the …rst column of the table. In either case the value 2n in the …rst is not counted. Then we say that F is R-robust against** the **di¤erential cryptanalysis, where R is de…ned by**

De…nition 29 Representing

> 26**by L the** biggest incentive **in the di¤erence distribution table** on **F, and by N the** quantity **of nonzero** sections **in the** main segment **of the table. In either case the** esteem **2n in the …rst**

isn't tallied. At that point

> 91**we say that F is R-** powerful **against** the **di¤erential cryptanalysis, where R is** characterized **by" R= 1 N** 2n **1** L **2n**

: (1.23) De…nition 30 [87] DPA work factor is identi…ed with genuine examinations, where the execu- tion is surveyed by a signal to noise ratio (SNR). As of now said, regardless of whether the DPA isn't uproarious, it doesn't permit to speci…cally detect the correct pinnacle (k=0) in light of the fact that there exists auxiliary pinnacles notwithstanding for wrong keys (k6 = 0). Secondary peaks are modeled as noise. DPA qualify is in this manner evaluated by the accompanying idea of SNR. To the extent the DPA signal is concerned, adjusted S-box F ful…lls: DP A(0) = 2 p (1)hli ljjS(x)i ; (1.24) Xi;j Xx = (li lj) = q; (1.25) Xi;j DP A = 2 2p (1)S(x)i (1)S(x k)j (1.26) Xi;jXx Xk ! ; = 0; (because S is balanced): (1.27) As a result, SNR DPA is de…ned as follows: p1 4 1=2 SNRDPA(S) = q22p 0 (1)Si (k) ; (1.28) Xx Xi=0 ! 1 @ A where f (k) = (1)hxjkif(x)

> 62**is the** Hadamard **-Walsh transform of the function.** x b P **1.**

3 Review on Information Security Preliminaries The essential of information security inside an a¢ liation has encountered two critical changes over the latest a signi…cant drawn-out period of time. The security of information felt to be gainful to an a¢ liation was given on a very basic level by physical and administrative …les, already the limitless of data planning equipment. An instance of the latter is workforce screening system used in the midst of securing process. An instance of the past is the use of harsh …lling pantries with a blend dart to store fragile reports. With the presence of the PC, the requirement for automated gadgets for guaranteeing reports and other information set away on the PC wound up mandatory. This is required for a structure like the time-sharing system and moreover sooner or later requires is impressively more extreme for systems that can be gotten to over an open telephone data framework or web. The second enormous change that a¤ected security is the presentation of passed on struc- tures and the utilization of systems and correspondences working environments for passing on information between terminal client and PC. Structure security is required to ensure informa- tion while in development. Everything considered, sort out security term is deluding since all business, government and scholarly connection interconnected their information dealing with hardware with a storing up of interconnected structures.

> 53**Cryptography is a science that applies complex** number-crunching **and** justi…cation **to** plot **strong encryption** methodologies. **Cryptography is** moreover a craftsmanship. **Cryptography** empowers **people to keep** con…de **in the electronic world. People can do their business on** an **electric channel without worrying of** dishonesty **and**

misleading. Right when people started cooperating on the web and anticipated that would trade …nances electronically; the employments of cryptography for trustworthiness began to beat its use for security. These days, a colossal number of people interface electronically reliably by di¤erent means like messages, ATM machines, web business or telephones. The speedy augmentation of information transmitted electronically achieved an extended reliance on cryptography and approval. This section is devoted to introducing the preliminaries related to information security systems to be discussed in this thesis. We explicitly de…ne the basics of the cryptography, watermarking and steganography primitives which will be helpful in subsequent chapters. Fig. 1.1: Classi…cation of information security systems. 1.4 Cryptology Cryptology is the investigation of data security.

110The word cryptology is gotten from the Greek kryptos, which means

covered up. Cryptology is the investigation of "mystery composing." In era of digitally advanced communication, secure information security is an important component of any nation. 1.4.1 Classi…cation of Cryptology The cryptology is additionally characterized by two branches cryptography and cryptanalysis. The term cryptography alludes to the workmanship or exploration of planning cryptosystems (to be characterized in no time), while cryptanalysis alludes to the science or craft of breaking them. 1.4.2 Basics Terminology of Cryptography Plain Text The plaintext is a simple information which can easily understand without any information. Cipher Text A message that come from some algorithm and which can't be understood with extra informa- tion. Ciphers A cipher/algorithm is a transformation that utilize the original message as an input and encoded message as an output is called cipher and some time algorithm. Encryption The process of transforming plaintext into ciphertext is encryption. The mathematical expres- sion for encryption is given below: C =

116E(P); where P is plaintext, C is ciphertext and E is encryption function. Decryption The process of transforming encoded message into

original message is called decryption. Let D is the decryption function, i.e. P = D(C); which means by applying the decryption process D to ciphertext C produces the plaintext P . Key A key is a simple information which is used to encrypt or decrypt plaintext and ciphertext. Fundamentally, key is a sort of knowledge which us used to that determines output of a cryp- tographic ciphers." Fig. 1.2: Block diagram for encryption and decryption. De…nition 31

33A cryptosystem is a quintuplets (M ;C;K;E;D) in which M is called the

plain- text space; C is a

148called the ciphertext space; K is called the key space; E is an encryption

rules; D is a decryption rules.

33For each K 2 K, there is a function eK 2 E and a corresponding function dK 2 D such that for any plaintext message x 2 P; dK(eK(x)) = x. Notice that this means dK is the inverse of the function eK.

De…nition 32 A mapping T :

33X ! Y is one-one or injective i¤ 8 a; b 2 X; T (a) = T (b)) a = b.

1.5 Prime Security Purposes of Cryptography Cryptography is the art/craft of writing to secure communication in insecure lines of commu- nications. There are four essential elements of cryptography today: 1.5.1 Con…dentiality Con…dentiality/Privacy is the major security bene…t gave by cryptography. It is a security bene…t that keeps the data from an unapproved individual. It is once in a while alluded to as security or mystery. Secrecy can be accomplished through various means beginning from physical securing to the utilization of scienti…c calculations for information encryption. 1.5.2 Data Integrity It is security bene…t that arrangements with recognizing any change to the information. The in- formation may get altered by an unapproved substance deliberately or accidently. Respectabil- ity bene…t a¢ rms that whether information is in place or not since it was last made, transmitted, or put away by an approved client. Information trustworthiness can't keep the adjustment of information, however gives a way to distinguishing whether information has been controlled in an unapproved way. 1.5.3 Authentication Authentication/Veri…cation

14gives the recognizable proof of the originator. It a¢ rms to the collector that the information got has been sent just by a recognized and con…rmed sender. Validation bene…t has two variations: i. Message authentication: recognizes the originator of the message with no respect switch or framework that has sent the message

ii. Person veri…cation /authentication: is a¢ rmation

14that information has been gotten from a particular element, say a speci…c site. Aside from the originator, veri…cation may likewise give a¢ rmation about di¤erent parameters identi…ed with information, for example, the date and time

> **of creation/transmission.** 1.5.4 **Non-** repudiation **It is a security** advantage **that** ensures **that** a component **can't deny the** obligation regarding **past** obligation **or an** action. **It is** an **affi** rmation **that the** primary producer **of the** data **can't deny the creation or transmission of the said** data **to a** recipient **or** pariah. **Non-** disavowal **is a property that is most alluring in** conditions **where there are** chances **of**

a contradiction in regards to the exchanging of data. For example, once a demand is sent electronically, a purchaser can't deny the purchase orchestrate, if the non-disavowal advantage was engaged in this trade. 1.6 Cryptographic Essentials Cryptography natives/essentials are only the instruments and strategies that can be specifically used to give an arrangement of wanted security administrations: 1. Enciphering 2. One-to-one functions 3. Message verification codes (MAC) 4. Digital signatures The accompanying table demonstrates the natives that can accomplish a specific security benefit without anyone else. Table 1.2: Security services and its primitives. Primitives =) Encryption Hash Function MAC Digital Signature Services + Confidentiality Yes No No Yes Data Integrity No May be Yes Yes Authentication No No Yes Yes Non-repudiation No No May be Yes Cryptographic natives are complicatedly related and they are regularly consolidated to accomplish an arrangement of wanted security administrations from a cryptosystem. 1.7 Classification of Cryptographic Algorithms There are a few methods for categorizing cryptographic algorithms. For motivations behind this section, they will be sorted in light of the different amount of keys that are used at the time of encryption and unscrambling, and assist characterized by their request and use. The modern cryptographic algorithms can be classified into three following broad categories: i. Private/Secret/Symmetric Key Cryptography ii. Asymmetric/Public Key Cryptography iii. One Way Hash Function Fig. 1.3: Classification of cryptographic algorithms. 1.7.1 Private/Secret Key Cryptography Private uses a single key for both encryption and unscrambling. Basically it is utilized for privacy and confidentiality There are numerous private key algorithms such as DES and AES used in literature for the security of digital information. The secret key algorithms can further be classified into two sub-classes namely, block ciphers and stream ciphers which are defined in [18]. Fig. 1.4: Symmetric private-key encryption system. 1.7.2 Public Key Cryptography Utilizes different keys for encryption and decryption; likewise called asymmetric encryption. Essentially utilized for authentication, non-repudiation, and key exchange. There are various public key encryption algorithms for instance RSA, Elgamal, Rabin and Elliptic curve crypto- graphic algorithms etc. Fig. 1.5: Public-key encryption system. 1.7.3 Hash Function Utilizations a numerical change to irreversibly "encode" information, giving a propelled ex- traordinary check. Essentially used for message respectability. Hash limits, moreover

> 76**called message** surveys **and one-way encryption, are** figuring **that, in some sense,** use **no key.**

Hash limits, by

> 76**then, give a measure of the trustworthiness of a record.**

Hash calculations that are in like way use today fuses message assimilation (MD) conspires, the safe hash calculation (SHA) and its distinctive variations. 1.7.4 Diffusion and Confusion Confusion and diffusion are two properties of the activity of a safe algorithms in cryptography. Confusion and diffusion/dissemination were recognized

> 122**by Claude** Elwood **Shannon in his** pa- per, **"Communication Theory of Secrecy Systems"** distributed **in 1949. In**

Shannon's unique definitions [1]: i.

> 127**Confusion makes the relationship between the key and the ciphertext as complex as**

pos- sible ii. Diffusion represents the characteristic that recurrence

> 120**in the statistics of the plaintext is "dissipated" in the statistics of the ciphertext**

Dispersion is related with the reliance of the yield bits on the information bits. In a cipher with great dissemination, flipping an information bit should change each yield bit with a like- lihood of one a large portion of (this is named the Strict Avalanche Criterion). Substitution (a control for supplanting plaintext images by another) has been recognized as a component for fundamentally perplexity (see S-box); then again transposition utilizing P-box (adjusting or swapping the request of images) is a strategy for dissemination, albeit different systems are likewise utilized as a part of present day hone, for example, straight changes (e.g. in AES, ShiftRow and Mix Column activities). Product ciphers utilize rotating substitution and trans- position stages (rounds) to accomplish both perplexity and dispersion individually.

Current block ciphers utilize both perplexity and dispersion. The codebook parts of such frameworks give perplexity practically equivalent to however on a considerably more fabulous scale-a basic substitution. All around planned block ciphers spread any nearby insights all through the piece, along these lines utilizing the guideline of dispersion [1, 2]. 1.7.5 Digital image processing Image process might be a strategy to play out a few operations on a photo, in order to ask an expanded image or to remove some accommodating information from it. it's a kind of signal processor inside which input is a photo and yield is likewise image or attributes/highlights identi…ed with that image. These days, the imaging procedure is among rapidly developing advances. It frames center examination space inside building disciplines too. Image handling is a strategy to play out a couple of exercises on a photo, with a particular true objective to get an enhanced picture or to isolate some accommodating information from it. It is a sort of banner taking care of in which input is a photo and yield may be picture or traits/features related with that photo. Nowadays, picture getting ready is among rapidly creating headways. It shapes focus inquire about an area inside building and programming designing orders too. Digital Image A picture is just a two dimensional exhibit. It is characterized by the scienti…c capacity f (x; y) where x and y represents two arranges on a level plane and vertically. The estimation of f (x; y) anytime is gives the pixel esteem by then of a picture running in the vicinity of 0 and 255: The measurements of the photo is really the measurements of this two dimensional cluster. These advanced pictures can be monochrome (bi-tone), grayscale or shading relying on the allowable force levels of every pixel i.e. regardless of whether every pixel is spoken to by just a single piece, 8 bits or 24 bits. As a rule, a monochrome picture can have just a single piece plane while

> 38**there are 8-bit planes in a** dark **scale** picture **and 24 bit planes (8-bits each,** as for **the** three **channels** Red, Green **and** Blue) **in a**

shading picture. The slightest critical piece

> 38**plane (LSB plane) is the plane that** comprises **of bits with** least **positional** esteem **(20 = 1) and the MSB plane (most** noteworthy piece **plane)** comprises **of bits with** most astounding **positional** esteems **i.e. 27 = 128.**

(a) (b) Fig. 1.6: RGB color space. 1.8 Basics of Watermarking Nowadays, billions of bits of data acquire into presence each a large portion of a second. What's more, because of extraordinary acknowledgment of the Internet alongside quick advancement of mixed media innovation, clients have more probability to utilize computerized information (picture, video and sound records, web distributed advanced storehouses and libraries). After all duplicating computerized information is a very sensitive issues of digital advanced world. Digital watermarking is an answer for these issues as it has di¤erent applications like copyright insurance, con…rmation, secret communication, and estimation. E-trade, E-voting, medical safety, broadcasting observing, military and ordering can be ensured by computerized water- marking. Watermark stays in place to the cover picture regardless of the possibility that it is replicated, is the normal for watermarking. Consequently to guarantee responsibility for water- mark is removed and tried.

> 193**Digital watermarking** is **the** strategy **of** installing **a watermark in** an interactive media **object.**

This object might be picture, sound, video and any computerized content with the end goal of data covering up. Intense watermarking method ought to be chosen for strong watermark embedding [46]-[47]. 1.9 Digital Watermarking A computerized watermark or digital watermark is an example of bits embedded into an advanced medium (picture, sound or video). Such messages for the most part convey copyright data of the record. In any case, the principle contrast between them is that computerized wa- termarks should be imperceptible or possibly not changing the view of unique document, not at all like paper watermarks, which should be to some degree noticeable. For example, a digital camera that would use lossless watermarking to embed a biometric identi…er together with a cryptographic hash value. A digital signature is a large unique integer generated by encrypting a hash value of a …le, image, video, etc. The formal de…nition of watermarking is given as follows: De…nition 33 A watermarking system is a quintuple (C; W; K; EK; DK); where C is space of cover image, W the set of all watermarks,

> 130**K is the set of** all **possible keys,** C0 **is the set of all**

original data with watermark. The two functions EK : C W K ! C 0 ; DK : C 0 K ! W; describe the embedding and detecting process. Fig. 1.7: Basic procedure of digital watermarking. 1.9.1 Basic Terminologies of Watermarking The general de…nitions of some common terms used in the area of watermarking are listed below: Watermark The data to be covered up. The term watermark additionally contains an insight that the concealed data is straightforward like water. Cover Media/Data The media utilized for conveying the watermark. At times the terms unique media, cover media and host media are additionally used to express it. Watermark Data The computerized medium which contains the watermark. Extraction The technique utilized for extricating the installed watermark from the water- mark question. Detection The technique utilized for identifying whether the given media containing a speci…c watermark. 1.9.2 Qualities of Computerized Watermarking The necessities for picture watermarking can be dealt with as qualities, properties or charac- teristics of picture watermarking. Diverse applications request distinctive properties of water- marking. Necessities of picture watermarking ‡uctuate and result in di¤erent outline issues relying upon picture watermarking applications and reason. These necessities should be mulled over while outlining watermarking framework. There are fundamental …ve necessities as takes after [5]. Fidelity Fidelity/Devotion is

100**considered as a measure of perceptual** straightforwardness **or** impercep- tibility **of watermark.**

It implies the similarity of un-watermarked and watermarked pictures. This perspective of watermarking mishandle limitation of human vision. Watermarking should not present unmistakable curves as it decreases business estimation of the watermarked picture. Robustness Watermarks ought not be expelled deliberately or inadvertently by basic picture handling ac- tivities. Thus watermarks ought to be strong against assortment of such assaults. Strong watermarks are intended to oppose typical handling. Then again, delicate watermarks are intended to pass on any endeavor to change computerized content. Data Payload Information payload is otherwise called limit of watermarking. It is the most extreme measure of data that can be covered up without debasing picture quality. It can be assessed by the measure of concealed information. This property portrays how much information ought to be implanted as a watermark with the goal that it can be e¤ectively distinguished amid extraction. Security Secret key must be utilized for implanting and identi…cation process in the event that

100**security is a** noteworthy **concern. There are three** kinds **of keys**

utilized as a part of watermark frame- works: private-key, recognition key and open key. Hackers ought not have the capacity to expel watermark with hostile to …guring out research algorithm. Computational Complexity Computational many-sided quality shows the measure of time watermarking calculation takes to encode and decipher. To guarantee security and legitimacy of watermark, more computational unpredictably is required. On the other hand, constant applications require both speed and e¤ectiveness. 1.10 Watermarking Attacks There are distinctive possible malignant deliberate or surprising assaults/strikes that a water- marked question is presumably going to subject to. The availability of the broad assortment of pictures dealing with sensitive items made it possible to perform strikes on the quality of the watermarking structures. The purpose of these ambushes is shielding the watermark from playing out its arranged reason. A succinct introduction to various sorts of watermarking ambushes/attacks is given beneath: 1.10.1 Elimination Attack Elimination Attack hopes

128**to remove the watermark data from the watermarked** dissent. **Such** ambushes abuse how **the watermark is** regularly **an**

additional substance racket hail show in the host signal. 1.10.2 Intrusion Assault Intrusion strikes are those which add additional confusion to the watermarked challenge. Lossy weight, quantization, plot, denoising, demodulation, averaging, and commotion storm are a couple of instances of this arrangement of ambushes. 1.10.3 Shapes Attacks All controls that impact the geometry of the photo, for instance, ‡ipping, turn, trimming, et cetera should be observable. A trimming ambush from the right-hand side and the base of the photo is an instance of this attack. 1.10.4 Security Attack Particularly, if the watermarking computation is known, an aggressor can furthermore endeavor to perform modi…cations to render the watermark invalid or to assess and change the watermark. For this circumstance, we examine a strike on security. The watermarking computation is seen as secure if the embedded information can't be pulverized, recognized or fabricated. 1.10.5 Protocol Attack The protocol/tradition ambushes do neither go for destroying the embedded information nor at devastating the recognizable proof of the embedded information (deactivation of the water- mark). Instead of that, they abuse semantic de…ciencies of the watermark's use. In this way, a solid watermark must not be invertible or to be recreated. A copy strike, for example, would go for recreating a watermark from one media into another without data of the puzzle key. 1.10.6 Cryptographic Assaults Cryptographic assaults manage the breaking of the security. For instance, …nding the mystery watermarking key utilizing comprehensive beast compel strategy is a cryptographic assault. An- other case of this sort of assault is the prophet assault. In the oracle assault, a non-watermarked protest is made when an open watermark locator gadget is accessible. These assaults are like the assaults utilized as a part of cryptography. 1.10.7 Dynamic Attacks Here, the programmer tries intentionally to expel the watermark or basically make it imper- ceptible. This is a major issue in copyright security, …ngerprinting or duplicate control for instance. 1.10.8 Passive Attacks For this situation, the assailant isn't endeavoring to expel the watermark yet just endeavoring to decide whether a given check is available or not. Cox et al (2002) recommend that assurance against latent assaults is absolutely critical in incognito interchanges where the basic information of the nearness of the watermark is frequently in excess of one needs to concede. 1.10.9 Collusion Attacks In deceitful assaults, the objective of the programmer is the same with respect to the dynamic assaults yet the strategy is somewhat extraordinary. Keeping in mind the end goal to evacuate the watermark, the programmer utilizes a few duplicates of similar information, containing each extraordinary watermark, to build another duplicate with no watermark. This is an issue in …ngerprinting applications (e.g. in the …lm business) yet isn't the broadly spread in light of the fact that the assailant must approach various duplicates of similar information and that the number required can be entirely vital. 1.10.10 Digital Image Degradation These kinds of assaults harm vigorous watermarks by evacuating parts of the picture. The parts that are supplanted may convey watermark data. Cases of these tasks are incomplete editing, push expulsion and segment evacuation. Addition of Gaussian clamor additionally goes under this classi…cation, in which the picture is corrupted by including commotion controlled by its mean and its di¤erence. 1.10.11 Image Augmentation These assaults are convolution activities that desynchronize the watermark data in a picture. These assaults incorporate histogram leveling, honing, smoothing, middle sifting and complexity improvement. 1.10.12 Image Firmness So as to diminish the storage room and cut the cost of transmission capacity required for transmitting pictures, pictures are for the most part packed with JPEG and JPEG2000 pres- sure strategies. These lossy pressure strategies are more unsafe when contrasted with lossless pressure techniques. Lossless pressure strategies can recoup the watermark data with back- wards activity. However lossy pressure strategies create irreversible changes to the pictures. Subsequently likelihood of recuperating watermarked data is constantly low. 1.10.13 Image Alterations These sorts of assaults are likewise called synchronization assaults or geometrical assaults. The well-known programming Stir Mark utilizes little neighborhood geometrical contortions to refute watermark recognition. Geometrical assaults incorporate revolution, scaling and interpretation likewise called RST assaults. A few scientists center around RST strength while planning the powerful watermarking frameworks, since it is basic issue. Other than RST changes, picture changes additionally incorporate di¤erent changes, for example, viewpoint proportion change, shearing, response and projection. 1.11 Watermarking Applications With the fast improvement of the data innovation and PC arrange innovation, the security of advanced sight and sound data has turned into a vital issue. The customary data security in- novation in view of cryptography hypothesis generally has its restrictions. Keeping in mind the end goal to determine the inadequacies of customary data security innovation, an ever-increasing number of specialists has been beginning to consider the computerized watermarking innovation since it can successfully adjust for the lacks of the security and insurance utilization of conven- tional data security innovation. The watermark data can be copyright data, veri…cation data or control data in order to decide the copyright proprietor of the computerized works, a¢ rm the legitimacy and honesty of interactive media works, control duplicating as per the inserted control data, and accomplish the reason for copyright assurance. Advanced watermarking in- novation has numerous applications in assurance, certi…cation, distribution, anti-counterfeit of the

2**computerized media and name of the client data. It has turned into an** imperative report **region in data covering up.**

As a rising interdisciplinary application innovation, computerized

2**watermarking includes the** thoughts **and** speculations **of** various **subject**

scopes, for example, ‡ag handling, cryptography, likelihood hypothesis and stochastic hypothesis, arrange innova- tion, calculation outline, and di¤erent strategies. It can implant

2**copyright data into the** mixed media **information through** speci…c calculations; **the data**

might be creator's serial number, or- ganization logo, pictures or content with uncommon noteworthiness, et cetera. Their capacity is …lled in as copyright security, mystery correspondence, credibility recognize the information document, and so forth. The installed famous data is normally not noticeable or subtle, and it must be identi…ed or removed through various extraordinary indicators or pursuers. A com- puterized watermark is …rmly coordinated with and hided into the source information and it is turning into an indivisible piece of the last mentioned. This section depicts seven utilizations of watermarking: secretive correspondence, communicate scrutiny, proprietor recognizable proof, con…rmation of possession, veri… cation, value-based watermarks and duplicate control [51]. 1.11.1 Secretive Correspondence One of the most punctual utilizations of watermarking, or all the more absolutely, information covering up, is a strategy for sending covert communications. The application has been point by point by Simmons as the detainee's stress, in which we envision two detainees in independent cells endeavoring to pass messages forward and in turn around. Their stress is that they can't pass these messages especially, yet rather, must depend upon the remedial o¢ ce overseer to go about as an operator. The chief will pass on harmless messages between them, regardless; will censure them in the event that he …nds that, for instance, their messages identify with a strategy for escape. The strategy is to cover the escape-layout messages by concealing them in safe messages. There are two or three mechanically open endeavors expected for this application, including stego tools. 1.11.2 Communicate Scrutiny In 1997, an embarrassment softened out up Japan with respect to TV promoting. No less than two locations had been regularly over…lling broadcast appointment. Promoters stood recompensing for a large number of advertisements that were never publicized. The training had remained to a great extent undetected for more than twenty years, to some degree on the grounds that there were no frameworks set up to screen the genuine communicate of promo- tions. There are a few sorts of associations and people intrigued by communicating checking. Publicists, obviously, need to guarantee that they get the transmission appointment bought from propagation …rms. Artists and on-screen characters need to guarantee that they get exact eminence installments for communicates of their performances. 1.11.3 Proprietor Recognizable Proof Despite the way that a copyright see isn't any more basic to ensure copyrights, it is still proposed. The kind of the copyright see is regularly "c date, proprietor". On books and photos, the copyright is put in plane sight. In …lms, it is joined to the total of the credits. In like manner, on prerecorded music, it is resolved to the bundling. One weight of such substance copyright sees is that they can as regularly as conceivable be expelled from the secured material. Bundling can be lost, motion pictures can have the credits cut o¤, and pictures can be spatially trimmed. An electronic watermark can be utilized to give looking at copyright checking comfort since it changes into a fundamental piece of the substance, i.e.

the copyright data is inserted in the music to supplement the substance see engraved on the bundling. The Digimarc a¢ liation has propelled a watermarking framework made arrangements for this application. Their watermark inserted and pioneers are packaged with Adobe's unmistakable picture managing the program, Photoshop. Right when the identi…er …nds a watermark, it contacts a focal database to perceive the watermark's proprietor (who must pay a cost to keep the data in the database). 1.11.4 Con…rmation of Possession Sight and sound proprietors may need to utilize watermarks not simply to perceive copyright possession, yet rather to really show proprietorship. To design the issue, we ought to rapidly show a few characters that are surprising in the watermarking forming. Acknowledge Alice makes a photograph and puts it on her site, with a copyright. Skip by then takes the photograph, utilizes a photograph managing the dare to supplant the copyright see with, and a brief time frame later claims to have the copyright himself. By what means can the request resolve? Normally, Alice could enlist the photograph with the copyright o¢ ce by sending a duplicate to them. The copyright o¢ ce records the photograph, together with data about the genuine proprietor. Right when the common contention among customer A and customer B comes up, customer A contacts the copyright o¢ ce to obtain certi…cation that she is the good 'old- fashioned proprietor. On the o¤ chance that customer A did not enlist the photograph, by then she ought to on any event can display the …lm negative. In any case, with the quick certi…cation of bleeding edge photography, there might never have been a negative. On a fundamental level, it is down to earth for Alice to utilize a watermark acquainted in the photograph with the show that she promises it. 1.11.5 Veri…cation As both still and camcorders continuously get a handle on cutting edge development, the limit with respect to intangible adjusting in like manner increases. The substance of mechanized photographs can without a doubt be balanced to such an extent that it is particularly di¢ cult to recognize what has been changed. For this circumstance, there isn't even a one of a kind negative to take a gander at. There are di¤erent applications where the veracity of a photograph is squeezing, particularly in genuine cases and helpful imaging. Check is a particularly considered issue in cryptography. Friedman [13, 14] …rst talked about its application to make a "strong camera" by …guring a cryptographic stamp that is related to a photograph. In the event that even one piece of one pixel of the photograph is adjusted, it will never again compose the check, so any altering can be perceived. In any case, this check is metadata that must be transmitted adjacent the photo, potentially in a header …eld of a speci…c picture coordinate. In the event that the photograph is …ttingly reproduced to another record layout that does not contain this header …eld, the stamp will be lost, and the photograph can never again be avowed. The

178**best course of action is to** bring **the** register straightforwardly with **the**

photograph utilizing watermarking. This sheds the issue of guaranteeing that the check remains with the photograph. It likewise opens up the likelihood that we can take in extra about what changing has happened since any developments made to the photograph will in like way be made to the watermark. In this manner, there are a few frameworks that can show the hostile zone of changes that have been made to the photograph. There are also structures proposed to permit certain developments, for example, JPEG weight, and essentially prohibit more huge changes, for example, expelling a man from a terrible conduct scene. 1.11.6 Value-based Watermarks Checking and proprietor perceiving a¢ rmation applications put a practically identical water- mark on all duplicates of a similar substance. Regardless, electronic stream of substance permits each duplicate scattered to be changed for every bene…ciary. This point of con…nement engages a novel watermark to be presented in every individual duplicate. Regard based watermarks, besides called …ngerprints, permit a substance proprietor or substance shipper to see the well- spring of an unlawful duplicate. This is conceivably basic both as an obstruction to unlawful utilize and as a creative manual for examination. One conceivable usage of huge worth based watermarks is over the span of …lm dailies. Over the cross of a¤ecting a development to picture, the postponed result of reliably photography is a great part of the time passed on to various individuals associated with its creation. These dailies are exceedingly private, yet periodically, a reliably is spilled to the press. Precisely when this happens, studios rapidly endeavor to perceive the wellspring of the break. Obviously, if each duplicate of the well-ordered contains a one of a kind regard based watermark that perceives the bene…ciary, by then prominent af- …rmation of the wellspring of the break is impressively less asking. Another utilization of huge worth construct watermarks was passed with respect to by the DivX wander. DiVX displayed a changed understanding of DVD. One of the security tries executed in DivX equipment was a regard based watermark that could be utilized to see a player utilized for theft. On the o¤ chance that unlawful duplicates of a DivX …lm turned up on the mystery advertise, DivX could utilize the watermark to track them to the source. 1.11.7 Reproduction Controller Esteem based watermarks and besides watermarks for watching obvious proof, and check of proprietorship don't ruin unlawful replicating. Or then again, potentially, they …ll in as con- vincing obstructions and investigative mechanical congregations. In any case, it is likewise pragmatic for recording and playback gadgets to respond to presented signals. Subsequently, a yearly gadget may deter recording of a ‡ag on the o¤ chance that it perceives a watermark that shows recording is blocked. Obviously, for such a framework to work, every single made recorder must unite watermark recognizing veri…cation hardware. Such frameworks are begin- ning at now being made for DVD video and for motorized music disseminating. Abnormally, the uses of watermarks in a video to control equip retreats to no under 1989 and in sound to conceivably 1953. 1.12 Classi…cation of Computerized/Digital Watermarking We will discussed the division of watermarking with respect to di¤erent characteristics that are currently available for real time applications. The detail ‡ow diagram of classi…cation of watermarking is given in Fig. 1.8. Fig. 1.8: Classi…cation of Digital Watermarking Techniques. 1.13 Steganography Steganography is a sort of hidden correspondence. The term gets from the old Greek steganos (covered up) and grafein (composing/writing). While cryptography is proposed to ensure/ protect the contents of messages, creating limitless content, steganography shrouds the message itself, without leaving a trace of its reality. While steganography conceals a message inside another message, leaving the typical pic- ture, video or music record practically unaltered and regardless rolling out improvements to the …rst documents indistinct, cryptography encodes the message, making an arrangement of immense images. While an arrangement of realistic pictures, video or music documents inside which the message is covered up does not excite doubt, a record of boundless characters does. While steganography requires consideration while reusing pictures or music documents, cryp- tography requires consideration while reusing keys. While there is no con…nement in utilizing steganography, there are sure limitations utilizing certain types of cryptography. Fig. 1.9: General embedding and extracting scheme for information hiding. 1.13.1 Applications of Steganography There are di¤erent applications in steganography; it changes among the client prerequisites, for example, copyright control, incognito/covert correspondence/communication, smart ID's applications, printers and so on etc. [41]. 1.14 Assessment Factors for a Steganography Schemes The principle targets for any steganography calculation are limit, imperceptibility and vigor. In spite of the fact that it is troublesome for a steganography calculation to have every one of the attributes in the meantime, on the grounds that there is by and large exchange o¤ among these qualities [41]. 1.14.1 Capacity The measure of information to be installed in cover medium and can recovered later e¤ectively without altogether changing the cover medium. 1.14.2 Imperceptibility There ought to be no visual distinction amongst cover and stego question i.e. inserted message ought not be obvious to human eye. 1.14.3 Robustness A stego framework is said to be robust, in the event that it can support any assault and on the o¤ chance that it experiences change, for example, scaling, turn, …ltering and lossy pressure and so forth. It ought to stay in place. 1.14.4 Security An installing algorithm is said to be secure, if the inserted data couldn't be expelled after recognition by the eavesdropper. It depends on the information about the embedded algorithm and mystery key. 1.14.5 Embedding Rate It is by and large indicated in supreme estimation, with the end goal that the span of the mystery message or in relative estimation called information inserting rate given generally in bits per non zero DCT pixel coe¢ cient (BPNPC) and bits per pixel (BPP). 1.14.6 Indistinctness or Fidelity Stego pictures are relied upon not to have any critical visual curios under a similar level of security and limit. Higher devotion of stego pictures suggests better indistinctness. 1.14.7 Sort of Pictures Supported As images are accessible in countless, it is essential to comprehend which kind of pictures are appropriate for the steganographic technique of di¤erent sorts. Pictures essentially utilize lossy or lossless pressure instrument and the properties of pictures in‡uence the steganographic strategies pertinent to those pictures. 1.14.8 Time Complexity Steganographic algorithm di¤ers as per the space of inserting. In less complex frameworks, the inserting work is less tedious yet may not be as secure as some other more entangled frameworks o¤ering better execution. By and by, time multidimensional nature of a algorithm is critical for judging the relevance of scheme for inserting into huge pictures and furthermore their usage is low asset framework, for example, cell phones and so on. 1.15 Features of Robust Steganography Regardless of the way that steganography's most clear target is to cover data, there are a cou- ple of other related goals used to judge a method's steganographic quality. These join restrict (how much data can be hidden), intangibility (weakness for individuals to perceive a mutila- tion in the stego-question), indistinctness (disappointment for a PC to use experiences or other computational procedures to isolate among covers and stego-objects), vigor (message's ability to continue despite weight or other customary adjustments), change security/alter protection (message's ability to endure regardless of dynamic measures to wreck it), and ‡ag to commo- tion proportion (how much data is encoded versus what amount disengaged data is encoded). The three essential parts, which work in opposition to each other, are limit, impalpability, and heartiness. Extending one of these in‡uences the others to decrease; consequently, no stegano- graphic procedure can be faultlessly indistinct and powerful and have the most extreme limit. When in doubt, a limit of the data isn't as basic as the other two, and however watermarking favors strength most …rmly, general steganography considers subtlety the most fundamental. An once-over of the properties of good steganography is shown in …gure underneath. Fig. 1.10: Properties of Good Steganography 1.16 Basic Components of Steganography 1.16.1 Secret Message The message to be embedded 1.16.2 Cover Image An image in which secret message will be embedded. 1.16.3 Stego Image Cover image that contain embedded message. 1.16.4 Key Additional data that is needed for embedding and extracting process. 1.16.5 Embedding Steganography Algorithm Steganography algorithm used toembed secret message with cover image. 1.16.6 Extracting Steganography Algorithm Inverse function of embedding, in which

172**it is** used **to extract the** embedded message **(secret** message) **from stego image.**

1.16.7 Embedding Domain The Embedding area alludes to the cover medium qualities that are abused in inserting message into it. It might be spatial space, when coordinate alteration of the constituent components of the cover is changed (e.g. pixels in a picture) or it can be the recurrence area or change space if scienti…c changes are carried on the medium before inserting. 1.17 Steganographic Models Steganography can be divided into steganographic models, the principle ones being: i. Injective steganography; ii. Substitutive steganography; iii. Generative steganography; iv. Selective steganography; v. Constructive steganography. In injective steganography, the secret information is truly infused into the cover. Much of the time, this outcomes in an expansion in the memory control of the …rst cover and this might be a sign for a potential programmer to the presence of a mystery message inside the cover. Thusly, the bigger the measure of the cover is, the more data can be embedded, and the lesser the likelihood of location of the mystery message. In substitutive steganography, some portion of the data of the cover is properly supplanted with the mystery message data, decreasing however much as could reasonably be expected detectable quality of the adjustment. This procedure brings about no expansion to the span of the cover and in that capacity is exceptionally viable. It is a standout amongst the most usually 52 utilized methods. A run of the mill case is the substitution of the clamor in the correspondence channel with the mystery message. In generative steganography, the cover is truly created to duplicate, in a reasonable way, the mystery message utilizing a …tting calculation. This strategy is extremely successful in that it is exceptionally hard to recognize the nearness of a mystery message inside the cover. On the o¤ chance that the cover is a picture, it is still extremely hard to produce a sensible picture. In particular steganography, just records that as of now have a property are chosen, from each one of those conceivable documents, and this property is utilized to shroud the mystery message. Thus, this system is extremely tedious and all things considered is seldom utilized despite the fact that it is exceptionally impervious to assaults. In constructive steganography, the operation is fundamentally the same as that of the substi- tution steganography. When all is said in done, it is abused by utilizing the channel commotion, where a …tting model is …rst developed and afterward supplanted the clamor with the mystery message, continually following the model made. Indeed, even for this situation, it is greatly hard to capture the mystery message, yet its shortcoming is in making a legitimate clamor demonstrate. 1.18 Steganographic Protocols The three basic types of steganographic protocols are: 1.18.1 Pure Steganography We call a steganography framework unadulterated when it doesn't require earlier trade of some mystery data before sending information. De…nition 34 A pure steganography is consisting of four parts (C;S

> 51**;D;E); where C is the set of possible covers,** S **is the set of secret** massages **with** jCj jSj, E : **C** S ! **C;the embedding function and D : C** ! S; is **the extraction function with the property that D(E(c;**

s)) = S 8 c 2 C and s 2 S: 1.18.2 Private Steganography We call a steganographic framework a private when it require an earlier trade of information like shared keys. In this case, sender chooses the cover and installs the mystery knead into the cover utilizing a mystery key. On the o¤ chance that the mystery enter utilized as a part of inserting process, is known to the recipient he can switch the procedure and concentrate the mystery rub. De…nition 35 A private key steganography is consisting of …ve parts (C; S; K; EK ; DK);

> 150**where C** is **the set of possible covers,** S is **the set of secret**

massages,

> 63**K is the set of** secret **keys, EK : C** S **K ! C;the embedding function and** D : **C K** ! S; **is the extraction function** with **the property that DK (EK (c;**

s)) = s 8 c 2 C; s 2 S and k 2 K: 1.18.3 Asymmetric Steganography This sort of steganography does not depend on shared key trade. Rather it depends on people in general

> 135**key cryptography,** guideline **in which there are two keys one being** open **key which**

can be typically acquired from the general population database and the other a private key. For the most part for this situation people in general

> 155**key is** utilized **as a** part **of the** inserting procedure **and** the **private key** in **the**

disentangling procedure. Fig. 1.11: Classi…cations of Steganographic Algorithms. 1.19 Signi…cance of Cryptography, Steganography and Water- marking The space of digital security is growing practically consistently. It has turned into a multi- disciplinary operation. The quantity of cyber incidents is on the rise. A few security …rms have recognized numerous updates to misuse packs which have as of late begun utilizing steganog- raphy as a fundamental part of their operations as they utilize steganography as an approach to shroud abuses and malware payloads as PNG records. The Stegano abuses pack (otherwise called Astrum) is utilized to exchange diverse malevolent code by means of PNG ‡ag adver- tisements. Once a web program hits such sites, JavaScript will extricate the code from the PNG document and divert the client to an alternate site that will taint the PC with malware. This recently refreshed endeavor unit was utilized by numerous malvertising e¤orts to circulate malware. The most in‡uenced nations were Japan, Canada, and France, however Japanese clients represented over 30% of the aggregate target. Steganography has been helpful in ensuring media copyrights (through computerized watermarks). Unfortunately, there may be a larger number of drawbacks than bene…ts. On the extraordinary end, fear based oppressor associations totally depend on steganography as their methods for correspondence. It is utilized to pass mystery messages without anybody yet the planned bene…ciaries monitoring it. For instance, what has all the earmarks of being a family photograph may surreptitiously contain the plans for an arranged psychological oppressor assault. Shockingly, steganography is likewise giving chances to cybercriminals. There are numerous steganography instruments at present accessible running from open source to business items. These instruments give a lot of alternatives for cybercriminals. To battle this issue, there is a requirement for people who know how to recognize and unscramble this concealed information. Just a couple of scholarly establishments o¤er these courses that spend signi…cant time in these innovative regions. These advances ought not be limited to just a couple of passages or parts in existing courses. They ought to be o¤ered as partitioned courses in cryptography, steganography, and watermarking. The objective of these three advancements is the same, to secure correspondences to just the expected sender and ben- e…ciary. These courses ought to be o¤ered in an organized arrangement that manufactures a far reaching comprehension of the idea, hypothesis, and utilization of cryptography, steganography, and watermarking. The capacity to split encoded records and …nd messages covered up through steganography will get ready understudies as they enter a world in which digital …ghting has turned into the standard. This will …ll in as a door to more particular, speci…c courses driving them to vocations in steganalysis, cryptography, cryptology, computerized media (sound, video, and pictures) legal sciences, and digital criminal investigation. 1.20 Some Di¤erences in Information Security

200**Systems In this section, we** mainly **discuss the** di¤erences among **the**

di¤erent information security systems. 1.20.1 Steganography Versus Watermarking The fundamental

32**objective of steganography is to conceal a message m in some sound or video (cover) information** C, **to** acquire **new information** C0, **for all intents and purposes** vague **from** C; **by individuals, such that a** busybody **can't distinguish the nearness of m in** C0: **The** primary **objective of watermarking is to** conceal **a message m in some sound or video (cover) information** C, **to** acquire **new information** C0, basically unclear **from** C, **by individuals, such that a** busybody **can't** evacuate **or supplant m in** C0. **The**

data covered up by a watermarking framework is constantly related to the advanced question be ensured or to its proprietor while steganographic frameworks simply shroud any data "heartiness" criteria are likewise unique, since steganography is fundamentally worried about identi…cation of the concealed message while watermarking concerns potential evacuation by a privateer steganographic correspondences are normally point-to-point (amongst sender and collector) while watermarking systems are generally one-to-many. 1.20.2 Cryptography Versus Watermarking Cryptography is the most widely recognized technique for ensuring computerized content and is extraordinary compared to other created science. Be that as it may, encryption can't enable the dealer to screen how a true blue client handles the substance after unscrambling. Computerized watermarking can ensure content even after it is decoded. 1.20.3 Cryptography Versus Steganography Cryptography is the examination of hiding information, while Steganography oversees framing covered messages so simply the sender and the bene…ciary understand that the message even exists. In Steganography, simply the sender and the bene…ciary know the nearness of the mes- sage, however in cryptography the nearness of the mixed message is clear to the world. Along these lines, Steganography empties the bothersome thought setting o¤ to the covered message. Cryptographic procedures try to guarantee the substance of a message, while Steganography uses techniques that would stow away both the message and what's more the substance. By solidifying steganography and cryptography one can achieve better security. In essential words, cryptography is tied in with securing the substance of messages (their signi…cance) and steganog- raphy is tied in with camou‡aging the nearness of messages. 1.21 Combination of Di¤erent Security Techniqes 1.21.1 Joined Cryptography and Steganography Both the systems can be consolidated to give one more level of insurance. The message can be …rst scrambled utilizing cryptography to encode the given information. This encoded message at that point can be implanted in a cover media utilizing steganography. This consolidated approach will ful…ll the three objectives of information concealing: security, limit, robustness. 1.21.2 Joined Watermarking and Steganography To secure the validness of the information, watermarking can be connected to it. This water- marked record can be implanted in the cover image by utilizing a stego-key and transmitted over the correspondence medium. At the collector end, the data can be …rst decoded utilizing the turnaround system and after that it can be approved for its genuineness utilizing the wa- termarking. This consolidated approach will ful…ll each of the four objectives of information concealing: security, limit, vigor, and detectable quality. 1.22 Cybersecurity vs. Network Security vs. Information Se- curity We are in a period where organizations are more carefully progressed than any other time in recent memory, and as innovation enhances, associations' security stances must be improved too. Inability to do as such could bring about an expensive information rupture, as we've witnessed with numerous organizations. Risk actors are pursuing any kind of association, so with a speci…c end goal to ensure your business'information, cash, and notoriety, it is important that you put resources into a propelled security framework. Be that as it may, before you can begin building up a security program for your association, it's important that you comprehend the diverse sorts of security and how they all cooperate. 1.22.1 Information security Data or information security (otherwise called InfoSec) guarantees that both physical and ad- vanced information is shielded from unapproved get to, utilize, revelation, interruption, ad- justment, review, recording or decimation. Data security contrasts from cybersecurity in that InfoSec intends to keep information in any frame secure, though cybersecurity ensures just computerized information. On the o¤ chance that your business is beginning to build up a security program, data security is the place you should initially start, as it is the establishment for information security. At the point when InfoSec specialists are creating arrangements and techniques for a suc- cessful data security program, they utilize the CIA (secrecy, integrity and availability) group of three as a guide. The CIA group of three has turned into the true standard model for keeping your association secure. The three crucial standards help fabricate an incredible arrangement of security controls to safeguard and ensure your information. 1.22.2 Cybersecurity Cybersecurity, a subset of data security, is the act of protecting your association's systems, PCs, and information from unapproved computerized access, assault or harm by executing di¤erent procedures, advancements and practices. With the incalculable re…ned danger actors focusing on a wide range of associations, it is important that your IT foundation is secured constantly to keep a full-scale assault on your system and hazard uncovering your organization'information and notoriety. At the point when digital danger actors focus on your association, they investigate your business, as well as your workers too. They realize that workers outside of IT security aren't as mindful of digital dangers, so they execute cyber-attacks that adventure human vulnerabilities. Through the procedure of social designing, danger actors control individuals into giving the entrance to touchy data. As a business pioneer, it is your duty to assemble a culture of security mindfulness and …ll in the holes in your group's cybersecurity information and comprehension. It's basic that your workforce is educated of cybersecurity dangers, so it will be more improbable for a representative to succumb to an assault. Give your workers the vital preparing and innovation to fortify your association's human …rewall and moderate the likelihood of a digital assault. 1.22.3 Network security Network security, a subset of cybersecurity, plans to ensure any information that is being sent through gadgets in your system to guarantee that the data isn't changed or captured. At the point when your system security is traded o¤, your …rst need ought to be to get the aggressors out as fast as could be expected under the circumstances. The more they remain in your system, the additional time they need to take your private information. As indicated by Ponemon Institute's 2013 Cost of Data Breach ponder, barring disastrous or uber information security breaks, the normal cost of an information rupture for each bargained record in the U.S. is $188. The normal total cost to an association in the U.S. is more than $5.4 million. The best technique for reducing the total cost is by getting the aggressors out of your system at the earliest opportunity. Fig. 1.12: Fundamental Security Classi…cations. 1.23 Conclusion The aim focus of this chapter is to characterized the applicable supporting concepts of Boolean functions, nonlinear component of block ciphers, cryptography, watermarking and steganogra- phy. Speci…cally, we have given various since a long time ago settled de…nitions and hypotheses for di¤erent parts of the hypothesis. The important

16**cryptographic properties which are** utilized **to** investigate **the** quality **of single and multiple output functions have** likewise **been** character- ized **and** talked about. **The**

main point of this part of the theory is to give a study of existing data hiding techniques, their central focuses and preventions. A couple of methodologies for hiding data in content, picture, and sound are depicted, with proper acquaintances with the earth of every medium, and additionally the qualities and weaknesses of every procedure. Most data disguising structures misuse human perceptual de…ciencies, yet have weaknesses they could call their own. In zones where cryptography and encryption are being denied, locals are look- ing to circumvent such methodologies and pass messages covertly. Business employments of modernized watermarks are at present being used to track the copyright and responsibility for media. This section moreover explains why data concealing is grabbing noteworthiness these days and the destinations that must be pro…cient by any data hiding system. The essentials of cryptography, watermarking and steganography are presented that will help us similarly in di¤erent parts of this thesis. Chapter 2

2**A Color Image Watermarking Scheme Based on** A¢ ne **Transformation and** S4 **Permutation**

With the improvement of computerized innovations and internet advances, digital contents could be e¤ectively acquired by means of diverse transmission channels, for example, internet, remote systems. Because of focal points of digital technologies, impeccably recurrent and e¤ort lessly adjusted, numerous issues have gotten more attention, for example, copyright security and content authentication. Particularly speaking, from perspectives of content suppliers, they need to present or o¤er their items through systems or di¤erent channels without dangers of any privateer. Subsequently, contents suppliers are excited to discover some novel measures to ensure their items. Also, in the wake of accepting a bit of computerized substance from authentic channel, clients expect that their gained item is simply from the genuine trader and is the …rst items without any alteration. Subsequently, there ought to be a validation component that backings the security of this kind activity and its way. Luckily, one making a guarantee to technology to unravel these issues has been proposed from the earliest starting point of 1990s, that is computerized watermarking, which is appropri- ating operations by putting additional data over host ones and is utilized for content veri…cation, tracking, copyright assurance, phony aversion and numerous other purposes [19]-[24]. Water- mark could be characterized into two types according to its utility, namely robust watermark for copyright security and fragile watermark for integrity con…rmation. The dominant part of watermarking strategies is to apply watermarks formed from pseudo-irregular number arrange- ments [21]-[27]. Chaotic maps such logistic map, skew map, cat map and Bernoulli maps have been generally used to produce water-mark sequences [28]-[29]. These watermarking systems can o¤er vagueness, security and strength as examined in [30], however, the fundamental obstruction lies in the implanting of the watermark in the original image. The binary map as a watermark is acquired by the development of pseudo- irregular arrangement of real numbers. As of late, chaotic structures have been utilized within watermarking mechanisms. In [31], a system for image watermark focused around chaotic sequences provided by diverse functions. The chaotic watermarking plan that embeds the chaotic sequence in the frequency domain was accounted in [32]. The signi…cant

9**purpose of** advanced **watermarking is to discover the** equalization **among the** view points, **for example,** vigor **to**

di¤erent assaults, sanctuary and imperceptibly. The invisi- bility

9**of watermarking** method **is focused around the** power **of implanting watermark.** Improved hiddenness **is attained for** a reduced amount of force watermark. Therefore,

9**we must select the ideal** force **to** embed **watermark. There is** slight compromise **between the**

embedding strength and quality. Increase robustness obliges stronger embedding that

9**builds the visual** damage **of the** images. **For a watermark to be** powerful, **it ought to**

vagueness, promptly extractable, un- mistakable and vigor. The

9**digital image watermarking** schemes **can be divided into two** classes. These **are visible** watermarking and invisible **watermarking** strategies. Visible **watermarking,**

the data are obvious

66**in the picture or video.** Commonly, **the information is** content **or a logo which** distinguishes **the** holder **of the**

original documentation. Invisible watermarking, data are

66**added as digital** information **to** sound, **picture or** feature; however, **it cannot be** seen **as**

being what is indicated. Further, the undetectable watermarks are arranged into watermarking pro- cedures as delicate and vigorous. For the most part, a vigorous imprint is by and large utilized for copyright assurance and proprietorship distinguishing proof

9**on the grounds that they are** in- tended **to withstand** assaults, **for example,** regular **picture** preparing **operations, which endeavor to** uproot **or** demolish **the** imprint. **These** calculations guarantee **that the**

picture transforming operations do not delete the implanted watermark indicator. Then, again a delicate or semidel- icate watermark is predominantly connected to content con…rmation and honesty check in light of the fact

9**that they are extremely touchy to** assaults, **i.e., it can identify slight** progressions **to the watermarked** picture **with high**

likelihood.

139**For a watermark to be** e¤ective, **it should satisfy the following features**

[33]: 1. Imperceptibility: It ought to be perceptually undetectable so that information quality is not corrupted and aggressors are kept from discovering and erasing it. 2. Promptly extractable: The information manager or a free control power ought to e¤ortlessly separate it. 3. Unambiguous: The watermark recovery ought to clearly recognize the information holder. 4. Robustness: It ought to endure a percentage of the regular image processing assaults. A few routines have been proposed in writing.

9**Two classes of digital watermarking** algo- rithms **are spatial** space methods **and recurrence**

area strategies. Least signi…cant bit (LSB) will be the least complex method in the spatial space procedures which speci…cally changes the

9**intensities of some** selected **pixels. The recurrence area** method **converts a picture into a set of recurrence space** coe¢ cients. In characteristic

9**based watermarking plan, watermark** will be created **by applying a few operations on the pixel estimation of host picture** rather than **taking from** outside **source. Late** explores **on secure advanced watermarking** strategies **have uncovered the way that the substance of the pictures could be utilized to enhance the imperceptibility and the power of a watermarking plan**

[34]-[39]. This chapter suggests a novel methodology for watermarking which is a gigantic exploration territory that is dynamically developing. This scheme is basically based on applying the Galois …eld GF (24), S4 permuta- tion and least signi…cant bits. The investigation of these methods prompts systems for assaults and counter measures which are utilized to discover blames and limitations in applications, empowering the improvement of better ones. Computerized watermarking is distinctive relying upon its strategies and applications. The extent of this examination is invisible computerized image watermarking for color images. The exploratory consequences of the proposed strategies are dissected utilizing entropy, contrast, homogeneity, energy, means square error, root

1**means square error, mean absolute error, peak signal-to-noise ratio,** universal **image**

quality index, mu- tual information, structural similarity, structural dissimilarity and structure content are

101**used to measure the similarity between the** cover **image and** watermarked **image**

[43]-[44],[67]-[68], [45]. 2.1 Some Algebraic De…nitions 2.1.1 De…nition Let V and W be real vectors paces (their dimensions are di¤erent) and let T be a function with domain V and range in W (written as

98**T : V** ! W). **We say T is** a linear transformation **if For all** ; 2 **V;**

T (+) = T ( ) + T ( ), (T is additive), For all 2 V; 2 R; T ( ) = T ( ), (T is homogeneous). 2.1.2 De…nition

168**A mapping** T **from V n to V m is**

an a¢ ne transformation if T is linear mapping followed by a translation. In other words, there exist a matrix A and vector b

65**such that** T **(x) = Ax + b; for all x. The**

nonlinear component of AES is fundamentally based on a¢ ne transformation [43]

118**y = Ax** b **mod m(x);** (2.1) **where A**

2 GL8(F2); b 2 Mn 1(F2) and

118**m(x) is an irreducible polynomial in**

F28: To be useful as nonlinear component of block cipher

196**generator, matrix A should be non-singular.** The new techniques **can**

easily be derived with the basis from F28. As F28 is a …nite …eld,

37**therefore, the multiplicative inverse of every element exists and 0 ! 0. This multiplicative inversion for the function** K **(x) is as follows:** K **(x)** = x1 **0** x6 = **0;** **x = 0:** (2.2) **The** a¢ ne **transformation is decomposed** into **two steps: 1.** T **(x) be a linear** mapping de…ned over F28 given as: T (x) = Ax: (2.3) 2. The AES which is famous block cipher, its nonlinear component involves an a¢ ne function G(x) in over F28 as: G = x d: The original nonlinear component of block cipher

37**of AES is the composition of these functions given as** [43]: AES **Sbox**

= G T K; (2.4) which clearly represents the a¢ ne transformation in AES nonlinear component of block cipher. 2.2 Algebra of New Watermarking

2**Technique The proposed watermark technique is based on small** …eld **of sixteen elements ,i.e., GF** (24) **whose elements have of the form:**

F24 = F2[x] (x4 + x + 1) ; = fb0 + b1 x + b2 x2 + b3 x3; bi 2 F2g; (2.5) (2.6) where p

92**(x) = x4 + x + 1;** is **a primitive** irreducible **polynomial of degree 4. The**

2**following table** represents **the elements of** F24 **along with its inverse elements and their corresponding binaries**

(Table 2.1). Table 2.1: Representation of Galois …eld GF (24) and its inverse elements. Elements Binary Multiplicative Binary of GF (24) representations inverses of representations of of GF (24) each elements inverse elements of GF (24) of GF (24) 1 0001 1 0001 2 0010 9 1001 3 0011 14 1110 4 0100 13 1101 5 0101 11 1011 6 0110 7 0111 7 0111 6 0110 8 1000 15 1111 9 1001 2 0010 10 1010 12 1100 11 1011 5 0101 12 1100 10 1010 13 1101 4 0100 14 1110 3 0011 15 1111 8 1000 The S-

74**box is generated by determining the multiplicative inverse for a given number in**

F24 = F2[x] =(x4 + x + 1) = fb0 + b1 x + b2 x2 + b3 x3; bi 2 F2g. The

2**multiplicative inverse is then transformed using the following** a¢ ne **transformation:** AES **Sbox = G** T K; **where** T **(x) is the** F2 **linear mapping**

and matrix over F2 is used to describe the F2 linear matrix. The

2**circulant matrix over** F2 **is of the form**

[44] 1110 2 0111 3 : 1011 6 1101 4 7 5 Finally, we have apply the permutations to each elements of a¢ ne mini nonlinear component of block ciphers which can be represented by: S4 AES Sbox = P (G L K); where P T = [e (1); e (2); :::; e (m)] 2 S4 (symmetric group) and ej

95**denotes a row vector of length m with 1 in the jth position and 0 in every other position**

(Tables 2.2, 2.3, 2.4). The proposed mini S4 S-box is given as follows: Table 2.2: Inversion in F24 : I nput 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 Output 0 1 9 14 13 11 7 6 15 2 12 5 10 4 3 8 Table 2.3: F2–linear mapping in F24: I nput 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 Output 0 13 11 6 13 7 10 1 14 3 5 8 9 4 2 15 Table 2.4: Proposed mini S-box. inj 0 1 2 3 0 1 2 3 12 11 2 9 3 14 7 13 15 1 0 5 4 10 6 8 2.2.1 Least Signi…cant Bits The least signi…cant

2**bit (lsb or LSB) is the bit position in** an adjusting entire **number giving the units** regard, **that is,** making sense of **if the number is even or odd.** It is like **the**

least signi…cant

2**digit of a decimal number, which is the digit in the ones (right-most) position**

[29]-[30]. 2.2.2 Most Signi…cant

2**Bits The most** signi…cant **bit (msb or MSB,** similar to insightful **called the high-** arrange **bit) is the bit position in a parallel number having the** most noteworthy esteem. **The msb is**

now and again proposed to as the furthest left bit as a result

2**of the** gathering **in positional documentation of** forming **more** signi…cant **digits further to**

one side. 2.2.3 Suggested Copyright Protection

2**Scheme In this section, we have implemented the proposed** algebraic **structure to watermarking. Our main purpose here is to hide an invisible watermarked with the help of proposed**

small nonlinear components of block ciphers and least signi…cant digits (see Fig. 2.1). The algorithm

2**of the proposed watermarking scheme** is give **as follow: Algorithm**

36 1. Choose a digital image, 2. Convert values of every pixels into a string

2**of eight bits, 3.** Distribute **MSBs and LSBs for each pixel,**

4. Apply nonlinear

2**transformation on LSBs that signify the position of values in** S4 S **box;**

5. S4 S

2**-box that has to be replacing with binaries of LSBs**

of an image, 6. Reiterate step 5

2**until the whole image is replaced,** 7. Finally, reconstruct **MSBs and transform LSBs.**

Read an image Use S-box transformation to an

2**Transform values of each pixel into** element **of**

selected S-box. binary of fixed length 2 bits Splitter i= Transform

2**MSB of 4 bits LSB of 4 bits**

bits into decimal 2 bits j = Transform bits into decimal Select element at (i,j) Convert each element of position from S-box S-box with four binary Insert

2**4 bits binaries of S-box with LSBs of image** Reconstruct **image** Watermarked image Combiner **MSB of image LSB of image End Fig. 2.**

1: Suggested watermarking scheme based on GF (24) and LSBs.

140**(a) (b) (c) (d) Fig. 2.** 2: **(a)** (c) **Original** and watermarked lena **image** of size **512 512**

3; (b) (d) 3D histogram visualization of original and watermarked lena image of 512 512 3: 2.3 Statistical Analyses In this section, we primarily talked about some tests which will show the competence of our proposed watermarking design [67]-[45]. 2.3.1 Entropy

3**Entropy is a** factual **measure of randomness that** might **be** utilized **to** portray **the** surface **of the** picture. **Entropy is** characterized **as:** N **H = p(**

xj) logb p(xj): (2.7) j=0 P Table 2

3**.5 shows the results of entropy analysis of the** original and watermarked **images.**

These analyses show that there will be no leakage of information in original and watermarked images. 2.3.2 Contrast The contrast dissection of the picture empowers the

3**viewer to vividly** distinguish **the objects in** surface **of** a picture. **The**

watermarked picture same contrast levels as unique picture.

3**We measure the contrast parameters of the** watermarked picture **and** assess **the** adequacy **of**

non- linear components of block ciphers in watermarking applications. This investigation gives back

3**a measure of the intensity contrast between a pixel and its neighbor over the** entire picture **and is mathematically represented as:** n 1m 1 **C** = ji jj2 p **(i;j);**

(2.8) i=0 j=0 P P

3**where the number of gray-level co-occurrence matrices is represented by p(i; j).** Table 2.5, **shows the results of contrast analysis when applied to** watermarked **images corresponding to various**

nonlinear components of block ciphers. 2.3

75**.3 Homogeneity The homogeneity** investigation **measures the closeness of the** dispersion **of** components **in the** gray **-level co-occurrence matrix (GLCM).**

The GLCM demonstrates the facts of combinations

19**of pixel** shine **values or** gray **levels in** plain structure. **The** recurrence **of the** examples **of** gray **levels** might **be** translated **from the GLCM table. The** mathematical expression of **homogeneity** is given **as**

follow: n 1m

165**1 K = p(i; j) i=0 j=0**

1 + ji jj ; (2.9) P P

3**where the gray-level co-occurrence matrices in GLCM is represented by p(i;j).**

Tables 2.5 and 2.6 show the results of homogeneity analysis for watermarked image. 2.3.4 Energy

3**In this analysis, we measure the energy of the** watermarked **images as processed by various**

nonlinear components of block ciphers.

75**This measure gives the sum of**

3squared elements in the gray-level co-occurrence matrix: E = p (i;j)

2; (2.10) i;j P

3where p(i; j) is the number of gray-level co-occurrence matrices. The numerical values of

en- tropy, contrast, energy and homogeneity

6show that our proposed scheme is robust. The

tabu- lated measures clearly elucidate that our scheme is useful and quite compatible with applica- tions. Table 2.5: Comparison of

68entropy, contrast, energy and homogeneity analyses of proposed S- box for original and watermarked images. Analysis Original image Watermarked image Entropy 7.8362 7. 8263 Contrast 0.

2988 0.3199 Homogeneity 0.8960 0.8854 Energy 0.0955 0.0908 Table 2.6: The comparison

68of entropy, contrast, energy and homogeneity analyses of proposed S-

box for color components of original and host images. Proposed Properties Color image

2components of original image Red Green Blue Color image components of watermarked image

Red Green Blue Entropy 7.7637 7.8664 7.7226 7.7700 7.8472 7.7284 Contrast 0.3014 0.2914 0.2966 0.3140 0.2972 0.3075 Homogeneity 0.1129 0.0962 0.1090 0.1089 0.0949 0.1061 Energy 0.8941 0.9000 0.8975 0.8879 0.8967 0.8914 2.3.5 Mean Squared

5Error To evaluate the reliability of the proposed algorithm, mean square error (MSE) between marked image and original image is measured. MSE is calculated using the following equation: "MSE = M 1 N Xi=1Xj =1 (f (i; j) g (i; j

))2 ; (2.11) M N

5where M N is the size of the image. The parameters f (i;j) and g (i;j) refer to the pixels located at the ith row and the jth column of original image and marked image, respectively

(see Fig. 2.1). The

6larger the MSE value, the better the watermarking quality (Fig.

2:1). 2.3.6

6Root Mean Square Error To evaluate the proposed watermarking system, this method is tested on the color Lena image of 512 512 pixels as shown in Fig.

2:2 (a) and 2:2 (b). The marked result is shown in Fig. 2:2 (c) and 2:2 (d). To find the accuracy

6of the results and the robustness of the watermarking, a root mean square of error is calculated. These criteria provide the error between source image and watermarked image. The RMSE value can be described by the following relation: RMSE = 1 M N

182(f (i; j) g (i; j))2 ; (2.

12) t vM u N Xi=1Xj

6=1 where the f(i;j) is the pixel intensity of the original image and g(i;j) is the pixel intensity of the watermarking image. The row and column numbers of these two images are de…ned by M N. 2 .3. 7 Mean Absolute Error To evaluate the

29reliability of the proposed algorithm, mean absolute error (MAE) between watermark image and original image is measured. MAE is calculated using the following equation MAE = M 1 N

Xi=1Xj=1 jf

205(i;j) g (i;j)j; (2. 13) M N

5where M N is the size of the image. The parameters f (i;j) and g (i;j) refer to the pixels located at the ith row and the jth column of original image and marked image, respectively.

2.3.8

5Peak Signal to Noise Ratio The watermarked image quality is evaluated using peak signal-to-noise ratio (PSNR) which is described by the following expressions: PSNR = 10log2 MIm2SaEx ; (2.

14)

5where Imax is the maximum of pixel value of the image. The PSNR should be a low value which corresponds to a great di¤erence between the original image and marked image. The e¤ectiveness of the proposed method, evaluated in terms of MSE and PSNR are tabulated in Table

2.7. 2.3.9 Universal Image Quality Index

186Let X and Y be two digial images consists of

N N pixels each. The universal quality index is de…ned as: Q = 4 XY XY (X2 + 2Y)(X2 + Y 2) ; (2.15)

105where X is a mean of X, Y is a mean of Y, 2X standard deviation of X, 2Y standard deviation of Y

72and XY is a covariance of X and Y respectively. 2.

3.10 Structure Similarity The structural similarity (SSIM) index is a technique

43for measuring the similarity between two pictures. The SSIM metric is calculated on various sizes of an image. The measure between original and marked images of size N N is:

(2XY +b1)(2 xy+b2) SSIM(X;Y)= (X2+Y2+b1)(2x+ 2y+b2) ; (2.16) where X

46is the average of X; Y is the average of Y , x is standard deviation of X, y is standard deviation of y and xy is covariance of X and Y , b1 = (k1L)2; b2 = (k2L)2

two variables which is **to stabilize the weak denominator, L is the** dynamics **range of the** pixels **-values.**

2.3.11 Mutual Information Shared/mutual data is an essential idea from information theory, estimating the factual re- liance between two irregular factors that one variable contains about the other. The mutual information is given as takes after:

55**I(x; y) = p(x; y)** ; (2.17) xX2XyX2Y **p(x; y)** log **p(x)p(y) where p(x; y) is joint probability** distribution **function of** original **and** marked images **and p(x); p(y) are the** probability **density functions**

in the individual images. 2.3.12 Structure Dissimilarity/Uniqueness Structural dissimilarity (DSSIM) is a separation metric got from SSIM (however the triangle imbalance isn't really ful…lled) DS S I M (X; Y) = 1 S S I M (X; Y) 2 : (2.18) This analysis basically analyze the dissimilarities between original and watermarked images. 2.3.13 Structure Contents The structure content (SC) of original and watermarked images is de… ned as follow: n m [f(n;m)]2 SC = nP=n1mPm=1 ; (2.19) [g(n;m)]2 n=1m=1 P P where f

143**(n; m) is** an **original image and** g **(n; m) is** a watermarked **image.** Table 2.7: **The**

numerical results of MSE, PSNR, RMSE, MAE, UIQI, MI, SSIM, DSSIM and SC of proposed S-box for color watermarked image. Proposed Analyses Color

1**image Color** image **components** of **watermarked image Red Green Blue**

MSE 8.73510 11.4537 10.1302 11.8925 PSNR 38.7181 37.5414 38.0746 37.3781 RMSE 2.95550 3.38430 3.18280 3.44860 MAE 2.17580 2.50400 2.33680 2.57840 UIQI 0.85250 0.83820 0.85060 0.86110 MI 0.25313 0.25059 0.25646 0.23425 SSIM 0.95030 0.9447 0.9476 0.9447 DSSIM 0.02485 - - - SC 1.00100 1.0018 1.0009 1.0004 The values of MSE, PSNR, RMSE, MAE, UIQI, MI and SSIM clearly elucidate the authenti- cations of robustness in our proposed algorithm. As it is evident from the analysis of Table 2.7, lower MSE, RMSE, MAE values and higher PSNR values imply good embedding results where are higher values (in probability sense) of UIQI, SSIM and lower values of MI signify that there is no change after watermarked is placed in original image and no sharing between the original and host image. Also values of SC and DSSIM represent good embedding quality. 2.4 Conclusion The principal idea of this part of the thesis is to develop a novel technique for digital copyright for advanced digital mediums. There has been a vast amount of literature available for the con- struction of new algorithms for digital watermarking and information hiding techniques. There are various new teachnues which are based on spatial and frequency domains were available in writing. Our suggested technique which is basically based on LSBs insertion with the help of new proposed nonlinear components of block cipher, which is quite easy and more e¤ective design methodology as compared to other schemes. The suggested design of digital copright protection is robust due to its algebraic as well as statistical charactersitics. Chapter 3 Construction of New nonlinear components of block ciphers Based on Permutation Matrices and its Implementation in Digital Patent Security Multimedia technology is being widely used nowadays. Besides, computer networking has also become a lot common which resulted in problems regarding copyright protection of digital con- tent (audio, video and image). Regarding copyright protection, digital watermarking/patent security has proved to be very potent and favorable.

173**One of the main advantages is that** one can hide **information**

in images using this technique. This technique has advantages such as it provides protection, robustness and the quality of being unnoticeable but to that, there is a hindrance. In this chapter, we have designed a novel procedure

1**for the construction of** substi- tution boxes **(nonlinear components of block**

ciphers) which is mainly based on permutations matrices of S4 and Galois …eld GF (24). We have analyze our nonlinear components of block ci- phers with statistical analyses along with watermarking application. The scope of this research is invisible digital image watermarking for color and gray-scale images. We have testi…ed our nonlinear components of block ciphers through some algebraic and statistical analyses. The al- gebraic analysis includes

77**Nonlinearity, Strict avalanche** criteria **(SAC), Bit independent** criteria **(BIC), Linear** approximation probability (LP) **and** Di¤erential **approximation probability** (DP) whereas statistical **tests**

113**are Mean squared error (MSE), Mean absolute error (MAE), Peak signal to noise ratio (PSNR),**

85**Universal image quality index (UIQI) and Structural similarity (SSIM).**

3.1 Basic De…nitions In this section, we have presented some basic de…nitions of permutations and their algebraic properties which will be useful in next sections. 3.1.1 Permutations Let X

98**be a non empty set** with n objects. **A** permutation **of a**

set X is a mapping : X ! X that is a one-to-one and onto mapping that is bijective transformation. 3.1.2 Permutation Matrix

97**A permutation matrix is a square matrix obtained from the same size identity matrix by** a **permutation of** rows. Such a **matrix is**

always row equivalent to an identity. (see Table 3.1). Table 3.1: Permutation matrices of S4: Elements Cycle decomposition notation Matrix (right action) Order of element 1000 0 0100 1 1 () 1 0010 B 0001 @ C A 1000 0 1 2 (3,4) 0100 2 0001 B 0010 @ A C Elements Cycle decomposition notation Matrix (right action) Order of element 1000 0 0 0 1 0 1 3 (2,3) 2 4 (2,3,4) 5 (2,4,3) 6 (2,4) 7 (1,2) 8 (1,2)(3,4) 9 (1,2,3) 0100 B 0001 @ C A 1000 0 0001 1 0100 B 0010 @ A C 1000 0 0010 1 0001 B 0100 @ A C 1000 0 0001 1 0010 B 0100 @ A C 0100 0 1000 1 0010 B 0001 @ A C 0100 0 1000 1 0001 B 0010 @ A C 0100 0 0010 1 1000 B 0001 @ A C 2 3 2 2 2 3 Elements Cycle decomposition notation Matrix (right action) Order of element 0100 0 0 0 1 0 1 10 (1,2,3,4) 4 0001 B 1000 @ C A 11 (1,2,4,3) 0 0100 0001 1000 0010 1 @ B A C 4 12 (1,2,4) 0 0100 0001 0010 1000 1 @ B A C 3 13 (1,3,2) 0 0010 1000 0100 0001 1 @ B A C 3 14 (1,3,4,2) 0 0010 1000 0001 0100 1 @ B A C 4 15 (1,3) 0 1 @ B 0100 0001 1000 0010 A C 2 16 (1,3,4) 0 0010 0001 0001 1000 1 @ B A C 3 Elements Cycle decomposition notation Matrix (right action) Order of element 0010 0 0 0 0 1 1 17 (1,3)(2,4) 2 1000 B 0100 @ C A 18 (1,3,2,4) 0 0010 0001 0100 1000 1 @ B A C 4 19 (1,4,3,2) 0 0001 1000 0100 0010 1 @ B A C 4 20 (1,4,2) 0 0001 1000 0010 0100 1 @ B A C 3 21 (1,4,3) 0 0001 0100 1000 0010 1 @ B A C 3 22 (1,4) 0 0001 0100 0010 1000 1 @ B A C 2 Elements Cycle decomposition notation Matrix (right action) Order of element 0001 0 0 0 1 0 1 23 (1,4,2,3) 4 1000 B 0100 @ C A 0001 0 0 0 1 0 1 24 (1,4)(2,3) 2 0100 1000 @ B A C 3.1.3

52**Permutation Group A permutation group is a** …nite **group G whose elements are permutations of a given set and whose group operation is composition of permutations in G. Permutation groups have orders dividing n!.**

3.2 Mathematical Structure of Suggested Nonlinear Compo- nent The nonlinear componet

74**is generated by determining the multiplicative inverse for a given** num- ber **in**

GF (24): The nonlinear component transformation therefore consists of three functions, namely linear transformation L, invertible function I and a¢ ne transformation G : S(x) = G L I: (3.1) The proposed symmetry group S4 based nonlinear components of block ciphers are given as follows (see Table 3.2): S box = S4 S; (3.2) which is action of S4 over small AES nonlinear components of block ciphers. Table 3.2: Elements of proposed nonlinear components of block ciphers. S1 12 13 5 2 1 7 11 10 3 14 0 9 6 8 15 S2 12 14 6 1 7 2 11 9 3 8 5 15 0 13 10 S3 12 13 5 2 7 1 11 10 3 8 6 15 0 14 9 S4 12 8 0 7 1 2 11 15 3 14 5 9 6 13 10 S5 12 14 10 1 2 11 7 5 3 13 0 6 9 4 15 S6 12 4 0 11 2 1 7 15 3 13 10 6 9 14 5 S7 12 4 0 11 1 2 7 15 3 14 9 5 10 13 6 S8 12 13 15 2 11 7 1 0 3 4 10 9 6 8 5 4 4 4 4 8 8 8 14 3.3 Suggested nonlinear components of block ciphers in Water- marking Application

2**In this section, we have implemented the proposed**

nonlinear components of block ciphers (see table 3.2)

2**to watermarking. Our main purpose here is to hide an invisible watermarked with the help of proposed**

small nonlinear components of block ciphers and least signi…cant

2digits. The algorithm of the proposed watermarking scheme is same as

discussed in previous chapter but using different nonlinear component of block cipher.

131(a) (b) (c) (d) (e) (f) (g) (h) Fig. 3:1 : (a) Original baboon image

of size 512 512 3; along with histograms of color components (b; c a (e) Watermarked image of size 512 512 3; along with histograms of color components (f; g; h). 3.4 Statistical Analysis of Watermarking Scheme To classify the large multimedia data, there exists no techniques other than the statistical analyses

181in order to justify the effectiveness of proposed schemes in

information hiding. The most commonly used statistics which are discussed in literature are, GLCM texture features (gray level co-occurrence matrix) based measures, pixel difference-based measures, correlation-

43based measures and human visual system-based measures.

Texture is one of the critical attributes utilized as a part of distinguishing articles or areas of enthusiasm for a picture. Surface of an image contains critical data about the basic course of action of textures. The textural highlights in view of dim

12tone spatial conditions have a general relevance in picture arrangement. The three

key example components utilized as a part of human elucidation of pictures are ghostly, textural and relevant highlights. Otherworldly highlights depict the normal aggregate varieties in different groups of the unmistakable as well as infrared part of

12an electromagnetic range. Textural highlights contain data about the spatial circulation of tonal varieties inside a band. The fourteen textural highlights proposed by Haralick et., [67] contain data about

picture surface attributes, for example, homogeneity, dark tone straight conditions, difference, number and nature of limits introduce and the many-sided quality of the picture. Logical highlights contain data got from pieces of pictorial information encompassing the zone being broke down. Haralick et.,[68] all initially presented the utilization of co-event probabilities utilizing GLCM for separating different surface highlights.

12GLCM is additionally called as dark level reliance lattice. It is characterized as a two dimensional histogram of dark levels for a couple of pixels, which are isolated by a settled spatial relationship. Different GLCM

parameters are identified with particular first

41-order statistical concepts. For example, contrast would mean pixel pair repetition rate, variance would mean spatial frequency detection etc. Relationship of a textural significance to every one of these parameters is extremely basic. Generally, GLCM is dimensioned to the quantity of dark levels G and stores the co-occurrence probabilities gij. To decide the

surface highlights, choose measurements are connected

12to each GLCM by repeating through the whole grid. The textural highlights depend on insights which outline the relative recurrence appropriation which depicts how regularly one dark tone will show up in a predefined spatial relationship to another dim tone on the

picture. The accompanying documentations are utilized to clarify the different textural highlights: 3.4.1 Entropy This measurement measures the turmoil or many-sided quality of a picture. The entropy is substantial when the picture isn't literarily uniform and numerous GLCM components have little esteems.

Complex surfaces have a tendency to have high entropy. Entropy is firmly, yet contrarily connected to vitality. A totally arbitrary circulation would have high entropy since it speaks to tumult. Strong tone picture

27**would have an entropy** estimation **of 0. This** component **can be** valuable **to** let **us** know whether **entropy is** greater **for** substantial surfaces **or for the smooth** surfaces **giving us** data **about which** kind **of** surface **can be considered** factually **more**

tumultuous. 3.4.2

12**Angular Second Moment It** gauges **the textural** consistency **that is pixel** combine reiterations. **It** identifies clutters **in**

surfaces. Vitality achieves a most extreme esteem equivalent to one. High vitality esteems happen when the dim level appropriation has a steady or occasional frame. Vitality

12**has a** standardized **range. The GLCM of less homogeneous** picture **will have** huge **number of**

little sections. Vitality is a measure of neighborhood homogeneity and in this manner it speaks to the inverse of the entropy. Fundamentally this element will reveal to

27**us how uniform the** surface **is. The higher the** vitality esteem, **the** greater **the homogeneity of the**

surface. The scope of vitality is [0,1], where vitality is 1 for a steady picture. 3.4.3 Inertia This measurement

12**measures the spatial** recurrence **of** a picture **and is** contrast snapshot **of GLCM.** This measure **is**

additionally called differentiate. It is the distinction between the most noteworthy and the least estimations of an adjacent arrangement of pixels. It quantifies the measure of neighborhood varieties display

12**in the** picture. **A low** inactivity picture **presents GLCM** focus **term around the**

important corner to corner and highlights low spatial frequencies. On the off chance

11**that the neighboring pixels are fundamentally the same as in their** dim **level** esteems **then the** differentiation **in the picture is low. If there should** be **an occurrence of** surface, **the** dim **level** varieties **demonstrate the** variety **of surface itself. High** differentiation esteems **are normal for** substantial surfaces **and low for smooth, delicate surfaces.**

3.4.4 Dissimilarity Dissimilarity is a measure that characterizes the variety of dim level matches in a picture. It is the nearest to stand out from a distinction in the weight - differentiate not at all like divergence develops quadratically. Ng 1Ng 1 D = (i j)P(i;j): Xi=0 Xj=0 It is normal that these two measures act similarly for a similar surface since they compute a similar parameter with various weights. Contrast will dependably give somewhat higher esteems than dissimilarity. Dissimilarity ranges from [0,1] and acquire greatest when the dim level of the reference and neighbor pixel is at the extremes of the conceivable dim levels in the surface sample. 3.4.5 Inverse Difference Moment Inverse difference moment is the neighborhood homogeneity. It is high when nearby dim level is uniform and opposite GLCM is high. Reverse distinction minute weight esteem is the opposite of the differentiation weight. It quantifies picture homogeneity as it expect bigger esteems for littler dim tone contrasts in combine components. It is more delicate to the nearness of close inclining components in the GLCM. It has most extreme esteem when all components in the picture are same. The scope of homogeneity is [0,1]. On the off chance that the picture has little variety

27**then homogeneity is high and if there is no** variety **then homogeneity is** equivalent **to 1.** Subsequently, **high homogeneity** alludes **to** surfaces **that contain** perfect dreary **structures, while low homogeneity** alludes **to** enormous variety **in both,** surface components **and their spatial** courses of action. **An inhomogeneous** surface alludes to a picture that has almost no redundancy of surface components and spatial comparability in it is

truant. 3.4.6 Correlation Correlation is a measure of dark tone straight conditions in the picture, speci…cally, the head- ing under scrutiny is the same as vector removal. High connection esteems suggest a direct connection between the dim levels of pixel sets. Hence, GLCM relationship is uncorrelated with GLCM vitality and entropy, i.e., to pixel sets reiterations. Relationship achieves it most extreme paying little mind to pixel combine event, as high connection can be estimated either in low or in high vitality circumstances. 3.4.7 Variance This measurement

12is a measure of heterogeneity and is emphatically related to …rst request factual variable, for example, standard deviation. Variance/ Fluctuation increments when the dim level esteems contrast from their mean.

Entropy =

203Ni=g0 1 Nj=g0 1 Pi ;j log Pi ;j;;

Angular second mPomentP= Ni=g0 1 Nj=g0 1 Pi2;j Inertia = Ng 1 i=0 Nj=g0P1(i jP)2Pi;j; Dissimilarity = Ng P1 Ng P1 Ng

1381 i=0 j =0 i= 0 Nj=g0 1(i j)P (i; j);

Inverse differPence mPoment =P Ni=g0P1 Ng 1 Pi;j j =0 1+(i j)2 ; Correlation = Ni=g0 1 NjP=g0 1 ijPi;Pj xy P P x y ; V ariance = Ni=g0 1 Nj=g0 1(i)2Pi;j; P P (3.3) (3.4) (3.5) (3.6) (3.7) (3.8) (3.9) where Pi;j is the (i; j) th

47entry of the co-occurrence matrix, Ng is the number of gray levels of an image, x, y, x and y are the means and standard deviations of the marginal probabilities Px(i) and Py(j) obtained by summing up the rows or the columns of matrix Pi ;j

respectively. A complete second order texture analyses of proposed technique is presented in Tables 3:3 3:4: The rest of the textural features are secondary whose mathematical expressions are given below: 2Ng Sum Average (sa) = iPx

71+y(i); (3. 10) Xi =2 2Ng Sum Entropy (sa) = Px+y (i) log Px+y (i); (3. 11) Xi =2

2042Ng Sum variance = (i sa)2Px+y(i); Xi =2

(3.12) Difference variance = varaince of Px y; (3.13)

104Ng 1 Sum Entropy (sa) = Px y (i) log Px y (i); (3.14) Xi =0 Maximum Correlation Coefficient (MCC) = (Second largest eigen value of Q)

710:5; (3. 15) where where Q(i; j) = P (i; k)P (j; k)

Xk Px (i)Py (k) ; (3.16) Information Measures of Correlation 1 = maxfHX ; HY g HX Y HX Y 1 ; (3.17) Information Measures of Correlation 2 = (1 exp[2:0(HX Y 2 HX Y); p (3.18) Ng 1 Ng Inverse di¤ erence normalized (IDN) =

111Ng 1 Ng 1 Cluster Shade = (i + j Xi =0 Xj =0

111Ng 1 Ng 1 Cluster Prominence = (i + j Xi =0 Xj =0

Xi=0Xj=0 x x 1 1 + ji jj =Ng y)3 Pi;j : y)4 Pi;j ; Pi;j ; (3.22) (3.23) (3.24) HXY HXY 1 HXY 2 = = = Xi Xj Pi;j log2fPx(i)Py(j)g; Xi Xj

21**Px(i)Py(j)** log2fPx **(i)Py(j)** g: Pi **;j** log2 Pi **;j; where HX and HY are entropies of Px and Py;**

(3.19) (3.20) (3.21) Xi Xj Inverse di¤ erence moment normalized (IDM) = Xi=0Xj=0 1 + (i j)2=Ng2 : (3.25) Ng 1 Ng 1 Pi;j The pixel di¤erence-based measures were derived based on pixel to pixel error such as

96**mean square error(** MSE), mean **absolute error (MAE), peak signal to noise ratio(PSNR) and universal image quality index (UIQI),** structural similarity **index**

metric (SSIM) are included in human visual system-based measures. The pixel di¤erence-based and human visual system-based mea- sures de…ned as follows: 3.4.8

141**Mean Squared Error (MSE)** The **mean squared error (MSE)** is **the** least di¢ cult, **and the**

most generally utilized, full refer- ence picture quality estimation. Closeness is controlled by registering the mistake between the watermarked picture and the …rst picture. M N MSE = 1

29**(C(i;j)** W **(i;j))2;**

(3.26) M N Xi=1Xj

29**=1 where M N is the** measure **of the** picture. **The parameters** C **(i; j) and** W **(i; j)** allude **to the pixels** situated **at the ith** push **and the jth** section **of** unique picture **and**

watermarked picture because of the installing of the mystery data. The

56**mean square error (MSE)** speaks to **the** combined **squared** mistake **between the watermarked**

and plain picture. A lower …gure of MSE passes on bring down error/mutilation between the cover and watermarked picture. 3.4.9

42**Mean Absolute Error (MAE) MAE is average of absolute** di¤erence **between the reference signal and test image. It is given by the equation MAE**

is normal of total contrast

42**between the reference and test** images. **It is given by the** following mathematical expression: **1 M N MAE = N** jC **(i;j)** W **(i;j))j:**

(3.27) M Xi=1Xj=1

72**3.4.** 10 **Peak Signal to Noise Ratio (PSNR)**

36**Peak signal to noise ratio** is **to estimate the image distortions containing the watermark after the watermark is embedded into the original image, and** re‡ects **a digital watermarking algorithm's imperceptibility indicator.**

36**It can be used as a good empirical rule to measure watermark's imperceptibility. The formula of PSNR is:** 2552 **PSNR**

= 10log10 MSE : (3.28) 3.4.11 Universal Image Quality Index (UIQI) The

6**universal image quality index can also be** de…ned **as the product of three components:**

Q = C1 L2 C3; (3.29) where C1 = xy ; (3.30) xy 2xy L2 = x2 + y2 ; (3.31) C3 = 2x + 2y 2 x y ; (3.32) where first term defines the correlation, second term measures the luminance and third term represents the contrasts of the images. Therefore through UIQI, we are measuring three char- acteristic at a time. 3.4.12 Structural Similarity Index Metric (SSIM) The general form of the SSIM index between signal X and Y is defined

61as: SSIM (X; Y) = [l(X; Y)] :[c(X; Y)] :[s(X; Y)] ; (3. 33) where ; and are parameters to define the relative importance of the three components.

Specifically,weset = = =1,andtheresultingSSIMindexisgivenby

112SSIM(X;Y)= (2 X Y +c1)(2 XY +c2) (X2+ 2Y +c1)(2X+ 2Y +c2)

: (3.34) Table 3.3: The GLCM analyses of original and watermarked color image. GLCM features

1Original image Color components Red Green Blue Watermarked image Color components Red Green Blue

Entropy 4.83290 4.7339 4.8837 4.8906 4.7656 4.9143 Angular Second Moment 0.00067 0.00081 0.0006 0.0006 0.0008 0.0006 Inertia 45.7318 50.3293 50.658 50.517 51.448 52.160 Dissimilarity 3.80220 3.99200 4.0573 4.0308 4.0674 4.1270 Inverse Difference Moment 0.19955 0.19637 0.1912 0.1915 0.1911 0.1878 Correlation 0.54859 0.48133 0.5565 0.5385 0.4773 0.5531 Autocorrelation 923.109 784.852 687.06 922.82 784.41 687.16 Variance 946.616 810.573 712.56 948.72 810.69 713.41 Sum Average 46.6716 43.8016 38.612 46.667 43.804 38.647 Sum Entropy 3.07445 2.94570 3.0895 3.0837 2.9489 3.0953 Sum Variance 3321.87 2815.68 2455.3 3324.3 2814.6 2456.3 Difference Variance 45.7316 50.3293 50.658 50.517 51.448 52.160 Difference Entropy 1.86210 1.89370 1.9041 1.9000 1.9057 1.9049 Information Measures of Corr. 1 -0.11886 -0.08192 -0.1121 -0.1095 -0.0785 -0.1084 Information Measures of Corr. 2 0.58027 0.51804 0.57313 0.56976 0.51195 0.56895 Cluster Shade 4113.93 -477.06 10071.4 3816.51 -477.73 9891.97 Cluster Prominence 795070 303246 1192263 812460 303883 1194388 Inverse Difference Norm. (IDN) 0.61612 0.61398 0.61305 0.61341 0.6130 0.61222 Inverse Difference Mom. (IDM) 0.65640 0.65542 0.65531 0.65538 0.65518 0.65501 Table 3.4: The pixel difference based features of proposed watermark scheme for color watermarked image. Pixel difference and correlation Color watermarked Color components of watermarked based features image image Red Green Blue MSE 68.8406 74.0624 71.4861 76.8383 PSNR 29.7524 29.4348 29.5886 29.2750 MAE 6.25782 6.54219 6.41020 6.66985 UIQI 0.88755 0.88297 0.88709 0.89380 SSIM 0.90180 0.89774 0.90134 0.90295 The feature is defined

60as a function of one or more measurements, each of which specifies some quantifiable property of an object, and is so computed that it quantifies some significant characteristics of the object.

49All features can be coarsely classified into low-level features and high-level features. Low-level features can be extracted direct from the original images, whereas high-level feature extraction must be based on low-level features. Texture is a

surface property. It

58is characterized by the spatial distribution of gray levels in a neighborhood. Since texture shows its characteristics both by pixel coordinates and pixel values, there are many approaches used for texture classification. The

image texture depends on the scale or resolution at which it is displayed. A texture with specific characteristics in a sufficiently small scale could become a uniform texture if it is displayed at a larger scale. The GLCM seems to be a well-known

21statistical technique for feature extraction. The GLCM is a tabulation of how often different combinations of pixel gray levels could occur in an image. The goal is to assign an unknown sample image to one of a set of known texture classes. Textural features can be scalar numbers, discrete histograms or empirical distributions. They characterize the textural

properties of the images, such as spatial structure, contrast, roughness, orientation, etc. and have certain correlation with the desired output.

Here we have calculated mainly second order texture features of plain and watermarked image in order to authenticate the presence of watermark in an original color image. There is minute di¤erence in all GLCM texture features which justify the existence of watermark statistically which cannot be seen through naked eye (see Table 3.3). Moreover the values of pixel di¤erence based features namely, MSE, PSNR and MAE and, correlation based measures UIQI and SSIM clearly 3.5 Cryptographic Properties of Secure Nonlinear Component of Block Ciphers The projected nonlinear component is also veri…ed by algebraic

31**methods to determine the strength and resistance against** cryptanalysis. **The primary objective of the** nonlinear compo- nent **is to** induce nonlinearity **in** plaintext. **In order to determine the extent of nonlinearity after transformation, a** nonlinear **test is conducted. The performance of the** nonlinear component **is further evaluated by observing the behavior of** output **when input is changed according to**

di¤erent criteria namely strict a. The e¤ects

31**of bit changes in the system at** di¤erent **stages are also analyzed. Similarly, linear and** di¤erential **approximation probability tests are** per- formed **to evaluate resistance against linear and** di¤erential **cryptanalysis, respectively.**

The detail description for each cryptographic properties namely nonlinearity, Bit independent cri- terion

147**(BIC), Strict avalanche criterion (SAC), Linear approximation probability (LP) and** di¤erential **approximation**

probability already given in chapter 1. Here we have only apply these cryptographic properties on our proposed nonlinear components of block cipher. Table 3.6: Nonlinearity, SAC and LP analyses for proposed

4**nonlinear components of block ciphers.** nonlinear components **of**

block ciphers Max. Min. Nonlinearity Avg. SAC LP S1 4 2 3.5 0.6250 0.3750 0.5000 0.3750 S2 4 2 3.5 0.6250 0.3750 0.5000 0.3750 S3 4 2 3.5 0.6250 0.3750 0.5000 0.3750 S4 4 2 3.5 0.5000 0.3750 0.4921 0.3750 S5 4 2 3.5 0.6250 0.5000 0.5078 0.3750 S6 4 2 3.5 0.5000 0.3750 0.4843 0.3750 S7 4 2 3.5 0.6250 0.3750 0.5000 0.3750 S8 4 2 3.5 0.6250 0.3750 0.5000 0.3750 S9[142] 4 2 3.5 0.6250 0.3750 0.4922 0.3750 S10[143] 4 2 3.5 0.7500 0.2500 0.5000 0.2500 S11[144] 4 4 4 0.5000 0.5000 0.5000 0.2500 S12[145] 4 2 3.5 0.6250 0.3750 0.4531 0.3750 S13[146] 4 4 4 0.6250 0.2500 0.4375 0.3750 S14[147] 4 2 3.5 0.7500 0.2500 0.4688 0.3750 Table 3.7: BIC-Nonlinearity, BIC-SAC and DP analyses for proposed nonlinear components of block nonlinear components of block ciphers BIC-Nonlinearity Max. Min. Avg. Max. BIC-SAC Min. Avg. Max. .

79**S1 4 S2 4 S3 4 S4 4 S5 4 S6 4 S7 4 S8 4 S9[** 142] 4 **S10[** 143] 4 **S11[** 144] 4 **S12[** 145] 4 **S13[** 146] 4 **S14[**

147] 4 2 2 2 2 2 2 2 2 0 0 0 0 0 0 2.5 2.5 2.5 2.5 2.5 2.5 2.5 2.5 2.5 2.5 2.75 2.5 2.5 3.0 0.5417 0.5417 0.5000 0.6250 0.6250 0.5417 0.6667 0.5833 0.6250 0.5833 0.5833 0.5833 0.5417 0.5417 0.4166 0.4166 0.3750 0.3750 0.3750 0.4166 0.3750 0.3333 0.4167 0.4167 0.4167 0.4167 0.4167 0.4167 0.5052 0.4844 0.4739 0.4739 0.4844 0.4844 0.4687 0.4479 0.5052 0.4688 0.4688 0.5000 0.5000 0.4739 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 We are taking only eight nonlinear components of block ciphers from twenty four proposed nonlinear components of block ciphers and compare these with some well known existing non- linear components of block ciphers. By investigating the tabulated values in tables 3:6 and 3:7, it is quite evident from that our proposed methodology clearly ful…ll the cryptographic need of nonlinear component. The nonlinearity of proposed nonlinear components of block ciphers is comparable to existing nonlinear components. Additionally, the SAC, BIC-SAC are near to 0:5 which shows the balancedness of

202**Boolean functions involved in the** present construction. **The linear** approximation **and**

di¤erential approximation probabilities of proposed nonlinear components of block ciphers values provides strong resistance against di¤erential and linear attacks. 3.6 Conclusion In this part, we have examined digital picture watermarking which is one of the unmistakable techniques to satisfy the hole between copyright issues and advanced dispersion of information. It is principally in light of data concealing systems and empowers helpful security instruments. It goes about as a decent medium for copyright issues as it implants an image or a logo as a watermark, which can’t be adjusted physically. One imperative segment that must be remem- bered while utilizing watermarking plan is to turn away any modi…cations to the creativity of the picture in the wake of installing the information. At the point when the picture with the mystery information is transmitted over the web, unapproved gatherings might need to hack the information covered up …nished the picture or change it. On the o¤ chance that the inventiveness of the picture has been changed, at that point it will be simpler to hack the data by unapproved people. Keeping in mind the end goal to enhance the security, the advanced watermarks are dominatingly embedded as the changed computerized motion into the source information utilizing key based inserting calculation and pseudo clamor design. The

83**best known watermarking** strategy **that works in the spatial** area **is the Least** Signi…cant **Bit (LSB), which replaces the** minimum noteworthy **bits of pixels** chose **to** shroud **the**

data. Our plan fundamen- tally here triple, right o¤ the bat build another nonlinear components of block ciphers, also present new factual and arithmetical examinations which depend

17**on gray level co-occurrence matrix (GLCM), and**

thirdly utilized these development to outline new watermarking plan. Chapter 4 Small Nonlinear Components in Image Encryption and Information Hiding The upswing of internet is

8**one of the most important factors of information technology and communication** which ultimately needs **the security of information**

that passes through any in- secure line of communications. There are several information security techniques available for securing information. The cryptography is one of technique used to safeguard the

8**secrecy of communication and many** di¤erent **methods have been developed to encrypt and decrypt data in order to keep the message secret.** Inappropriately **it is** occasionally **not enough to** preserve **the** insides **of a** communication **secret, it may also be** essential **to** preserve **the** presence **of the** communication **secret. The** procedure **used to** device **this, is called steganography.** Steganogra- phy **is the** skill **of hiding messages in a medium called cover object in such a way that** presence **of message is** untraceable. **Imperceptibility is clearly is the most important requirement in steganographic schemes. The cover object could be a digital image, an audio** …le, **or a video** …le. **The secret message called payload could be a plain text, an image, a video** …le **or an audio. Steganographic methods are** classi…ed **into spatial domain embedding and frequency domain embedding. In frequency domain, images are transformed into frequency components by using DCT, FFT or DWT and then messages are embedded either in bit level or in block level. In spatial domain LSB replacing is the most widely used data hiding method.** Because **of**

8**low computational complexity and high embedding capacity this** chapter **mainly deals with LSB steganography method.**

The proposed work in chapter displays a novel procedure for image steganography in view of the S-Box mapping. The pre-processing of emit image is conveyed by rearranging of hidden image segments by utilizing three 4 4 nonlinear components of block ciphers. The preprocessing give abnormal state of security as extraction is unrealistic without the learning of mapping guidelines of nonlinear component. The proposed plan is additionally equipped for holding self-extraction system to recoup the hidden image. 4.1 Logarithmic Permutation of GF (24)

23**In this section, we report a new class of**

4**nonlinear components of block ciphers** developed **in**

GF (24). These small nonlinear components of block ciphers

> 23**can be used to construct a compact cipher for the devices with limited computing and memory resources, such as those in wireless sensor or mobile communications. We found these permutations by means of the multiplication table of GF** (24) (see table **4.**

2). We notice that the inverses de…ned in Table 4.2 is equivalent to7 !

> 23**14 in GF** (24), **which belongs to the class of permutations generated by the power** functions7 ! **k (k = 1; 2; 4; 7; 8; 11; 13; 14). In**

> 23**the present work, we investigate an alternative class of permutations** de…ned **by**

the7 ! logm (m = 2; 3; 4; 5; 9; 11; 13; 14) in GF (24). Table 4.2: Logarithmic permutations. x Permutations

> 184**P2 P3 P4 P5 P9 P11 P13 P14**

0 0 0 0 0 0 0 0 0 1 15 15 15 15 15 15 15 15 2 1 4 8 2 14 13 7 11 3 4 1 2 8 11 7 13 14 4 2 8 1 4 13 11 14 7 5 8 2 4 1 7 14 11 13 6 5 5 10 10 10 5 5 10 7 10 10 5 5 5 10 10 5 8 3 12 9 6 12 9 6 3 9 14 11 7 13 1 2 8 4 10 9 6 12 3 6 12 3 9 11 7 13 11 14 8 1 4 2 12 6 9 3 12 9 3 12 6 13 13 7 14 11 2 4 1 8 14 11 14 13 7 4 8 2 1 15 12 3 6 9 3 6 9 12 4.2 Mathematical Structure for Proposed nonlinear components of

> 94**block ciphers The** nolinear component **of block cipher is** by using **the**

> 198**the multiplicative inverse for a given number in**

GF (24) = Z2[x]=fx4 + x + 1g = fb0 + b1x + b2x2 + b3x3=bi 2 Z2g:The

> 2**multiplicative inverse is then transformed using the following** a¢ ne **transformation:** S box = **G L**

J; (4.1) where L(x) is the 4 4 linear map over GF (2) and G(x) = x d and J is inverse function as de…ned in chapter 3. The linear map over GF (2) is given as follows: 1110 201113 : (4.2) 1011 6 1101 4 5 7 The proposed a¢ ne logarithmic permutation based nonlinear components of block ciphers are given as follows: Table 4.3: Proposed a¢ ne logarithmic permutation based nonlinear components of block ciphers.

> 4**nonlinear components of block ciphers** Elements **of** nonlinear components **of**

block c S1 12 3 11 1 2 7 6 9 5 4 0 8 15 13 14 S2 12 3 1 11 7 2 6 9 10 14 15 13 0 8 4 S3 12 3 7 2 11 1 9 6 0 8 10 14 5 4 13 S4 12 3 2 7 1 11 9 6 15 13 5 4 10 14 8 S5 12 3 4 14 13 8 3 6 10 11 15 7 0 2 1 S6 12 3 13 8 14 4 6 9 0 2 10 11 5 1 7 S7 12 3 8 13 4 14 6 9 15 7 5 1 10 11 2 S8 12 3 14 4 8 13 9 6 3 1 0 2 15 7 11 4.3 Proposed Steganographic Technique Proposed steganography scheme is based on scrambling and transposition transformation which clearly satisfy the idea of Shannon principal of di¤usion and confusion using nonlinear compo- nent mapping. A complete ‡ow chart of suggested algorithm is give as follows: Start Cryptographic Part Steganographic Part Conceal image Cover image Scrambling Embedding Transformation Algorithm Encrypted image Stego image Encrypted image Extraction Algorithm Decrypted image Conceal image Fig. 4.1: Flow chart for suggested steganographic process. 4.3.1 Scrambling Transformation Establishment of chunks from Conceal image The …rst part of this hiding technique includes the conversion of secret image into blocks of …xed size and then divides the size of secret image by the size of blocks in order to assign a unique address to each block in secret image. In order to understand this scrambling function, we are giving a toy example which shows how our scrambling function work. Let us consider a secret image of size 256 256 and is distributed into blocks of 4 4 pixel. Chunk dimension = 4 4 pixel = 16 Pixel Total number of chunks = 256 256=4 4 = 4096 Chunks Bits required to signify discourse of 4096 chunks = 12 Allocating the discourse of primary chunk = 000000000000 address of latter chunk = 111111111111 4.3.2 Algorithm for Transposition of Blocks using Nonlinear Component Transformation The clusters of 4 bits of the locations block are inputted to the …rst, second and third nonlinear components of block ciphers correspondingly. These nonlinear components of block ciphers ful…lled alluring mathematical cryptographic properties. Each block in the input image now exchanges to the new address …gured by three nonlinear components of block ciphers. The operational detail and meaning of S-box as takes after: Table 4.4: S-box Transformation. 00 00 12 01 2 10 5 11 15 S1 S2 01 10 11 00 01 3 11 1 00 12 3 7 6 9 01 7 2 4 0 8 10 10 14 13 14 10 11 0 8 S3 00 01 10 11 00 12 3 7 2 01 11 1 9 6 10 0 8 10 14 11 5 4 13 15 10 1 6 15 4

11 11 9 13 5 1 0 1 1 0 1 0 1 0 0 1 1 Address of Block = | S1 } | S2 } | S3 {z {z {z } The info 1011 is linked to S1, 0101 to S2 and 0011 associated to S3. The first two bits gives direction of row and last two bits give direction about column. To start with and fourth bits of info speak to line and second and third piece speak to section in nonlinear component of block cipher. So the information 1011 regarded as a 10 (third line) and 11 (fourth column) giving yield 8 in first nonlinear component. This yield is presently changed over into four bit binary grouping giving 1000. In like manner 0101 and 0011 contributing gives yield 2 (0010) and 2 (0010). Hence concluding firsthand block address is: 1000 0010 0010. So the firsthand position of 1011 0101 0011 (2899th Block) is 1000 0010 0010 (2082th Block). In the similar techniques the new addresses of all the 4096 blocks are calculated and reordered consequently. (a) (b) Fig. 4.2: Original secret image (a); Encrypted secret image (b). 4.4 Inserting Algorithm The implanting component contains: 4.4.1 Process of Hiding Address into Cover Image We are now taking original image mean cover image of size M N is dividing into four M=2 N=2 segments the first segment contain information about the address of block and rest three segments contain information about encrypted image. Image of size Start M×N Division of cover

101**image of size M×N into** n segments **of size**

M/2×N/2 n 3 2 1 End Fig. 4.3: Division of stego image. For instance the first segment of the original image is divided into 212 blocks of size 4 4. The total 12 bit modified address of each segment is stored in first 12 pixels and four continuing stay unaffected. Now the LSB of all 12 pixels is altered and interchanged by the bits of the block address. 4.4.2 Hiding of Secret Encrypted Image into Cover Image The pixel value of encrypted image is hidden in the corresponding

187**pixel in the cover image. The** first 3 **bits of**

first pixel of encrypted image is distributed in 2nd region, next 3 bits in 3rd region and 2 bits in 4th region. The bits from encrypted image replace the bits of cover image (see Fig. 4.4). 8 bits pixel value of encrypted image z }| { 3 bits substituted by 3 bits substituted by 2 bits substituted by | {z } | {z } | {z } second segment third segment fourth segment Fig. 4.4: Distribution of bits of encrypted image. (a) (b) (c) Fig. 4.5: Process of hiding encrypted image of size 256 256 3 into cover image of size 512 512 3; (a) Secret image, (b) Encrypted secret image and (c) Stego image. 4.5 Image Retrieval Algorithm The process of image retrieval consists of two algorithms one for recovery of encrypted or scrambled image and second one is recapturing of secret image from encoded image or encrypted image. These procedures are defined separately in subsequent sections. 4.5.1 Regaining of Scrambled Image The hided image is recuperated via taking one pixel concurrently from second, third and fourth region. Now with the aid of taking 3 LSB from second vicinity pixel, three LSB from third region pixel and a pair of bits from forth neighborhood pixel types eight bits of first pixel of encrypted picture. Likewise through taking every pixel one at a time from above region forms entire encrypted image. 4.5.2 Regaining of Secrete Image from Scrambled Image In this phase of the information hiding scheme, we will recover the secret image from our encrypted image. Firstly, we have divided our image into segment of 4 4 pixels having sixteen pixels in each block. Secondly, the address of each block is calculated by compelling first segment of stego image first twelve pixels among 4 4 block are taken and one LSB from these 12 pixels gives 12 bits. These block of twelve bits are inserted to inverse S-box transformation which give the actual address of that block. Each segment from the first part of stego image gives original address of block of that segment into the secret image (see

171**Fig 4.6). (a) (b) (c) Fig. 4.6:**

Process of retrieving secret image from stego image 512 512; (a) Stego image, (b) Encrypted secret image and (c) Secret image. 4.6 Analysis of Evaluation Metrics for Steganographic Algo- rithm In most

44**sciences, statistical analysis is at the heart of** utmost **experiments. It is very hard to obtain general theories in these areas that are universally valid. In addition, it is through experiments and surveys that a scientist is able to** confirm **his theory.**

In information secu- rity different types of statistical metrics were used in order to verify the validity of suggested algorithms. But here we limit ourselves to watermarking performance assessment distortion metrics. The distortion measures the difference between the original cover content and its steganographic version. The stego embedding process introduces some amount of distortion to the original cover image. This distortion can be measured geometrically or perceptually. The measurements which can be used to quantify these distortions are further classified into following most useful categories: i. Pixel Difference

43**-based measures, ii. Correlation-based measures, iii.** Human Visual System **based measures.**

The pixel difference-based measures were derived based on pixel to pixel error such as mean square

6**error(MSE), root mean** square **error (RMSE), mean absolute error (MAE)** and **peak signal to noise ratio(PSNR), signal to noise ratio.**

The correlation based measures includes normalized cross correlation (NCC), structure content (SC) and

151**universal image quality index (UIQI), structural similarity index** metric **(SSIM) are**

included in human visual system-based measures. The mathematical expression for each of the above listed statisitcal analyses were already been discussed in previous chapters. Table 4.5: The results of MSE, PSNR, RMSE, MAE, UIQI, SSIM, SC and NCC of proposed steganographic algorithm for color image. Proposed Analyses Color image (cover & stego) Color image components (cover & steg Red Green Blue MSE 8.8156 10.1537 9.1302 8.8021 PSNR 39.8781 38.5512 37.0159 38.5531 RMSE 2.96910 3.38430 3.18280 3.44860 MAE 2.71580 2.50400 2.33680 2.57840 SC 1.00213 1.00130 1.00070 1.00020 NCC 1.00512 1.00319 1.00100 1.00218 UIQI 0.90360 0.83820 0.85060 0.86110 SSIM 0.93143 0.94470 0.94760 0.94470 4.7 Results and Discussions The projected scheme is stronger information hiding technique as a result of while not prior data of S-box mapping operate and bits distribution mechanism, the extraction of secrete image from the stego image is impossible. what is more quality of cover image is additionally not degraded due to variation in maximum 3 LSB of 50% of pixel that mirrors solely zero eight distinction component value and 2 LSB of 25% of component that re‡ects solely 0 3 distinction component price and rest having only 1 bit distinction that re‡ect solely 0-1di¤erence. In addition the projected theme is capable of not simply scrambling knowledge however conjointly changes the intensity of the pixels that contributes to the protection of the secret writing. The degree of distortion of image can be measured by using

114**mean square error (MSE), root mean square error (RMSE), peak signal to noise ratio (PSNR),**

mean absolute error (MAE). These measures are fundamentally belong from the category of pixel di¤erence based measures. All the pixels of an image are equally important. With the use of PSNR, MSE, RMSE and MAE, gray-value di¤erence between corresponding

136**pixels of the original image and the pixels of** stego **image** are considered. All **the** pixels **of**

an image are independent of their neighbor pixels. Therefore, pixels at di¤erent position have di¤erent e¤ect on human visual system (HVS). The values of pixel di¤erence approximation namely MSE, PSNR, RMSE and MAE clearly re‡ected that our proposed scheme is quite suitable for information hiding of images. Here we not only consider pixel di¤erence based quality measures of an image but also use correlation based and human visual based analyses. The correlation based measures includes structure content (SC) and normalized cross correlation (NCC), and

129**human visual based metrics** consists of **universal image quality index (UIQI) and** structure **similarity index** measure **(SSIM).**

The correlation based measure namely SC and NCC represent the correlation among the neighboring pixels. The values of SC and NCC (see Table 4.5) close to unity which clearly shows a small disturbance caused by proposed scheme with respect to pixel neighbor. Also the similarity between cover and stego image can be veri…ed through the use of HVS based measures. The HVS based measures is comprises of UIQI and SSIM respectively. The close investigation of the values of UIQI and SSIM (see Table 4.5) which is near to unity re‡ect that with naked eye it is quite tough to di¤erentiate between cover and stego images. 4.8 Conclusion The suggested information hiding technique utilize small nonlinear components of block cipher namely S-box that improve the confusion capability of pixels value and address of blocks in encrypted secret image. The present work not only uses small nonlinear components of block ciphers but also combine steganography and cryptography in order to transmit any information through insecure line of communication secretly. With the quick improvement of computerized innovation and web, steganography has propelled a considerable measure over past years. The majority of the current techniques for steganography concentrate on the installing system and lesser thought to the preprocessing stages, for instance encryption of emit picture, as they depend vigorously on the routine encryption algorithms which clearly are not custom-made to steganography applications where ‡exibility, robustness and security are required. The present steganographic algorithm is mainly depending on double layer security that is cryptography and steganography which is clearly a major re…nement is existing technique. Chapter 5 Optimal Criteria for the Selection of Cryptographically Secure Nonlinear Component The block ciphers are the most important components due to is applicability

6**in the region of cryptography. The execution of a** new **cipher relies on** upon **the quality of the algorithm which is** in charge of making

> 6**confusion in the encryption process. This usefulness is** accomplished **by the utilization of** nonlinear component **which is the main segment included in numerous block ciphers** [64]. **The** change **in the** mathematical **and statistical properties of** nonlinear component **has been a** focal point **of fascination in the** …eld **of encryption.**

In this chapter, we demonstrate the Balancedness, Nonlinearity, Correlation immunity, Absolute indicator, Sum of square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Number of …xed points, Number of opposite …xed points, Composite algebraic immunity, Robustness to di¤erential cryptanalysis, Delta uniformity, SNR(DPA) and Confusion coe¢ cient variance for existing S- boxes. There are various rising encryption techniques as of late proposed in writing. In spite of the fact that these algorithms have all the earmarks of being

> 3**promising, there** power **is not yet** settled **and they are** advancing **to** wind up models. **Some of these** ciphers **worth** specifying **are the** general population **key cryptosystems** in view of **chaotic Chebyshev polynomials**

[61],

> 54**advanced encryption standard (AES)** cryptosys- tem utilizing **the** highlights **of mosaic** picture **for**

to a great degree secure high information rate [54], and picture encryption by means of strategic guide capacity and store tree [57]. The most widely recognized strategies used to break down the measurable quality of nonlinear components of block ciphers are the connection investigation, direct estimate likelihood, di¤erential guess likelihood, and strict torrential slide paradigm and so forth. We have included relationship strategy as a benchmark for the rest of the investigation utilized as a part of this work. Except for connection investigation, the application and utilization of the aftere¤ects of factual exam- ination, introduced in this section, have not been connected to assess the quality of nonlinear components of block ciphers. The connection investigation, entropy examination, di¤erentiate examination, homogeneity investigation, vitality examination, and

> 54**mean of** outright **deviation** investigation **are performed on AES** [56], **APA** [55], **Gray** [64], **Lui** [60], **residue prime** [53], **S8 AES**

[59], SKIPJACK [63], and Xyi [62] nonlinear components. The aftere¤ects of these examinations are broke down by the proposed basis by considering the estimations of all the investigation on various nonlinear components.

> 179**The proposed criterion uses the results from** Balancedness, Nonlinearity, **Correlation**

im- munity, Absolute indicator, Sum of Square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Strict Avalanche Criteria, Number of Fixed Points, Number of opposite Fixed Points, Composite Algebraic Immunity, Robustness to Dif- ferential cryptanalysis, Delta Uniformity, SNR(DPA) and Confusion coe¢ cient variance.

> 19**These analyses are applied to advanced encryption standard (AES),** a¢ ne **-power-** a¢ ne **(APA), gray, Lui J, residue prime, S8-AES, SKIPJACK, and Xyi S-boxes**

in order to determine the appro- priateness of an nonlinear component to multimedia applications. 5.1 Cryptographic Properties Next we enumerate cryptographic properties of Boolean functions and

> 4**nonlinear components of block ciphers. With** each of the **properties**

we list the references where an interested reader can …nd de…nitions and formulas. First block of citations refers to Boolean functions and second one to nonlinear components of block ciphers which we have already discussed in chapter 1. Here in this chapter, we will apply all possible cryptographically strong algebraic properties in order to provide a new scheme

1for the selection of good nonlinear component of block cipher.

5.2 Algebraic and Statistical Analyses In this section, we analyze nonlinear components of block ciphers

19(AES, APA, Gray, Lui J, Residue Prime, S8 AES, SKIPJACK, and Xyi) used in popular block ciphers. Without the loss of generality, the analysis can be extended to nonlinear components of block ciphers of other sizes. The algebraic and statistical analyses are used to determine the application and appropriateness of an S-box

[64]. The strength of an S

3-box can be evaluated by examining various parameters generated by numerous algebraic and statistical analyses. It is imperative to be familiar with the signi…cance and relationship between the outcomes of di¤erent types of analyses. Therefore, we develop a criterion which carefully inspects and scrutinizes the available parameters and makes a decision based on optimum assessment. The procedure begins with the Balancedness, Nonlinearity, Correlation

immunity, Absolute indicator, Sum of square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Num- ber of …xed points, Number of opposite …xed points, Composite algebraic immunity, Robustness to di¤erential cryptanalysis, Delta uniformity, SNR(DPA) and Confusion coe¢ cient variance.

3These analyses, when applied in combination, provide more vivid results and consequently assist in evaluating the performance of

nonlinear components of block ciphers. To the best of our knowledge, Balancedness, Nonlinearity, Correlation immunity, Absolute indicator, Sum of square indicator, Algebraic degree, Algebraic immunity, Transparency order, Propagation characteristics, Number of …xed points, Number of opposite …xed points, Composite algebraic immunity, Robustness to di¤erential cryptanalysis, Delta uniformity, SNR(DPA) and Confusion coe¢ cient variance,

3have not been extensively analyzed and studied for the evaluation of

non- linear components of block ciphers. The results for the above mentioned analyses for nonlinear components of block ciphers

19(AES, APA, Gray, Lui J, Residue Prime, S8-AES, SKIPJACK, and Xyi) are given in table

5:1 and 5:2 respectively. Also the algorithm that classi…es the lists of given

4nonlinear components of block ciphers to

be useful for further real world applications is given in next section. Several examples of

4nonlinear components of block ciphers are given in

tables 5:1 and 5:2. These

4nonlinear components of block ciphers should be

regarded as benchmarks. Additionally, we give values for the following cryptographic properties: algebraic degree (deg), correlation immunity (CI), signal to noise ratio (SNR),

86global avalanche criterion (GAC)-absolute indicator and sum of square indicator, and di¤erential-uniformity. 5.3 Proposed Procedure The proposed benchmarks for the selection of optimal best nonlinear components of block ciphers for multimedia applications is give as follows: Algorithm 37 Let us consider n nonlinear components of block ciphers say S1; S2; :::; Sn . We can say that S-box Si is optimal with respect to algebraic analyses than Sj for j 2 f1; 2; :::; ngn i if 1. If the Nonlinearity of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 2. If Correlation immunity of Si is less than Sj for j 2 f1; 2; :::; ngn i. 3. If absolute indicator of Si is less than Sj for j 2 f1; 2; :::; ngn i. 4. If the sum of square indicator of Si is less than Sj for j 2 f1; 2; :::; ngn i. 5. If algebraic degree of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 6. If algebraic immunity of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 7. If transparency order of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 8. If propagation characteristics of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 9. If number of …xed points of Si is less than Sj for j 2 f1; 2; :::; ngn i. 10. If number of opposite …xed points of Si is less than Sj for j 2 f1; 2; :::; ngn i. 11. If composite algebraic immunity of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 12. If robustness to di¤ erential cryptanalysis of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 13. If delta uniformity of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 14. If SNR (DPA) of Si is greater than Sj for j 2 f1; 2; :::; ngn i. 15. If Confusion coe¢ cient variance of Si is less than Sj for j 2 f1; 2; :::; ngn i. Table 5.1: Comparison of algebraic analyses for AES, APA, Gray and Prime nonlinear components of block Existing nonlinear components of block ciphers Algebraic Properties AES AP A Gray P rime Balanced Nonlinearity Correlation immunity Absolute indicator Sum of Square indicator Algebraic degree Algebraic immunity Transparency order Propagation characteristics Number of Fixed Points Number of opposite Fixed Points Composite Algebraic Immunity Robustness to Di¤erential cryptanalysis Delta Uniformity SNR (DPA) Confusion coe¢ cient variance Y es 112 0 32 133120 7 4 7:860 0 0 0 4 0:984 4 9:600 0:11304 0:139337 0:111304 Y es 112 0 32 133120 7 4 7:859 0 0 2 4 0:984 4 8:910 Y es 112 0 32 133120 7 4 7:860 0 5 0 4 0:984 4 9:600 Y es 112 0 152 324736 7 4 7:756 0 2 0 4 0:719 72 9:925 0:100074 By analyzing the algebraic characteristics presented in above table, the nonlinearity, algebraic degree, algebraic immunity, propagation characteristics, composite algebraic immunity of AES, APA, Gray, Prime nonlinear components of block ciphers are 112, 7, 4, 0 and 4. The high values of absolute indicator, sum of square indicator, delta uniformity, number of …xed points and low value of robustness to di¤erential cryptanalysis in case of prime S-box does not qualify it for optimally best S-box whereas transparency order, SNR(DPA), confusion coe¢ cient variation is quite comparable properties of prime S-box with AES, APA and Gray nonlinear components of block ciphers respectively. Table 5.2: Comparison of algebraic analyses for S8-AES, Skipjack and Xyi nonlinear components of block ci Existing nonlinear components of block ciphers Algebraic Properties S8-AES Skipjack Xyi Balanced Nonlinearity Correlation immunity Absolute indicator Sum of square indicator Algebraic degree Algebraic immunity Transparency order Propagation characteristics Number of …xed points Number of opposite …xed points Composite algebraic immunity Robustness to di¤erential cryptanalysis Delta uniformity SNR (DPA) Confusion coe¢ cient variance 0:123747 0:147139 Yes 110 0 40 143104 8 4 7:857 0 0 1 4 0:969 6 9:227 Yes 100 0 96 238336 7 4 7:821 0 0 0 4 0:953 12 8:743 Yes 88 0 96 316672 7 4 7:822 0 1 2 4 0:953 12 9:448 0:116957 The nonlinearity of S8-AES S-box is high as compared to Skipjack and Xyi nonlinear com- ponents of block ciphers which show that Boolean functions involved in S8-AES S-box are cryptographically secure. All the nonlinear components of block ciphers enumerated in the tables 5:1 and 5:2 are balanced so we did not write that property in the tables. Also, all the nonlinear components of block ciphers have algebraic degree equal to 7. We omitted correlation immunity property from the table since it must be 0 as evident by Siegenthaler's inequality [9]. Further, none of the nonlinear components of block ciphers satisfy SAC property so we also omitted it from the table. Low nonlinearity value does not ensure low transparency order. In fact, it is easy to …nd nonlinear components of block ciphers with nonlinearity below 90 and with transparency order comparable to that of AES S-box. Since we could not …nd any S-box with nonlinearity level the same as in AES case and with signi…cantly lower transparency order, we opted to …nd nonlinear components of block ciphers with nonlinearity lower than in AES, but also with transparency order signi…cantly lower than in AES case. The lower values of absolute indicator, sum of square indicator and delta uniformity clearly elucidates the e¤ectiveness of S8-AES nonlinear components of block ciphers in terms of mentioned criteria and also the val- ues of transparency order, robustness to di¤erential cryptanalysis, SNR (DPA) and confusion coe¢ cient variance are quite comparable with Skipjack and Xyi nonlinear components of block ciphers. The number of …xed points and opposite …xed points in case of AES is not found whereas APA, Gray, Prime, S8-AES and Xyi nonlinear components of block ciphers have …xed and opposite …xed points which clearly re‡ecting the weakness in these nonlinear components of block ciphers. 5.4 Conclusion In this work, we are mainly consider some standard nonlinear components of block ciphers likewise AES, APA, Gray, Prime, S8-AES, Skipjack and Xyi etc., for our proposed optimal criteria. We have analyzed transparency order for the nonlinear components of block ciphers of size 8 8 which is the DPA resistance properties. The properties of balancedness, nonlinearity, correlation immunity, absolute indicator, sum of Square indicator, algebraic degree, algebraic immunity, transparency order, propagation characteristics, number of …xed points, number of opposite … xed points, composite algebraic immunity, robustness to di¤erential cryptanalysis, delta uniformity, SNR(DPA) and confusion coe¢ cient variance were not yet been presented for the classi…cation of AES, APA, Gray,

160**Prime, S8-AES, Skipjack and Xyi** nonlinear components of **block ciphers.**
Chapter 6 Nonlinearity **of**

Nonbalanced and Nearly Bent Boolean Functions An important criterion that a Boolean function would satisfy is high nonlinearity to introduce confusion into the secure system. There are several types of famous Boolean functions were introduced in literature in order to food the need of cryptographic applications. Usually in literature available for Boolean functions, authors discussed one property of these functions with respect to other characteristics of a Boolean function.

> 124**A variety of desirable criteria for Boolean functions with cryptographic application have been**

identi…ed which includes; balancedness, high nonlinearity, strict avalanche criterion (SAC),

> 88**correlation immunity** (CI) **of reasonably high order, low autocorrelation** (AC), **high algebraic degree**

(AD), algebraic immunity (AI), transparency order (TO), linear approximation (LA), di¤erential approximation (DA), sum of deviation (SD) and sum of square deviation (SSD) etc. The exchange o¤ between

> 152**these criteria have** gotten **a** great deal **of** consideration **in Boolean function** writing **for** quite **a**

while. The more criteria that must be considered, the more troublesome

> 88**it is to** produce **Boolean functions** ful…lling **those properties** absolutely **by** useful logarithmic **means.**

Without a doubt, late work has tried to mix development with parts of PC look. A considerable lot of the best functions on little quantities of factors have been gotten along these lines. The connection

> 4**between the Walsh-Hadamard** change **and the autocorrelation** capacity **of Boolean** capacities **is** utilized **to** think about **propagation** attributes **of these** capacities [79]. **The** SAC paradigm **and the** ideal **nonlinearity** standard **are**

summed up in a propagation model of degree k. New properties and developments for Boolean bent functions are given and further- more the augmentation of the de…nition to odd estimations of n is examined. New properties of functions ful…lling higher order SAC are inferred. At long last a general system is built up to arrange functions as per their propagation attributes if various bits is kept steady.

> 4**Nonlinearity criteria for Boolean** functions **are** arranged **in** perspective **of their** reasonable- ness **for**

cryptographic outline. The characterization is set up as far as the biggest change amass

> 4**leaving a** measure **invariant. In this** regard **two criteria**

end up being of unique intrigue, the separation

> 4**to linear structures and the** separation **to** a¢ ne capacities, **which are** appeared **to be invariant under**

every single a¢ ne change. As

> 4**to these criteria an** ideal **class of functions is** considered. **These functions** all the while **have** most extreme **distance to** a¢ ne **functions and**

greatest distance to linear structures, and additionally least connection to a¢ ne

> 4**functions. The functions with these properties are** demonstrated **to** match **with** speci…c functions **known in combinatorial** hypothesis, **where they are called bent functions.** They are appeared **to**

have reasonable applications for block and stream ciphers [80]..

> 10**The nonlinearity of a function f on the n dimensional vector space Vn, is** limited **from above by** 2n **1 2**

2 1. In cryptographic practice, nonlinear functions are normally usefully gotten n such that they bolster certain numerical or cryptographic prerequisites. Thus an imperative inquiry is the way to compute the nonlinearity of a function when additional data is accessible. This inquiry is address with regards to auto-relationships, and infer

10**four (two upper and two lower)** limits **on the nonlinearity of a function.**

Qualities and shortcomings of each bound are additionally inspected [81]. The importance

10**of nonlinear functions in cryptology is best** delineated **by the** accomplish- ment **of** straight **cryptanalytic**

assaults as of late found by Matsui in [105]. Understanding its signi…cance, cryptographers regularly wish to discover the

10**nonlinearity of a cryptographic function, or when the**

correct esteem isn't e¤ectively possible,

10**a lower and** additionally **an** up- per **bound on the nonlinearity. A** veri…able truth **about the upper bound on nonlinearity is Nf 2n 1 2**

2 1, where Nf signi…es the nonlinearity of f . Conversely,

10**less is** thought **about** n **the lower bound on nonlinearity, other than**

some advance made in [11,13] and additionally such paltry certainties

10**as Nf > 0 if and only if f is nonlinear. In cryptographic practice,** for example, **the** outline **of a substitution box** utilized **by a private key encryption** calculation **or a** restricted **hashing** calculation, **or a nonlinear**

criticism work utilized as a part of a pseudorandom arrangement generator, one as a rule produces a nonlinear capacity such that the capacity would ful…ll certain numerical or cryptographic necessities.

10**Two upper and two lower** limits **on the nonlinearity of a Boolean** capacity **have been** built up. **These** limits **could be** especially valuable **when certain** basic data **on a Boolean** capacity **is**

accessible. Every one of the limits have been fundamentally in view of the autocorrelation of a capacity under thought.

10**This opens up a** conceivable **new** road **for future research,** which **is to** expand **the** outcomes **so they**

consider di¤erent factors, for example, direct structures, logarithmic degree and worldwide torrential slide qualities (GAC) presented in [81]. Boolean functions utilized as a part of cryptographic applications need to ful…ll di¤erent cryptographic criteria. Despite the fact that the decision of the criteria relies upon the cryp- tosystem

18**in which they are** utilized. **There are** a few **properties (balancedness, nonlinearity, high algebraic degree, correlation immunity, propagation criteria) which a cryptographically** solid **Boolean function** should **have.** In [82], **the** previously **mentioned properties in the** arrangement **of** every **Boolean** function **(all** adjusted **Boolean functions) and** demonstrate **that** relatively **every Boolean function** (relatively **every** adjusted **Boolean function)** ful…lls **all** previously **mentioned criteria on levels**

near ideal and along these lines can be thought to be cryptographically solid. Boolean functions used as a piece of cryptographic applications need to satisfy diverse cryptographic criteria. In spite of the way that

18the choice of the criteria depends upon the cryptosystem in which they are used. There are a couple of properties (balancedness, non- linearity, high logarithmic degree, relationship insusceptibility, propagation criteria) which a cryptographically strong Boolean function ought to have. In [82], the

already speci…ed prop- erties

18in the plan of each Boolean function (all balanced Boolean functions) and show that moderately every Boolean function (generally every balanced Boolean function) satis…es all be- forehand said criteria on levels close perfect and thus can be believed to be cryptographically strong.

Nonlinear qualities of (Boolean) functions are one of the imperative issues both in the outline and cryptanalysis of (private key) encryption schemes. In [108], examines nonlinear properties of functions from three extraordinary however …rmly related viewpoints: maximal odd weight- ing subspaces, limitations to cosets, and hypergraphs, all related with a function. Primary commitments of this work incorporates: (1) by utilizing a duality property of a function, cre- ators have gotten a few outcomes that are identi…ed with bring down limits on nonlinearity and on the quantity of terms, of the function, (2) the limitation of a function on a coset signi…cantly a¤ects cryptographic properties of the function, (3) creators recognize connections between the nonlinearity of a function and the conveyance of terms in the mathematical ordinary type of the function, (4) Also they have demonstrated that cycles of odd length in the terms, and also quadratic terms, in the arithmetical typical type of a function assume an imperative part in deciding the nonlinearity of the function. The

25relationship between the nonlinearity and the order of resiliency of a Boolean function

were investigated in [84]. They have proven

25a sharper version of McEliece theorem for Reed- Muller codes as applied to resilient functions, which also generalizes the well-known Xiao- Massey characterization. As a consequence, a nontrivial upper bound on the nonlinearity of resilient functions is obtained.

In addition to that these

25functions achieving the best possible trade- o¤ which can be constructed by the Maiorana-McFarland like technique.

The connection

25between the nonlinearity and the request of ‡exibility of a Boolean function

were examined in [84]. They have demonstrated a more keen adaptation of McEliece hypoth- esis

25for Reed-Muller codes as connected to versatile functions, which likewise sums up the notable Xiao-Massey portrayal. As an outcome, a

nontrivial

159upper bound on the nonlinearity of strong functions is gotten. Notwithstanding that these functions accomplishing the

most ideal exchange o¤ which can be developed by the Maiorana-McFarland like strategy. The connection

81between the nonlinearity of a Boolean function and its propagation

at- tributes were researched in [86]. They got a totally new class of Boolean

> 192**function with high nonlinearity and** great propagation measure. **On the** other hand, any **Boolean**

function ful- …lling the propagation measure as for a direct

> 81**subspace of codimension 1 or 2 has a high nonlinearity. We**

additionally call attention to

> 28**that most** exceptionally **nonlinear functions with a three-** esteemed **Walsh** range **can be** changed **into 1 resilient functions. The** plan **of** ordinary **cryptographic** frameworks depends **on two** basic standards presented **by Shannon** [2]: disarray **and**

dissemination. Disarray goes for disguising any algebraic struc- ture in the framework. Dispersion comprises in spreading out the impact of a minor change of the info information over all yields. Most ordinary natives are worried about these basic standards: mystery key …gures (square …gures and stream …gures) and additionally hash func- tions. Disarray and dispersion can be measured by a few

> 28**properties of the Boolean functions** portraying **the** framework. Disarray relates **to the nonlinearity of the** included **functions, i.e., to their Hamming** separations **to the** arrangement **of**

a¢ ne functions. Dispersion is identi…ed with the propagation attributes of the considered Boolean function. The important cryptographic amounts are the predispositions of the yield likelihood disseminations of the subsidiaries mod- erately to the uniform dispersion; they are estimated by the auto-relationship coe¢ cients of the function. Dispersion is along these lines assessed by integral pointers: propagation paradigm, sepa- ration to the arrangement of every single Boolean function with a straight structure and sum- of-squares marker. Every one of these amounts will be here considered in a brought together approach. A noteworthy connection amongst dispersion and perplexity criteria was brought up

> 28**by Meier and** Stafelbach [80]. **They** demonstrated **that maximal nonlinearity and** impeccable **propagation** qualities **are** equal necessities **for Boolean functions with** a signi…cantly **number of** factors. Tragically **those functions which** accomplish culminate dispersion **and**

immaculate per- plexity (called bowed functions) are not adjusted; that implies that they don't have a uniform yield conveyance. The development of adjusted

> 50**Boolean functions having a high nonlinearity and**

great propagation attributes at that point

> 28**remains an open** issue albeit **such functions are** basic segments **of cryptographic**

natives and, further research the connection amongst disper- sion and perplexity

> 50**criteria for Boolean functions** and demonstrated **that** profoundly **nonlinear functions**

more often than not match

> 50**with the functions having** amazing **propagation** qualities. **In this**

unique situation, they bring up the signi…cant pretended by the exceptionally nonlin- ear functions whose Walsh range takes three esteems. They display general developments of such functions and demonstrate that it can without much of a stretch be changed into ad- justed …rst-arrange connection safe functions. They are hence appropriate joining

28**functions for pseudo-** irregular **generators since they** guarantee **a high**

protection from quick connection assaults. Dispersion is in this way evaluated by reciprocal markers: propagation rule, separation to the arrangement of every single Boolean function with a direct structure and entirety of-squares pointer. Every one of these amounts will be here considered in a bound together approach. As of late, weight detachability comes about

22**on resilient and correlation immune Boolean functions have** gotten **a** great deal **of** consideration. **These** outcomes **have** coordinate results **towards the upper bound on nonlinearity of resilient and correlation immune Boolean functions of certain** request. Presently **the** unmistakable prerequisite **in the** outline **of resilient Boolean functions (which** improves **Siegenthaler's** imbalance) **is to** give comes about **which** accomplish **the upper bound on nonlinearity. Here we** build **a 7 variable,** 2 resilient **Boolean function with nonlinearity 56. This** understands **the** greatest **nonlinearity issue for 7 variable functions with any** request **of** ‡exibility. Utilizing **this 7 variable function, we** likewise build **a 10-variable, 4-resilient Boolean function with nonlinearity 480.**

Additionally creators …nished up with de- velopments of some uneven

22**correlation immune functions of 5 and 6** factors **which** accomplish **the upper bound on nonlinearity**

[87]. It is realized that Boolean functions utilized as a part of stream and piece …gures ought to have great cryptographic properties to oppose mathematical assaults. Up to this point, there have been a few developments of Boolean functions accomplishing ideal arithmetical in- vulnerability. Nonetheless, the greater part of their nonlinearities are low. Carlet and Feng contemplated a class of Boolean functions with ideal logarithmic resistance and concluded the lower bound of its nonlinearity, which is great, however not high. In addition, the principle prag- matic issue with this development is that it can't be executed e¤ectively. As of late Qichun et. al.,[100], set forward another technique to develop cryptographically noteworthy Boolean func- tions by utilizing crude polynomials, and build three interminable classes of Boolean functions with great cryptographic properties: balancedness, ideal logarithmic degree, ideal arithmetical resistance, and a high nonlinearity. As of late, a few development strategies for very nonlinear Boolean functions with generally great mathematical properties were proposed. These methodologies oversee in enhancing the vast majority of the signi…cant cryptographic criteria, however not every one of them in the meantime. Typically, either the nonlinearity limits are somewhat free (however the real nonlin- earity is moderately high) or the functions don't give a decent protection from quick logarithmic cryptanalysis. Enes and Yongzhuang built up a hypothetical system for utilizing objects in rea- sonable projective geometry spaces for development of exceedingly nonlinear Boolean functions. This enables us to set up tight limits on the nonlinearity utilizing straightforward checking con- tentions, accordingly maintaining a strategic distance from rather convoluted assessments of certain follow aggregates. This technique produces a class of completely advanced functions, that is the functions separated from high nonlinearity additionally have the most extreme math- ematical degree and ideal arithmetical insusceptibility. Contrasted with the classes of functions proposed via Carlet and Feng, Wang et. al., and Zeng et al., these proposed Boolean func- tions in [101], accomplish a somewhat better nonlinearity which is exchanged o¤ against a little more terrible protection against quick arithmetical assaults. Then again, contrasted with the functions by Tang et al. also, Tu and Deng, the nonlinearity in [101], is to some degree lower, however the mathematical properties are somewhat better. The fundamental aspects of our work here is to concern about the properties and construc- tions of a new class of S-box namely Boolean functions that attain high nonlinearity, satisfy SAC and remains non-balanced. We presented a novel technique for constructing highly nonlinear non-balanced functions which is based

1**on maximal cyclic subgroup of a Galois ring.**

It is very interesting to note that these non-balanced functions obtained by using proposed technique, achieve

123**nonlinearity higher than that attainable by any previously known construction method. We also**

initiate the research into the systematic

50**construction of highly nonlinear** non **-balanced** functions satisfying the **SAC** and BIC of SAC criterion. 6.1 Fundamental Properties of

1**Galois Rings We begin with** few **basic** de…nitions **of unitary commutative rings.** De…nition 38 **Let R be a commutative ring with** identity. 1. **An element u is** a **unit in R if there exists an element v in R such that u:v = 1, where 1 is the identity of R.** 2. Nonzero element **a** of **ring R is**

34**called zero divisor if there** exist **a nonzero element b in R such that a:b = 0.**

De…nition 39

1**A commutative ring R with** identity **is said to be** a **local** ring **if and only if its all non unit elements form an additive Abelian group.**

Alternatively,

34**a commutative ring R with identity is local if**

it has a unique maximal ideal. For instance Zpk , where

1**p is a prime integer and** m **is any positive integer, is a local ring.** De…nition 40 **Let (R;** M) **be a** local **commutative ring with**

identity having residue …eld K(= R=M). ' : R ! R=M is a canonical epimorphism, de…ned as '(a) = a = a + M;a 2 R: An irreducible polynomial (x) = a0 + a1x + + amxm 2

1**R[x] over R is said to be a basic irreducible if**

'((x)) = (x) = a0 + a1x + + amxm 2 K[x] is irreducible over K [78] b Theorem 41 [148, Theorem 2] Tbhere bis unique mcaximal

34**cyclic subgroup of R** of **order** rela- tively **prime to p. This cyclic subgroup has order** ps **1. The maximal cyclic subgroup** Gn **is**

isomorphic to the Galois group K : 6.2 Fabriaction of Nonlinear Component over Galois Ring GR 23; 8 In this section, we construct an 8 8 S-box by using the

1**maximal cyclic subgroup** G255 **of group of units of** the **Galois ring GR** 23; 8 . The **constructed**

S-box is used in image encryption. For this construction we use the computational techniques of [78] in obtaining the maximal cyclic subgroup G255. 6.2.1 Cyclic Subgroup of Invertible elements of GR (Z23 ; 8) For the local ring Z23, the binary …eld Z2 is its residue …eld. The polynomial (x) = x8 + x4 + x3 + x2 + 1 2 Z23[x]

34**is a basic irreducible polynomial. Galois ring** GR (Z23; 8) **of order** 88 **is** obtained **by**

constructing the factor ring (Z8([xx)]) ; whose elements are of the form fa0 + a1x + a2x2 + ::: + a6x6 + a7x7 : a,is 2 Z8g. The corresponding Galois …eld GF (2; 8) of order 256 becomes Z2[x] and its elements are obtained by using the identity u8 + u4 + u3 + u2 + 1 modulo ((x)) 2 and modulo (u):

1**Maximal cyclic subgroup of group of units of GR(**

Z23;8) is obtained by considering u as the root of (x) in Z2: By using the algorithm given in [78], which calculating the successive powers of u modulo 2 and module (u); we have u255 = 1: Hence, the

1**maximal cyclic subgroup of group of units of GR(**

Z23;8) has 255 elements. To …nd these elements, let be the root of (x): Then by calculating the consecutive powers of modulo 8 and modulo ( ); we have 1020 = 1: Thus, the elements of G255 are generated by = 4: These elements are listed in Table 6.1, in which the polynomials are given in increasing powers of ; i.e., the element 77370203 represents the polynomial 7 + 7 + 3 2 + 7 3 + 2 5 + 3 7: Table 6:1 : Elements of

1**maximal cyclic subgroup of group of units of GR**

(Z23 ; 8) : 6.2.2 Algorithm for Nonlinear Component Construction Nonlinear component of block cipher over Galois ring GR (Z23 ; 8) is built by de…ning the fol- lowing mapping from G255 [f0g to G255 [f0g: 1. The invertibel transformation Inv is de…ned as Inv ( ) = 1; 8 2 G255: 2. The mutiplication map T is de…ned as T ( ) = c ; where c is a …xed element taken from G255: 3. The nonlinear component for block cipher is fabricated by using combination of invertible and scalar transformations as: Iiv T ( ) = (c) 1 : By selecting di¤erent scalars from G255; we can construct 255 di¤erent nonlinear components of block ciphers. The S-box given in Table 6:2 is constructed by selecting one particular scalar. Table 6:2 : S-Box based on GR (Z23 ; 8) : The entries of S-box are the decimal representation of elements of G255; by converting these entries into binary form, we can obtain maximum 24 binary bits. 6.3 Analysis for Cryptographically Secure Nonlinear Compo- nent It is vital to assess the performance of the proposed nonlinear component of block cipher in an e¤ort to establish its usefulness in encryption. Several properties are listed in literature, which indicate the strength of any nonlinear component [121]. Among some of the prevailing methods used by cryptanalysis include di¤erential analysis used for the analysis of DES [112] and infor- mation theoretic analysis with excerpts from the original concepts presented by Shannon [1]. In this work, we analyze the proposed nonlinear component for …ve di¤erent properties, which includes

89**nonlinearity, strict avalanche criterion (SAC), bit** independence **criterion (BIC), linear approximation** probability **and** di¤erential **approximation probability.**

45**In order to** determine **the** strength **of the proposed nonlinear component,**

the results of these analyses are prudently analyzed.

191**In the following subsections, we** present the **details of these**

69**analyses and** discuss **the results** pertaining **to the strength** the S **-box**

under analysis. 6.3.1 Nonlinearity In the nonlinearity analysis, the constituent Boolean functions are assessed with reference to the behavior of the input/output bit patterns.

102**The set of all a¢ ne functions is**

used

69**to compare the distance from** the **given Boolean function.** Once **the**

initial distance is determined, the bits

80**in the truth table of the Boolean function** are modi…ed **to** approximate to **the** closest a¢ ne **function.**

Number of modi…cations required to reach the closest a¢ ne functions bears useful characteristics in determining the nonlinearity of the transformation used in encryption process. The measure of nonlinearity is bounded by [123], Ng = 2m 1 (1 2m max jSg(w)j) : (6.1) The Walsh spectrum Sg(w) is de…ned as Sg(w) = (1)g(x) :w : (6.2) w2XF2m Table 6.3: Nonlinearity of non-balanced boolean functions. Functions Ng Functions Ng Functions Ng g0 8388586 g8 8388578 g16 8388580 g1 8388584 g9 8388588 g17 8388586 g2 8388586 g10 8388580 g18 8388582 g3 8388580 g11 8388582 g19 8388586 g4 8388580 g12 8388586 g20 8388580 g5 8388588 g13 8388584 g21 8388586 g6 8388586 g14 8388582 g22 8388580 g7 8388582 g15 8388582 g23 8388588 As a rule, cryptographic Boolean capacities ought to ful…ll di¤erent criteria at the same time, for the most part high

89**nonlinearity, strict avalanche criterion** and **bit independent criterion.**

The nonlinearity of a Boolean capacity is characterized as least separation from the capacity to the relative capacities. A cryptosystem that utilizes work with a low nonlinearity is defenseless against numerous cryptanalytic assaults including the linear cryptanalysis found by Matsui (1994).

30Nonlinearity has been thought to be a critical criterion. Late advances in Linear cryptanalysis set forward by Matsui have made it express that nonlinearity

isn’t simply vital yet basic

30to DES like piece encryption calculations. Linear cryptanalysis abuses the low nonlinearity of

nonlinear components of block ciphers utilized by a piece …gure

30and it has been e¤ectively connected in assaulting FEAL and DES. It has been demonstrated that to inoculate a S- box against linear cryptanalysis it accomplishment for the Hamming separation between each nonzero linear blend of the segment capacities and each new capacity not to

veer o¤ to a long way from n in particular a S

30box is insusceptible to linear cryptanalysis if the nonlinearity of each nonzero linear mix of its segment capacities is high.

It is notable that bent functions have the most noteworthy nonlinearity and ful…ll the propagation criterion as for all non-zero vectors (Dillon, 1972). However two drawbacks of bent functions prohibit their direction application in practice. The …rst drawback is that they are not balanced, and the second drawback is that they exist only when the number of input coordinates is even. Our proposed S-box consist

84Boolean functions which are not balanced as a whole and

also exist for even number of coordinates. Also our proposed S-box does not follow the existing bound on nonlinearity which is new discovery in the …eld of cryptographic criteria. The components of proposed S-box namely even number of Boolean functions exhibits characteristics of balancedness and bentness but these Boolean functions doesn’t satisfy the nonlinearity bounds as ful…ll the by bent Boolean functions. These classes of Boolean functions are more general as compared to the existing Boolean functions. The proposed S-box which is fundamentally based on the non-balanced and non-bent

197Boolean functions. We have proposed a new bound for nonlinearity of

these non-balanced and non-bent Boolean functions. The comparison of among the di¤erent bounds are also depicted in Table 6.2. 6.3.2 Comparison with Already Exiting Results in Literature For simplicity, we suppose N1 = 2n 1 2 ln 2 n2 n2 ; N2 = 2n 1 ln 2 n2 4 1; N3 = max 6 n n

1532 2n 1 2; 2n 1 ln 2 2n 3 (n 1) + 2

2 3 2 (6.3)

24denote the lower bounds of the nonlinearity of the results in [125], [126], [127], respectively, where n = 2tm with gcd(2; m) = 1:

Also the nonlinearity bound available in [128] N4 = 2n 1 ti=1022i+1 2 2 is much better than N1;N2 and N3: More precisely, by a tedious n m 1 computaPtion, we can validate that N4 is larger than N1; N2 and N3

24if n 4: In [125], [126], and [127], some concrete values of the nonlinearity were given which are denoted by

N1; N2 and N3 for convenience

24which are much better than their bounds. The comparison table is along with our nonlinearity bounds is presented in the following table. Table 6

24:4 : Comparison among the nonlinearity bounds of Boolean functions. Construction n even

Ng Canteaut et. al., [86] Stanica [129] Stanica [129] Stanica and Sung [130] Maitra [88] Stanica and Sung [131] Xiaohu Tang et. al., [128]

156n n n n n n n 8 4 8

8 6 4 10

872n 1 2n 2 2n 1 2n 1 2n 1 2n 1 2n 1 2 2 n 2 2 n 2 2 n 2 2 n 2 2

180n 2 2 n 1 1 2d n4 e +1 2 2 n 2

Table 6:5 :

24Comparison of the nonlinearity of balanced and nonbalanced Boolean functions (n even). n

Balanced Boolean Functions N1 = N3 [125]; [127] N2 [126] N4 [128] Nonbalanced Boolean Functions Bent Boolean Functions Proposed NF 4 4 4 4 6 - 6 24 24 26 28 - 8 112 116 116 120 124 10 478 490 492 496 - 12 1970 2008 2010 2016 - 14 8036 8118 8120 8128 - 16 32530 32624 32628 32640 32748 18 130442 130792 130800 130816 - 24 - - - 8386560 8388588

24When compared with the newly proposed Boolean function, which is recorded to have the best nonlinearity among all the known bent Boolean function constructions, our function still has better nonlinearity.

This benchmark is through the mixed behavior of our proposed nonlinear components of block ciphers which is mainly at the same time depend on balanced and non- balanced Boolean functions. 6.3

70.3 Strict Avalanche Criterion Analytically In strict avalanche criterion (SAC), the behavior of the

output bits is analyzed that results from a

70change at the input bit applied to the

nonlinear S-box transformation. It is desired that almost half of the output bits change their value or simply toggle their state

40in response to a single change at the input.

The change in the output bit patterns cause a series of variations in the entire

40substitution-permutation network (S-P network)

and thus causes an avalanche e¤ect. The extent of these changes assists in determining the resistance

69to cryptanalysis and the strength of the cipher.

Table 6.6: The

39results of strict avalanche criterion for proposed S-box.

D1 2 SAC = D3 D5 6 D7 4 D2 D4 3 ; D6 D8 5 7 where 0.5391 8 0.5391 0.5391 0.5391 0.5391 D1 = 0.5391 >< 0.5391 0.5391 0.5391 0.5391 0.5391 0.5391 :> 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.5000 0.5000 9 0.5000 0.5000 0.5000 0.5000 0.5000 >= 0.5000 0.5000 0.5000 0.5000 0.5000 >; 8 0.5000 0.5000 0.5000 0.5000 D2 = 0.5000 >< 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 : > 0.5000 8 0.5000 0.5000 0.5000 0.5000 D3 = 0.5000 >< 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 : > 0.5313 0.5313 0.5313 0.5313 0.5313 0.5313 0.5313 0.5313 0.5313 0.5313 0.5313 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5234 0.5391 9 0.5391 0.5391 0.5391 0.5391 0.5391 >= 0.5391 0.5391 0.5391 0.5391 0.5391 ; > 0.5547 0.5547 9 0.5547 0.5547 0.5547 0.5547 0.5547 >= 0.5547 0.5547 0.5547 0.5547 0.5547 ; > 8 0.5000 0.5000 0.5000 0.5000 D4 = 0.5000 >< 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 : > 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.5469 0.5469 0.5469 0.5469 0.5469 0.5469 0.5469 0.5469 0.5469 0.5469 0.5469 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.5391 9 0.5391 0.5391 0.5391 0.5391 0.5391 >= 0.5391 0.5391 0.5391 0.5391 0.5391 ; > 0.5000 8 0.5000 0.5000 0.5000 0.5000 D5 = 0.5000 >< 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 : > 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4531 0.4766 0.4766 9 0.4766 0.4766 0.4766 0.4766 0.4766 >= 0.4766 0.4766 0.4766 0.4766 0.4609 ; > 8 0.5000 0.5000 0.5000 0.5000 D6 = 0.5000 >< 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 : > 0.5156 8 0.5156 0.5156 0.5156 0.5156 D7 = 0.5156 >< 0.5156 0.5156 0.5156 0.5156 0.5156 0.5156 : > 0.4453 0.4453 0.4453 0.4453 0.4453 0.4453 0.4453 0.4453 0.4453 0.4453 0.4453 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4609 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.4922 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5078 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.5000 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 0.4688 9 0.4688 0.4688 0.4688 0.4688 0.4688 >= 0.4688 0.4688 0.4688 0.4688 0.4688 ; > 0.4609 0.4609 9 0.4609 0.4609 0.4609 0.4609 0.4609 >= 0.4609 0.4609 0.4609 0.4609 0.4609 ; > 8 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 9 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 D8 = 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 : >< 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 >= 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 > : > ; Table 6.7: Comparison of SAC analysis of proposed nonlinear components of block ciphers with chaotic non nonlinear components of block ciphers SAC values Proposed S-box 0.4999 Wang[117] 0.4850 Chen[115] 0.4999 Tang[119] 0.4993 Jakimoski[120] 0.4972 Table 6.8: Comparison of SAC analysis of proposed nonlinear components of block ciphers with some well k nonlinear components of block ciphers Min Max Avg

40**Proposed S-box 0.** 445300 **0.** 539100 **0.499 AES 0.** 453125 **0.** 562500 **0.504 APA 0.** 437500 **0.** 562500 **0.** 437 **Gray 0.** 437500 **0.** 562500 **0.499**

6.3.4 Bit Independent Criterion The Bit Independence Criterion (BIC) also relies on the

40**changes at the input bits and the**

prop- erties exhibited by the independence behavior of pair-wise input/output variables of avalanche vectors [123]. This criterion

70**is analyzed by** modifying **single input bit from the plaintext.**

Table 6.9: Comparison of nonlinearity and SAC

39**of BIC of proposed S-box.**

SAC of BIC nonlinear components of block ciphers Min Max Avg. Proposed 0.487400 0.509200 0.500000

39**AES 0.** 480469 **0.** 525391 **0.** 504604 **APA 0.** 472656 **0.** 515625 **0.** 499651 **Gray 0.** 478516 **0.** 515625 **0.**

502581 6.4 Results and Discussions The comparison of the strong encryption capabilities

39**show that the performance of the proposed S-box is comparable**

or superior to some prevailing

125**nonlinear components of block ciphers** used in **the**

area of cryptography. The nonlinearity analysis depicts that the properties are comparable to the nonlinear components of block ciphers use as a benchmark in this work. The comparison of nonlinearity bounds is listed in table 6.4. The results for each nonlinearity bounds are given in table 6.5. The through investigations of table 6.5, clearly justify the claim of being highly nonlinear Boolean functions are obtained that have yet not been devised in literature which is in fact a central point of the proposed construction technique. The result of SAC is very close 0.5, which assures the acceptability of this S-box to encryption applications. The results are shown in table 6.6. We have also drawn a comparison of SAC among the chaotic and some well known nonlinear components of block ciphers (see table 6.7, 6.8). Our suggested S-box satisfy the SAC and quite comparable with the SAC of already existing nonlinear components of block ciphers. In table 6.9, a comparison of BIC is presented between the proposed S-box and AES, APA, Gray, Prime

134**nonlinear components of block ciphers.** The results are **in**

agreement with the desired range. In these tests, it is observed

80**that the performance of the proposed S-box is comparable to**

the existing well known

134**nonlinear components of block ciphers** used as benchmarks **in**

this chapter. 6.5

174**Conclusion In this chapter, we** mainly provides **a novel** construction technique **for**

nonlinear component of block cipher namely S-box which is based

126**on maximal cyclic subgroup of Galois ring.**

Ad- ditionally, we have studied the three cryptographic

126**properties of Boolean functions** including nonlinearity, SAC **and** BIC. **An**

innovative technique has been displayed to build nonlinear com- ponents of block ciphers that comprise of Boolean functions whose nonlinearity is much higher than accomplished by any beforehand known development. Also comparison with already ex- isting results in literature have been drawn in order to verify the significance of suggested construction scheme.

10**This opens up a** conceivable **new** parkway **for** advance **research that is to** develop **the** outcomes do **that they** consider **other**

cryptographic components, for example,

10**linear structures, algebraic degree, global avalanche characteristics (GAC),**

autocorrelation, algebraic immunity, correlation immunity, transparency order, linear and differential approximation prob- abilities of proposed nonlinear components of block ciphers in order to resist against the linear and differential attacks. Chapter 7 A Novel Video Encryption Technique and its Statistical Analyses Security is turning into a heightening worry in an undeniably mixed media characterized world. The current rise of installed interactive media applications, for example, versatile TV, video informing, and telemedicine have expanded the effect of mixed media and its security on our own lives. For instance, a huge increment in the utilization of disseminated video reconnaissance innovation to screen movement and open spots has raised concerns with respect to the protection and security of the focused on subjects. Mixed media content encryption has pulled in an ever-increasing number of scientists and architects attributable to the testing idea of the issue and its interdisciplinary nature in light of di¢ culties looked with the prerequisites of sight and sound interchanges, mixed media recovery, mixed media pressure, and equipment asset utilization. With the proceeding with improvement of system interchanges (wired and remote), e¤ectively catching recordings and fast advances in Internet innovation and installed …guring frameworks sight and sound information (pictures, recordings, sounds, and so on.) are of signi…cance for utilizing increasingly generally, in applications, for example, video-on-request, video conferencing, broadcasting, and so forth. Presently, it is …rmly identi…ed with numerous parts of day by day life, including training, trade, safeguard, diversion, and legislative issues. With a speci…c end goal to keep up protection or security, touchy information should be shielded from transmission or dispersion. The progressions in a universal system condition and fast advancements in distributed computing have advanced the quick conveyance of computerized mixed media information to the clients. Clients are anxious to not just appreciate the accommodation of constant video gushing like- wise shares di¤erent media data in a fairly modest manner without consciousness of conceivably abusing copyrights. In perspective of these, encryption and watermarking advancements have been perceived as a supportive method for managing the copyright insurance issue in the previ- ous decade. Encryption permits secure end-end correspondence of information while advanced watermarking permitting still faces some trying troubles for viable utilizations; there are no di¤erent methods that are prepared to substitute it. Inside the ‡ag preparing and interactive media groups, numerous plans have been proposed for ensuring touchy data while enabling certain genuine activities to be performed. These plans normally do not have a thorough model of security, and their insurance ends up faulty when scaled to huge datasets. The cryptogra- phy group has since quite a while ago created thorough protection models and provably secure techniques for information controls. Be that as it may, these systems are essentially intended for non-speci…c information. Accordingly, they ordinarily prompt an explode in computational expenses and overheads when connected to genuine interactive media applications. Multimedia data security is getting to be plainly vital with the consistent increment of advanced correspondences on web. With the fast improvement of di¤erent mixed media ad- vancements, more interactive media information are created and transmitted in the restorative, business, and military …elds, which may incorporate some touchy data which ought not be got- ten to by or must be halfway presented to the general clients. The encryption schemes created to secure information which are not reasonable for mixed media application as a result of the huge information size and continuous limitation. In this way, there is an incredible interest for secured information stockpiling and transmission systems. Data security has customarily been guaranteed with information encryption and veri…cation procedures. The introduced work goes for secure video transmission utilizing arbitrariness in encryption designs in view of standard substitution boxes (nonlinear components of block ciphers), accordingly making more disarray to get the …rst information. For the determination of best S-box for speci…c video encryp- tion, we have proposed another choice factual foundation. The security of the …rst …gure has been improved by expansion of polluting in‡uences to mislead the cryptanalyst. The proposed work discovers its application in therapeutic imaging frameworks, military picture database correspondence and classi…ed video conferencing, and comparative such application. 7.1 Introduction With the quick development of interactive media innovation numerous armed forces over the world are utilizing recordings to prepare recently enlisted troops. Such touchy information must be ensured either in transmission or capacity. One conceivable approach to secure interactive media data is to stop unapproved get to. In any case, this approach can’t ensure that the mixed media data is physically secure. Another simple approach is to scramble the entire piece stream with a cryptographic calculation, for example, DES or AES. However recordings for the most part have a lot of information and require constant operations. Additionally, on account of the remote portable frameworks, there is restricted preparing force, memory and data transfer capacity, and is seldom ready to deal with the overwhelming encryption handling load. Along these lines, thinking about the particular attributes for asset constrained frameworks, new video encryption calculations should be produced. For certi…able applications, a video encryption cal- culation needs to consider di¤erent parameters like security, computational pro…ciency, pressure e¤ectiveness et cetera. Distinctive kinds of

206**video applications require** diverse **levels of security. For** instance, **for**

Video on Demand, low security will be …ne, though for military purposes or money related data, abnormal state of security is required to totally counteract unapproved get to. Computational e¤ectiveness implies that the encryption or decoding procedure ought not cause excessively time delay, with the goal that the necessities of ongoing applications are met. Video compression is utilized to lessen the storage room and spare transmission capacity, with the goal that the encryption procedure ought to have minimal e¤ect on the compression pro…ciency. All things considered, a very much planned video encryption algorithm ought to give adequate security, high computational e¢ ciency impose little e¤ect on the compression e¤ectiveness. The wide utilization of advanced pictures and recordings in di¤erent applications conveys genuine thoughtfulness regarding security and protection issues today. Information encryption is an appropriate strategy to secure information. Till now, di¤erent encryption techniques have been proposed and broadly utilized (DES, RSA, IDEA, AES and so on.), a large portion of which are utilized for content and binary data. It is hard to utilize them speci…cally in video en- cryption as video information is regularly of extensive volumes and require constant operations. In reasonable applications, for a video encryption technique, security, time productivity, arrange consistence and compression benevolence are extremely essential. Among them, security is the essential prerequisite, which implies that the cost of breaking the encryption algorithm is no littler than the ones purchasing the video’s approval. The aim of proposed work is three fold, …rstly we design a new algorithm to create huge numbers of nonlinear components of block ciphers, and secondly we developed a novel video encryption technique along with statistical analyses and thirdly suggested a new criterion on the basis of statistical analyses for the selec- tion of best S-box. The analyses are second order texture characteristics

170**which are based on** GLCM **(Gray level co-occurrence matrices).**

7.2 Requirement of Video Encryption The encryption of multimedia data is important due to the following reasons: i. For averting undesirable review of

15**transmitted video, for** instance **from law** requirement **video** reconnaissance **being** transferred **back to a**

focal survey focus. ii. To secure the private interactive media

15**messages that is** traded **over the** remote **or wired** systems. iii. **Video encryption is** useful **in securing**

recordings utilized as a part of administrations like video on request (VOD) and video conferencing learning. iv. For ensuring medicinal recordings

15**which may contain private** data **of a patient from** un- approved **access by** malignant clients. **This study is based on video encryption based on study of** S-box transformation **algorithm which is useful in protecting various medical videos that contain private information of patients and requires sharing among various doctors that belongs to** di¤erent **department of hospital. In** …rst **part of study I have focused on various prevailing algorithms used for video encryption.**

This examination depends on video encryption in view of investigation of S-boxtransformation algorithm which is valuable in ensuring di¤erent medicinal recordings

15**that contain private** data **of patients and requires sharing among** di¤erent specialists **that**

has a place with various divi- sion of doctor's facility. In initial segment of study, we have concentrated on di¤erent prevailing algorithms utilized for video encryption. Fig. 7.1: Classi…cation of video encryption techniques. 7.3 Production of New Nonlinear Components of Block Ci- phers In this correspondence, we have displayed a procedure to orchestrate versatile nonlinear com- ponents

5**for the** development **of substitution box for** video **encryption that** use **a multiplicative group of nonzero** components **of Galois** …eld **of order 256**

alongside symmetry group S8. The proposed nonlinear part helps with changing the comprehensible

5**message or plaintext into an enciphered** organize **by the** utilization **of exponential**

map. 7.3.1 Exponential Map Di¤erent types of maps are right now used in cryptography which includes chaotic and non- chaotic maps. A cryptographically sound maps

207**play an important role in the** encryption **of**

digital medium. These maps not only create confusion but also di¤usion in cryptosystems. In part of chapter is mainly reserve for the development of mathematical expression for exponential map over a …nite …eld of order 256. Let h : M ! M de…ned as: x7 ! hx mod 257 if x < 256; 8 (7.1) < 0

29**if x = 256; where x** = hx **(mod 257) and x 2**

M = f0; 1; 2; :::; 255g.

5We select h as a primitive element : which generates the multiplicative group of nonzero elements of Galois …eld of order 256

7.3.2 Mathematical Expression of the Suggested Nonlinear Component

5In this section, we are mainly discussed the algebra of proposed S-box. The following are main steps in constructing proposed

nonlinear components of block ciphers: i. First of all select unit elements of …nite …eld Z257; with one extra condition that 256 is mapped to 0. ii. The inverse function G(x) in Z257 corresponding to multiplicative unit step is given below: x 1 if x < 256; G(x) = (7.2) < 8 0 if x = 256: The unit element x is equals to x to the power 255 which is can be represented by the : expression, x 1 = x2s 1 = x255 for x6 = 0 2 Z257: Therefore inverse function G(x) becomes G(x) = x255: iii. Let LA

29(x) be a linear transformation in F28 which can be expressed as follows: y

= LA(x); (7.3) where y0 1 2 y1 3 2

1461 y2 1 y3 = 1 y4 1 y5 0 y6 0

0 0 1 0 1 1 1 1 1 1 1 1 0 1 0 1 0 0 0 0 1 0 1 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 1 1 1 x0 1 32 3

183x1 1 x2 1 ; x3 (7.4) 0 x4 0 x5 0 x6

6 y7 7 6 0 0 0 1 1 1 1 1 x7 4 5 4 7 6 7 5 4 5 iv. We de…ne the nonlinear a¢ ne transformation function K (x) in F28 : K (x) = x d: The suggested nonlinear component of block cipher is therfore, a combination of three functions namely

5power function G (x), the linear transformation LA(x) and the a¢ ne transformation K (x): S box

= K LA G = K(LA(G)) = LA(x 1) d; (7.5) where 1 2 1 1 LA = 1 1 0 0 0 1 1 1 1 1 0 0 0 0 0 1 0 1 1 1 1 1 1 1 1 1 1 0 1 0 0 0 0 1 0 1 1 1 1 1 1 0 1 1 3 2 1 3 1 1 1 0 1 ; d= 0 : (7.6) 0 0 0 0 0 0 1 0 1 6 0 0 0 1 1 1 1 1 7 1 4 7 We now applying action of symmetry group S8 on Eq. (7:6) to get 40320 new nonlinear 4 5 6 5 components of block ciphers. The mathematical expression for these nonlinear compo- nents of block ciphers is given as follows: S8(S box) = S8(K LA G) = S8(K(LA(G)) = S8(LA(x 1) d): One of the

5proposed S-box is presented in Table 7.1. Table 7.1: The proposed S -box.

45 103 226 9 147 148 190 235 69 38 21 168 174 107 120 189 3 24 135 52 164 27 184 187 56 191 207 114 63 247 8 64 53 167 72 62 156 220 81 134 47 119 59 215 85 166 227 17 192 251 159 244 216 186 211 146 243 145 141 100 177 131 255 241 51 151 180 155 212 154 204 239 113 133 36 31 248 185 218 202 74 78 110 109 101 44 95 245 169 67 22 176 181 163 19 152 188 219 210 178 139 84 158 236 89 198 43 87 182 171 83 150 172 136 60 223 242 137 68 60 209 130 12 96 254 233 65 153 196 23 208 122 205 98 203 82 142 108 93 230 41 140 92 222 234 73 70 46 132 28 224 250 201 66 14 29 232 57 199 50 143 116 20 160 252 217 194 10 80 129 4 32 0 249 193 2 90 206 195 18 37 39 123 213 138 76 42 79 91 214 240 121 6 48 13 104 71 54 111 117 112 125 157 228 126 237 16 128 106 77 144 124 55 183 162 11 94 238 118 173 170 75 197 34 124 245 61 231 175 115 165 35 229 33 25 200 97 5 253 225 102 221 179 88 105 99 85 15 161 49 149 23 7 58 40 1 7.4 Proposed Video Encryption Algorithm

15Various video encryption techniques are proposed to encrypt the videos and used for obtaining highly encrypted videos. Our scheme mainly focuses on

the full encryption techniques. The following …gures (see Figs. 7.2-7.3) represent the proposed video encryption and decryption algorithm includes following stages: Start Read S-box Read Video Read Video Frames Split Frame into 3 Layers Pick one frame layer and convert each pixel into binary (Repeat it for other layers too) Split 8 bits binaries 4 bits MSB's 4 bits LSB's Row= Convert

2bits into decimal Column= Convert bits into decimal Pick element from S -box

Replace S-box element with video frame pixel Reconstruct video frame layers into one frame End Fig. 7.2: Video encryption algorithm. Read Encrypted Start Read Inverse S-box Video Read Encrypted Video Split

Frame into 3 Frames Layers Pick one frame layer and convert each pixel into binary (Repeat it for other layers too) Split 8 bits binaries 4 bits MSB's 4 bits LSB's Row= Convert

2**bits into decimal** Column= **Convert bits into decimal** Pick **element** from Inverse S **-box**

Replace Inverse S-box element with video frame pixel Reconstruct original video frame layers into one frame End Fig. 7.3: Video decryption algorithm. 7.5 Performance Parameters A decent encryption method ought to be vigorous against a wide range of cryptanalytic, alge- braic, statistical and other well-known security attacks. We have to characterize an arrangement of parameters in light of which we can assess and compare video encryption algorithms. A few parameters recorded underneath are accumulated from writing. Here we examine the secu- rity examination of the proposed video encryption plans in view of statistical investigation, for example, correlation, contrast, homogeneity, energy and entropy and so on. In statistical tex- ture examination, texture highlights

35**are computed from the statistical** conveyance **of observed combinations of intensities at** determined **positions** with respect **to each other in the** picture. **According to the number of intensity points (pixels) in** every **combination,** measurements **are** characterized **into** …rst-arrange, **second-** arrange **and higher-** arrange insights. **The Gray Level** Co-occurrence **Matrix (GLCM)** strategy **is a** method for extricating **second order statistical texture features. The approach has been** utilized as **a** part **of** various **applications.**

There are number of measurable strategies used to arrange the data security (encryption, watermarking and steganography) procedures in sight and sound applications. The …ve basic textures highlights talked about here are contrast, correlation, energy, homo- geneity, and entropy. Contrast is utilized to gauge the nearby varieties, relationship is utilized to quantify likelihood of event for a couple of particular pixels, energy is otherwise called con- sistency of ASM (angular second moment) which is the whole of squared components from the GLCM, homogeneity is to quantify the dissemination of components in the GLCM as for the corner to corner, and entropy measures the factual arbitrariness. The …ve regular surfaces highlights are given underneath: Entropy = p(xi; xj) logb p(xi; xj); XiXj Contrast = XiXj ji jj2

56**p(i;j);** Homogenity = XiXj **p(i; j)**

; 1 + ji jj

17**Energy = p(i;j)2;** Xi;j **Correlation = (i** i **)(j j)** p **(i;** j); XiXj **i j**

(7.7) (7.8) (7.9) (7.10) (7.11)

17**where i and j are two** di¤erent **gray levels of the image, p is the number of the co-appearance of gray levels i and j;**

i; j , are mean of i and j levels of image (a frame of video),

167**i and j are the** standard deviations **at i and j**

levels of an image. Entropy is utilized to gauge the substance of a picture with higher esteem demonstrating a picture with wealthier subtle elements. Contrast restores

17**a measure of the** power distinction **between a pixel and its neighbor over the** entire picture. **Homogeneity measures the** comparability **of** dim **scale levels** over **the** picture. Hence, bigger **the** adjustments **in the** dark **scale, the higher the GLCM Contrast and lower the homogeneity. GLCM energy measures the** general likelihood **of having** particular dark **scale** designs **in** picture. Relationship restores **a measure of how** associated **a pixel is to its neighbor over the** entire picture **and it** gauges **the joint** likelihood **of** event **of the** prede…ned **pixel**

sets. The exhibitions of these

4**nonlinear components of block ciphers transformation**

6and rely upon the idea of information and their applications.

The inquiry emerges how one can verify that one S-box is superior to other? To answer this inquiry, we have examined encourage measurable examinations which are able to answer the above inquiries. We take just two casings from unique video and encode these edges with most famous nonlinear parts of square …gure which incorporates

108Advanced encryption standard (AES), A¢ ne -power- a¢ ne (APA), Gray, Lui J, Residue prime, S8 AES, SKIPJACK, Xyi nonlinear components of

block ciphers. We use the second order texture analyses on the encrypted frames of given video. The aftere¤ects of these investigations are additionally analyzed

54to decide the propriety of an S-box to video encryption applications

(a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.4: Encryption of video …le through AES S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.5: Encryption of video …le through APA S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.6: Encryption of video …le through Gray S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.7: Encryption of video …le through Lui S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.8: Encryption of video …le through Prime S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.9: Encryption of video …le through S8-AES S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.10: Encryption of video …le through Xyi S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.11: Encryption of video …le through Skipjack S-box. (a)

13Original frame 1 (b) Original frame 2 (c) Encrypted frame 1 (d) Encrypted frame 2

Fig. 7.12: Encryption of video …le through proposed S-box. 7.5.1 Statistical Analyses Based Best S-box Selection Algorithm Here, we are giving a best selection criteria in the list of nonlinear components of block ciphers for video encryption techniques. This criteria fundamentally based on testing number of given nonlinear components of block ciphers for video encryption applications. Algorithm 42 Let us consider n nonlinear components of block ciphers say S1; S2; :::; Sn . We can say that S-box Si is optimal with respect to statistical analyses than Sj for j 2 f1; 2; :::; ngnf ig if the following conditions holds: i. If the Contrast and Entropy of Si is greater than Sj for j 2 f1; 2; :::; ngn fig, ii. If Correlation, Energy and Homogeneity of Si is less than Sj for j 2 f1; 2; :::; ngn fig. Table 7.2: Statistical analyses for a gray scale image. Statistical Properties Original Encryption of …rst frame with nonlinear components of block ciphers frame AES AP A Gray Lui P rime S8-AES Skipjaik Proposed Contrast Homogenity Entropy Correlation Energy 0:1688 0:9285 7:6315 0:9759 0:1445 4:8011 4:6630 4:4605 4:5877 4:6841 4:5957 4:5750 4:1867 0:4343 0:5307 0:5358 0:5300 0:5289 0:5297 0:5299 0:5395 7:9282 7:8361 7:7846 7:8140 7:8573 7:8312 7:8062 7:7454 0:0833 0:2299 0:1770 0:2135 0:2648 0:2229 0:1778 0:1761 0:0158 0:0269 0:0303 0:0279 0:0258 0:0274 0:0291 0:03185 Table 7.3: Statistical analyses for AES S-box for color frame image. Statistical properties Color components of original frame

11Color components of encrypted frame Red Green Blue Red Green Blue Contrast 0: 168844 0: 168391 0:

171648 4:814660 4:856900 4:867450

1Homogenity 0: 927243 0: 928763 0: 927245 0: 437077 0: 417827 0: 396663 Entropy 7: 785210 7: 495870 7: 487560 7: 961220 7: 927490 7: 940200 Correlation 0: 981038 0: 973687 0: 972199 0: 173149 0: 115769 0: 098270 Energy 0: 123563 0: 153702 0: 150333 0: 018441 0: 021502 0: 017411 Table

7.4: Statistical analyses for APA S-box for color frame image. Statistical properties Color components of original frame

11Color components of encrypted frame Red Green Blue Red Green Blue Contrast 0: 168844 0: 168391 0:

171648 4:64397 4:76191 4:56811

1Homogenity 0: 927243 0: 928763 0: 927245 0: 525618 0: 528458 0: 524481 Entropy 7: 785210 7: 495870 7: 487560 7: 82943 7: 85796 7: 80127 Correlation 0: 981038 0: 973687 0: 972199 0: 305289 0: 327557 0: 290148 Energy 0: 123563 0: 153702 0: 150333 0: 0248075 0: 0237682 0: 0257022 Table

7.5: Statistical analyses for Gray S-box for color frame image. Statistical properties Color components of original frame

11Color components of encrypted frame Red Green Blue Red Green Blue Contrast 0: 168844 0: 168391 0:

171648 4:46005 4:56879 4:44538

1Homogenity 0: 927243 0: 928763 0: 927245 0: 528096 0: 531388 0: 527558 Entropy 7: 785210 7: 495870 7: 487560 7: 78134 7: 80279 7: 75448 Correlation 0: 981038 0: 973687 0: 972199 0: 274416 0: 276426 0: 2440 Energy 0: 123563 0: 153702 0: 150333 0: 0269791 0: 0262526 0: 0281263 Table

7.6: Statistical analyses for Lui S-box for color frame image Statistical properties Color components of original frame

11Color components of encrypted frame Red Green Blue Red Green Blue Contrast 0: 168844 0: 168391 0:

171648 4:6073 4:70589 4:53046

1**Homogenity 0:** 927243 **0:** 928763 **0:** 927245 **0:** 523077 **0:** 526427 **0:** 523965 **Entropy 7:** 785210 **7:** 495870 **7:** 487560 **7:** 80182 **7:** 83796 **7:** 78305 **Correlation 0:** 981038 **0:** 973687 **0:** 972199 **0:** 274219 **0:** 312519 **0:** 302507 **Energy 0:** 123563 **0:** 153702 **0:** 150333 **0:** 0256633 **0:** 0241991 **0:** 0254364 **Table**

7.7: Statistical analyses for Prime S-box for color frame image. Statistical properties Color components of original frame

11**Color components of** encrypted frame **Red Green Blue Red Green Blue Contrast 0:** 168844 **0:** 168391 **0:** 171648 **0:**

46772 4:79047 4:56216

1**Homogenity 0:** 927243 **0:** 928763 **0:** 927245 **0:** 522392 **0:** 52806 **0:** 524674 **Entropy 7:** 785210 **7:** 495870 **7:** 487560 **7:** 8282 **7:** 89079 **7:** 83554 **Correlation 0:** 981038 **0:** 973687 **0:** 972199 **0:** 310132 **0:** 370774 **0:** 371136 **Energy 0:** 123563 **0:** 153702 **0:** 150333 **0:** 0248877 **0:** 0228422 **0:** 0235903 **Table**

7.8: Statistical analyses for S8-AES S-box for color frame image. Statistical properties Color components of original frame

11**Color components of** encrypted frame **Red Green Blue Red Green Blue Contrast 0:** 168844 **0:** 168391 **0:**

171648 4:56799 4:72119 4:552

1**Homogenity 0:** 927243 **0:** 928763 **0:** 927245 **0:** 524465 **0:** 524465 **0:** 523927 **Entropy 7:** 785210 **7:** 495870 **7:** 487560 **7:** 82253 **7:** 84331 **7:** 80726 **Correlation 0:** 981038 **0:** 973687 **0:** 972199 **0:** 31173 **0:** 325783 **0:** 304344 **Energy 0:** 123563 **0:** 153702 **0:** 150333 **0:** 024802 **0:** 0239544 **0:** 025042 **Table**

7.9: Statistical analyses for Skipjack S-box for color frame image. Statistical properties Color components of original frame

11**Color components of** encrypted frame **Red Green Blue Red Green Blue Contrast 0:** 168844 **0:** 168391 **0:**

171648 4:5651 4:67912 4:54009

1**Homogenity 0:** 927243 **0:** 928763 **0:** 927245 **0:** 523372 **0:** 525459 **0:** 522016 **Entropy 7:** 785210 **7:** 495870 **7:** 487560 **7:** 8045 **7:** 8144 **7:** 78273 **Correlation 0:** 981038 **0:** 973687 **0:** 972199 **0:** 285098 **0:** 279685 **0:** 262988 **Energy 0:** 123563 **0:** 153702 **0:** 150333 **0:** 0256217 **0:** 0251742 **0:** 0263711 **Table**

7.10: Statistical analyses for Xyi S-box for color frame image. Statistical properties Color components of original frame

11**Color components of** encrypted frame **Red Green Blue Red Green Blue Contrast 0:** 168844 **0:** 168391 **0:**

171648 4:45472 4:57534 4:42644

1**Homogenity 0:** 927243 **0:** 928763 **0:** 927245 **0:** 524562 **0:** 52732 **0:** 522999 **Entropy 7:** 785210 **7:** 495870 **7:** 487560 **7:** 81467 **7:** 85229 **7:** 80984 **Correlation 0:** 981038 **0:** 973687 **0:** 972199 **0:** 323574 **0:** 344926 **0:** 335634 **Energy 0:** 123563 **0:** 153702 **0:** 150333 **0:** 0250035 **0:** 0237999 **0:** 0247389 **Table**

7.11: Statistical analyses for proposed S-box for color frame image. Statistical properties Color components of original frame

11**Color components of** encrypted frame **Red Green Blue Red Green Blue Contrast 0:** 168844 **0:** 168391 **0:**

171648 4:83686 4:871580 4:866630

1**Homogenity 0:** 927243 **0:** 928763 **0:** 927245 **0:** 53130 **0:** 535748 **0:** 531762 **Entropy 7:** 785210 **7:** 495870 **7:** 487560 **7:** 84411 **7:** 854680 **7:** 782900 **Correlation 0:** 981038 **0:** 973687 **0:** 972199 **0:** 25098 **0:** 262701 **0:** 273437 **Energy 0:** 123563 **0:** 153702 **0:** 150333 **0:** 02879 **0:** 028085 **0:**

028427 The proposed criteria is justify for AES nonlinear components of block ciphers as it is quite evident from the tabulated values of contrast, homogeneity, correlation, energy and entropy of an encrypted frame through AES nonlinear components of block ciphers (see Tables 7.2-7.11). Applying the proposed algorithm for the selection of best S-box among eight, we have the following results: a. Contrast and entropy encrypted frames through proposed algorithm and AES S-box is higher than other nonlinear components of block ciphers. b. Correlation, homogeneity and energy of encrypted frames through suggested and AES nonlinear components of block cipher are less than the other existing nonlinear compo- nents of block ciphers. The investigations talked about

3**in this** exchange **for** video **encryption applications in** con- junction **with the proposed novel criteria to** pick **the best S-box,** additionally encourages **the** client **in** deciding **the** ideal S **-box**

for video encryption (see Tables 7.2-7.11).

3**While the proposed** standard **in this work** relates **to** video **encryption applications, this** rule **and** investigations **can be** adjusted **for other** imperative **encryption applications,** for example, **voice, video** conferenc- ing **and watermarking. The** investigation **of the proposed** foundation **for** various **encryption applications is the** subject **of** enthusiasm **for future work.**

7.6

189**Conclusion In this chapter, we have developed a**

new algorithm for video encryption that is based on substitution boxes. We have encrypted a video …le (number of frames) through well-known nonlinear components of block ciphers, i-e.,

39**AES, APA, Gray,** Prime, **S8-AES, Skipjack, Xyi**

and Lui. Also we have veri…ed the strength of all encrypted frames through our proposed statistical criteria which is based on second order texture features of an image developed by Haralick et. al., [67]. Such an analyses and technique is yet not available in existing literature. Chapter 8 Cryptosystems and Key Exchange Alforithms Based on Commutaitve Subgroups of GL2(Zpn); GL2(Zpn) and GL2(GF (pn)) Security is the most essential perspective in the …eld of web and system application. It is a vital errand to secure data over the system. To secure data, cryptography can be utilized. Cryptography can be separated into two sections that are "symmetric key cryptography" and "asymmetric key cryptography. In this part, we will primarily talk about public key cryptog- raphy. The

92**idea of "public key cryptography"** (PKC) **was presented by**

Whit…eld Di¢ e and Mar- tin Hellman in 1976 [132]. After that numerous executions of it have been proposed, and a signi…cant number of these cryptographic applications construct their

175**security with respect to the** unmanageability **of hard** scienti…c issues, **to**

be speci…c the limited …eld discrete logarithm problem (DLP) [139] and integer factorization problem (IFP) [133] [138]. To take care of these issues, sub-exponential time schemes have been produced throughout the years. Subsequently, key sizes developed to in excess of 1000 bits, 50**in order to** accomplish **a** sensible **level of security.** In **the**

conditions where transfer speed, registering force and capacity are constrained, doing thousand-piece tasks turns into a doubtful approach for giving adequate security. This is most obvious close by held gadgets, for example, the cell phones, PDAs, and pagers that have the extremely constrained preparing force and battery life. The idea of PKC advanced from an endeavor to assault two of the most troublesome issue related with symmetric encryption. The principal issue is that of key circulation under symmet- ric encryption requires either: (1) that two communicants as of now share a key, which has been conveyed some way or another to them; or (2) the utilization of key dispersion focus. The gen- eral public key cryptography process is portrayed in …rst chapter with the de…nition; it is clear that public key techniques depend on one key for encryption and an alternate yet numerically related key for unscrambling. These schemes have the accompanying critical attributes. Because of quick advancements in points of con…nement and conceivable outcomes of in- terchanges and data transmissions, there is a developing interest of cryptographic methods, which has prodded a lot of escalated examine exercises in the investigation of cryptography. A speculation of the discrete logarithms design schemes of secure information communication is the elliptic curve (EC) algorithms. Di¤erent new techniques were developed in literature by using EC along with already existing techniques for symmetric and asymmetric key cryp- tography, like EC-Di¢ e algorithm, EC-RSA, EC-Elgamal and EC-digital signatures schemes [140] [141]. Note that every one of the three families can be utilized to give the fundamental public key systems of the key foundation, nonrepudiation through computerized marks and encryption information. In this chapter, we have developed a novel public-key cryptosystem that uses large commutative subgroup of general linear group of units of local ring of degree 2. Moreover this chapter, depicts a key trade calculation that depends on Chebyshev polyno- mials. The primary extent of this chapter is to supplant the monomial with the Chebyshev polynomials Tn(x); Un(x) and supplant lattices in the contentions of Chebyshev polynomial in the Di¢ e-Hellman (DH) algorithms. As we know that Chebyshev polynomials ful…ll the semi-group characteristic on the set of real …eld R; they additionally have semi-group stu¤ over the set of integers Z. At that point, we can additionally expand the prescribed de…ni- tion over … nite …eld and also de…ne Chebyshev polynomials of …rst and second kinds denoted by Tn(x) and Un(x) over a …nite …eld Zp. Di¤erent properties of chebyshev polynomails were de…ned in therein references [150] [154]. 8.1 Commutative Subgroup of GL2(Zpn) Let H2(Zpn) be the subgroup of GL2(Zpn); which is given as follows: H2(Zpn) = 8 0 a1 b1 a a1; b1 2 Zpn and a21 b216 = 0 ; (8.1) < b 1 1 1 9 @ A = which shows that elements of subgroup H2(Zpn) are belong to unit group of residue ring Zpn that : ; is Zpn. The subgroup H2(Zpn) is an abelian subgroup GL2(Zpn). 8.2 Cryptosystems Established on Commutative Subgroups of GL2(Zpn) In this section, we are mainly discussed de…nition of cryptosystem, correspondence between mes- sages and rings; and proposed cryptosystem one which are based subgroup of GL2(Zpn) de…ned in section 2. We will discussed and explain in detail about the about the key generation, encryption and decryption algorithms of our proposed novel schemes. De…nition 43 A cryptosystem consists of quintuplet (A; R; ; E; D); where an alphabet A that contains all characters that can be used in messages, commutative ring R, one-one and onto transformations : A ! R, E : P ! C and D : C ! E: The main concepts which will be utilized in this chapter is that we de…ne a correspondence between element of alphabets set A and ring R that maps original message to the elements in R: The second step is to apply encryption function E that maps plaintext to cipher text C. We will apply the reverse procedure in order to recover the plaintext. In this chapter, we will use the following mapping which maps alphabets to a ring. We suppose that all messages are written in the alphabet A = fA1; A2; A3; A4g. We will take R = Z4 and let 1 : A1 ! R be given by 1

158**(A) = 0; 1(B) = 1; 1(C) = 3** and 1 **(D) = 4.**

For reference,we list the correspondence for 1 below [149]: Table 8.1: List of correspondence for 1: A1

190**A B C D** Z4 **0 1 2 3**

Now we will take R = Z8 and let 2 : A2 ! R be given by 2(A) = 0; 2(B) = 1; 2(C) = 2; :::; 2(H) = 7. For reference,we list the correspondence for 2 below: Table 8.2: List of correspondence for 2: L2 Z8

48**A 0 B 1 C 2 D 3 E 4 F 5 G 6 H 7**

Similarly for other rings, we have list the correspondence for 3 and 4 given as follows: Table 8.3: List of correspondence for 3: L3 Z16

48**A 0 B 1 C 2 D 3 E 4 F 5 G 6 H 7 I 8 J 9**

145**10 11 12 13 14 15 K L M N** O **P**

Table 8.4: List of correspondence for 4: L4 Z32 L4 Z32 16 17 18 19 20 21 22 23 24 25 26 27 28 29 A 0 Q B 1 R C 2 S

67**D 3 T E 4 U F 5 V G 6 W H 7 X I 8 Y J 9 Z K L M N**

10 11 12 13 ! # . O 14 & 30 P 15 * 31 where represent blank space. Suppose f(x) = x2 + 2x + 2 be irreducible and primitive polynomial for GF(32). Let root of this polynomial then f( ) = 0; i:e:; be the Galois Field (32) 2+2 +2=0 2= 2 and Since 2= 2 2 2 + 3 + 3) 3 mod 3 = 0 2 = + 1; p n 1 = 1;) 32 1 = 8 = 1 3 = 2 + 1; 4 = 2; 5 = 2 ; 6 = 2 + 2; 7 = + 2; 8 = 1: Gf (32) = 0; 1; ; 2; 3; 4; 5; 6; 7 ; = f0; 1; ; + 1; 2 + 1; 2; 2 ; 2 + 2; + 2g: Galois Field (33) Suppose f (x) = x3 + 2x2 + 1 be irreducible and primitive polynomial for GF(33). Let be the root of this polynomial therefore 3+2 2+1=0 3 = 2 2 1 ; = 2 2 1 + 3 + 3; = 2 + 2;) 3 mod 3 = 0 and pn 1 = 1) 33 1 = 26 = 1 3 = + 2; 2 4 = 2 + 2 + 2; 5 = 2 + 2; 6 = 2 +2 ; 2 7 8 9 10 26 = = 2 + 1; 2 + + 2; = 2 + 2 + 2; 2 = 2 + 2 + 1; . = 1: Gf (33) = f0; 1; ; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12; 13; 14; 15; 16; 17; 18; 19; 20; 21; 22; 23; 24; 25g; Gf (33) = f0; 1; ; 2; 2 + 2; 2 + 2 + 2; 2 + 2; 2 2 + 2; 2 + 1; 2 + + 2; 2 2 + 2 + 2; 2 + 2 + 1; + 2; 2 + 2; 2; 2 ; 2 2; 2 2 + 1; 2 2 + + 1; + 1; 2 + ; 2 2 + 2; 2 2 + 2 + 1; 2 + + 1; 2 2 + + 2; 1 + 2 ; 2 2 + g: 8.3 Projected Data Security System Established on Commuta- tive Subgroups 8.3.1 Cryptosystem I Process of Key Generation Since

195**in public key cryptography, the** owner **of public** and private **keys**

are receiver, therefore, at receiving end, user apply the steps given below in order to generate a keys: 1. Choose a prime number p and computes i = pn with n 2 2. Choose a matrix arbitrary A 2 GL2(Zpn) 3. Calculate the following matrices: B = A2; D = A3; B2D and BD2: 4. Choose a matrix F 2 GL2(Zpn): We now de…ne the automorphism : W ! (B2D) 1W(B2D); : W ! (BD2) 1W(BD2); (8.2) (8.3) (8.4) 8 W 2 M2(Zpn): The automorphisms and commute with each other. 5. Calcuate the following matrices: BD ; (F); (F 1): (8.5) 6. Receiver public keys are: n; BD ; (F); (F 1) ; (8.6) and receiver private keys are: (B; D): (8.7) Process of Encryption At the sending end, sender will do the following tasks: 1. We can represents the original messgae P as a array of 2 2 matrices over residue ring Zpn :

106**P (1); P (2); P (3); :::; P (k):**

(8.8) 2. Choose a arbitrary integer ki computes matrix: Y (i) = (BD)ki: (8.9) 8 P (i) (i = 1; 2; :::; k): 3. The automorphisms for 8 i = 1; 2; :::; k are given below: =(i) : W ! (Y (i)) 1W (Y (i)); (8.10) 8 W 2 GL2(Zpn): 4. Computes 8 i = 1;2;:::;k matrices

157**=(i)((N)); =(i)((N 1))** and **m(i)=(i)((N)):** 5. Choose 8 **i**

= 1;2;:::;k a arbitrary invertible elements 2Zn and …nd the ciphertext: C =

133**C(1); C(2); :::; C(k) ; C(i)** = (C1 **(i);** C2 **(i));** (8.11) C1 **(i) = i**

185**1=(i)(** (F **1));** C2 **(i)** = iP **(i)=(i)(** (F)); **i = 1;**

2; :::; k: (8.12) Process of Decryption At the receiving end, receiver will

125**perform the following steps in order to**

deciphering enciphered message: 1. Computes 8 i = 1; 2; :::; k using the private key:

161**d(i) = 1** (C1 **(i)) = 1 (i 1=(i)(** (F **1))):**

(8.13) 2. Computes 8

209**i = 1; 2; :::; k** matrices: P **(i)** = C2 **(i)**

d(i): (8.14) 3. In a …nal step, receiver can easily get back the original message i.e., plaintext P; as a string of sequences

106**P (1); P (2); P (3); :::; P (i):**

8.3.2 Cryptosystem II Process of Key Generation The process of key is generation is given below which will be peformed at receivers end: 1. Choose a arbitrary prime number p 2. Consider the general linear group GLn(Zp) = fA 2 Mn(Zp)j det(A)6 = 0g and take H GLn(Zp) 3. Choose matrices A; B 2 GLn(Zp) A = x1 y1 2 y1 x1 3 ; B = x2 y2 2 y2 x2 : 3 where x1; x2; y1; y2 2 Zp: 4 5 4 5 4. Now check A; B 2 H , if not then repeat step and choose those matrices which belong to H 5. Choose two polynomials

144**of the form f(x) = anxn + an 1xn 1 + ::: + a1x + a0;**

g(y) = bnyn + bn 1yn 1 + ::: + b1y + b0: where ai; bi 2 Zp 8 0 i n. 6. Find f(A); g(B) such that det(f(A))6 = 0; det(g(B))6 = 0 7. De…ne two commutative automorphisms of GLn(Zp) :

93**K ! (f(A))** 1K **(f(A)); : K** ! (g **(B))** 1K **(g(B))** for A; **B**

2 GLn(Zp). As the matrices A and B belongs to H therefore the automorphisms and : 8. Now de…ne the following automorphisms of GLn(Zp) : K !

73**(f(A)** 2g **(B))** 1K **(f(A)** 2g **(B));** : K ! **(f(A)** g **(B)** 2) 1K **(f(A)** g **(B)**

2); such that = 2; = 2: The automorphisms and comutes therefore, = 1; = 1 9. Choose an arbitrary matrix D 2 GLn(Zp) such that D 2= H 10. Find the following matrices D 1; (D); (D 1) 11. Public key for encryption is (p; (D); (D 1)); and private key for decryption is (f(A);g(B)): Process of Encryption For encryption following steps are performed 1. Consider the matrices of plaintext be

82**m(1);m(2);m(3);:::m(k) 2** GLn(Zp): **2.**

For every plaintext matrix m(i) (0 i k); choose a random matrix N(i) 2 H 3. De…ne automorphism for every 0 i k (i) : D (N(i)) 1D(N(i)): ! for every D 2 GLn(Zp): 4. For every 0 i k compute the following matrices

208**(i)((D 1)); (i)((D));** m **(i)**

(i)((D)): 5. Select a random unit 2 Zp and calucate the

109**ciphertext C = (C(1); C(2); :::; C(k));**

64**C(i) = (C1(i);** C2 **(i));** C1 **(i) = i** 1 **(i)((D** 1)); C2 **(i)** = m **(i) (i)(** (D)); 0 **i**

k : Process of Decryption Now follow the given steps below to decipher the encrypted messaage: 1. By using the private key

65**for 0 i k** comupte d **(i) = 1** (C1 **(i))** = 1 (1 **(i)(**

(D 1))): 2. Calculate the following matrices for 0

99**i k** m **(i)** = C2 **(i)d(i)** = (im **(i)** (i)(**(D)))** d **(i):**

3. Finally, deciphered message matrices

107**are m(1); m(2); m(3); :::; m(**

k): 8.3.3 Cryptosystem III Process of Key Generation 1. Consider a Galois …eld of order pn, i.e. GF (pn) 2. Choose two elements A; B 2 GF (pn) 3. Now choose an arbitrary element K 2 GF (pn) 4. De…ne the following automorphisms of GF (pn) : K ! (A2B) 1K(A2B); : K ! (AB2) 1K(AB2); such that = 2; = 2: The automorphisms and comutes therefore, = 1; = 1 : 5. Choose an arbitrary elements D 2 GF (pn) 6. Find the following elements D 1; (D); (D 1) 7. Public key for encryption is (p; (D); (D 1)); and private key for decryption is (A; B): Process of Encryption For encryption following steps are performed 1. Consider the plaintext be

82**m(1); m(2); m(3); :::m(k) 2** GF (pn): **2.** For every plaintext **m(**

i) (0 i k); choose a random element N(i) 2 GF (pn) 3. De…ne automorphism for every 0 i k (i) : ! (N(i)) 1D(N(i)): D for every D 2 GF (pn): 4. For every 0 i k compute the following elements (i)((D 1)); (i)((D)): 5. Select a random unit 2 GF (pn) and calucate the

109**ciphertext C = (C(1); C(2); :::; C(k));**

64**C(i) = (C1(i);** C2 **(i));** C1 **(i) = i** 1 **(i)((D** 1)); C2 **(i)** = im **(i) (i)(** (D)); 0 **i**

k: Process of Decryption Now follow the given steps below to decipher the encrypted messaage: 1. By using the private key

65**for 0 i k** compute d **(i) = 1** (C1 **(i))** = 1 (1 **(i)(**

(D 1))): 2. Calculate the following elements for 0

99**i k** m **(i)** = C2 **(i)d(i)** = (im **(i)** (i)(**(D)))** d **(i):**

3. Finally, deciphered messages

107**are m(1); m(2); m(3); :::; m(**

k): 8.4 New Extension of DH

201**-Algorithm In this section, we** are mainly discussed **the** extension **of** DH **algorithm**

over general linear group (which is already discussed in detail in previous chapter) chebyshev polynomials of …rst and second kind over prime residue …eld Zp. 8.4.1 Extension of DH Algorithm based on Tn(x) and GL(2; Zp) In this section, we are mainly discussed DH key exchange algorithm for …rst order chebyshev polynomial of …rst kind along with general linear group of degree 2 over …nite …eld. The key agreement algorithm using Tn(x) based on prime residue …eld and GL(2; Zp) is given as follows: 1. Sender generates a matrix h 2 GL(2; Zp) and prime p; 2. Sender selects a private number i which is degree of polynomial with constrain 0 < i < p; 3. Sender computes e = Ti(h) mod p 2 GL(2; Zp); 4. Transmitter sends p, h and e and to receiver, 5. Receiver selects a private number j with condition 0 < j < p; 6. Receiver computes f = Tj(h) mod p 2 GL(2; Zp); 7. Receiver then sends an emails f to sender, 8. Sender calculates the private key k1 = g with g = Ti(f) mod p; 9. Receiver calculates the private key k1 = l with l = Tj(e) mod p: The integer g for sender and integer l for receiver establish the shared secret key k1 as both have calculated Ti j(h) mod p. 8.4.2 Extension of DH Key Exchange Algorithm based on Un(x) and GL(2; Zp) We are now presenting a DH key agreement algorithm by using Chebyshev polynomials of second kind Un(x): 1. Sender generates a matrix h 2 GL(2; Zp) and prime p; 2. Sender selects a private integer i and j with a condition 0 < i; j < p; 3. Sender computes e = Tj(h) mod p; 4. Sender emails p; h and e to receiver, 5. Receiver takes a secret integer j with constrain that 0 < j < p; 6. Receiver computes f = Uij 1(h) mod p; 7. Receiver sends f to sender, 8. Sender …nds the private key k1 = g with g = Ui 1(Tj(h))Uj 1(h) mod p; 9. Receiver …nds the private key k1 = l with d = Uij 1(h) mod p: The integer g for sender and the integer l for receivers which establish the mutual secret key k1. 8.5 Case Study We have discussed in detail the examination of our proposed schemes in this section of chapter in order to authenticate our suggested techniques. 8.5.1 Example Process of Key Generation Since in public key encryption process, receiver at receiving end, will have to perform the following procedure to generate public and private keys: 1. Choose a prime number say p = 2 (due to local ring) and calculate n = p2 = 4: 2. Choose an arbitrary matrix A = 1 2 0 2 H2(Z4): (8.15) 2 1 1 @ A 3. Computes matrices B = A2 = 1 0 3 2 1 2 ; BD2 = 1 0 0 ; D = A3 = 0 1 1 0 2 3 1 ; B2D = 0 2 1 1 0 0 1 1 @ A @ A @ A @ (8.16A) 4. Receiver, choose an arbitrary invertible matrix F 2 GL2(Z4) : F = 3 2 0 1 1 : (8.17) 2 @ A 5. De…nes automorphisms of the ring GL2(Z4) : : W ! B 1W B; : W ! D 1W D; (8.18) 8 W 2 GL2(Z4): Now computes the automorphisms = 2 ; = 2; : W ! (B2D) 1W (B2D); : W ! (BD2) 1W (BD2): (8.19) (8.20) 6. Calculating the following matrices: BD = 3 2 ; (F) = 3 2 3 2 0 2 3 1 0 2 1 1 ; (F 1) = 0 1 : (8.21) 2 1 @ A @ A @ A 7. User A public key is 0 n = 4; (F) = 3 2 26 15 0 ; (F 1) = 3 2 0 ; BD = 2 1 1 2 1 1 0 ; (8.22) 17 11 11 @ @ A @ A @ A @ AA and private key 1 0 1 2 0 B = 0 1 ; D = 0 : (8.23) 0 1 2 1 11 @ @ A @ AA Process of Encryption Sender at message sending end, will do the following sequence of steps: 1. Presents the plaintext "BDAC" as a matrix P 2 GL2(Z4) : P = 3 1 0 (8.24) 0 2 1 2 GL2(Z4); @ A 2. Select the random integer k for instance k = 3; and computes the matrix: Y = (BD)3 = 2 0 2 @ 1 (8.25) 1 1 : A 3. De…ne automorphism # of the ring GL2(Z4) : = : W ! Y 1W Y; for every W 2 GL2(Z4): 4. Compute the matrices: =(

154**(F)) = Y 1 (F)Y** = 3 0 2 @ =(**(F** 1)) = **Y 1** (F 1 **)Y = 1**

0 2 @ 5. Now choose an invertible element of Z4 arbitrarily: = 3; 1 = 1: 6. Computes the ciphertext C = (C1; C2): 2 1 1 ; 2 A 1 1 : A C1 = 1=((F 1)) = 1 2 0 2 3 1 ; @ 1 1 A C 2 = P =((F)) = 0 1 : 0 2 @ A Process of Decryption Receiver, will do the following steps in order to recover original message: 1. Calculates the matrix d; using the private key: d = 1(C1) = (BD 1) 1C1(BD 1) = 3 0 2 @ 2 : 1 1 A (8.26) (8.27) (8.28) (8.29) (8.30) (8.31) (8.32) 2. The following matrix manipulations is use to get the original message: P = C2d = 1 3 0 (8.33) 0 2 1 : @ A 8.5.2 Example Process of Key Generation 1. Select a prime number p = 23 2. Consider a group GL2(Z23) and H GL2(Z23) 3. Choose two matrices A; B 2 GL2(Z23) A= 5 4 2 ;B= 6 1 (8.34) 5 5 3 2 1 6 3 4 5 4 5 4. NowcheckthatA; B2H,ifnotthenrepeatstep2andchoosethosematriceswhichbelongs to H 5. Choose two polynomials f (x) = 3x3 + 4x2 + 5x + 6; g(x) = x4 + 5x3 + 2x + 1; 6. Determine f (A) and g(B); i.e.

(8.35) (8.36) f(A) = 2 7 ; g(B) = 5 9 2 ; 7 2 3 2 9 5 3 and det(f(A)); det(g(B))6 = 0: 4 5 4 5 7. De…ne two commutative automorphisms of GL2(Z23): :

93**K ! (f(A))** 1K **(f(A)); : K** ! (g **(B))** 1K **(g(B));**

(8.37) (8.38) for A; B 2 GL2 2(Z23). As the matrices A and B belongs to H therefore the automorphisms and : 8. Now de…ne the following automorphisms of GL2 2(Z23) : K !

73**(f(A)** 2g **(B))** 1K **(f(A)** 2g **(B));** : K ! **(f(A)** g **(B)** 2) 1K **(f(A)** g **(B)**

2); such that = 2; = 2: (8.39) Automorphisms and commutes therefore, = 1; = 1 : (8.40) 9. Select a random matrix D= 12 2 35 3 2 GLn n(Zp); (8.41) 4 5 D 1= 18 2 2 3 22 3 (8.42) such that D 2= H: 4 5 10. Find the following matrices D 1= 18 2 3 4 2 22 3 5 (D) = 7 22 2 6 22 3 4 5 (D 1) = 20 9 2 19 20 3 11. Public key for encryption is 4 5 (8.43) (8.44) (8.45) p = 23; (D) = 7 22 20 9 0 2 6 22 3 ; (D 1) = 2 ; (8.46) 19 20 31 and private key for decryption is @ 4 5 4 5A 0 f (A) = 27 59 2 ; g(B) = 72 3 2 : (8.47) 95 31 @ 4 5 4 5A Process of Encryption For encryption following steps are performed 1. Consider the matrix of plaintext be m= 10 1 2 3 2 GL2(Z23): (8.48) 3 1 4 5 2. Choose a random matrix N= 41 2 H and its inverse N 1 = 11 3 2 14 3 2 3 11 3 4 5 4 5 3. De…ne automorphism of GL2(Z23) for every 0 i k (i) : D (N(i)) 1D(N(i)): ! for every D 2 GL2(Z23): 4. Compute the following matrices ((D)) = N 1 (D)N = 21 16 2 12 8 3 ; 4 5 (

62**(D 1)) = N 1 (D 1)N = 2**

16 2 12 15 3 : 5. Now select a unit element of Z23 randomly: 4 5 (8.49) (8.50) (8.51) = 3; 1 = 8: (8.52) 6. Compute the ciphertext C = (C1; C2); (8.53) C1 = 1 ((D 1)) = 16 13 2 ; 4 5 3 C2 = m ((D)) = 2 18 4 22 21 7 5 3 : 4 5 Process of Decryption Now follow the given steps below to decipher the encrypted message: 1. By using the private key for 0 i k compute (8.54) (8.55) d = 1 (C1) = 1 (1 ((D 1))) = 5 13 2 4 16 3 : (8.56) 2. Calculate the following matrices for 0 i k 4 5 m = C2d = (m ((D)))d = 10 1 2 3 : (8.57) 3 1 3. Finally, deciphered matrix is 4 5 m = 10 1 2 3 : (8.58) 3 1 4 5 8.5.3 Example Process of Key Generation 1. Consider a Galois …eld of order 32;i.e. GF (32): 2. Select two elements A; B 2 GF (32) A = 2 + 2; B = 2 ; (8.59) 3. De…ne the following automorphisms of GF (pn) : K ! (A2B) 1K(A2B); (8.60) : K ! (AB2) 1K(AB2): (8.61) 4. Let D = 2 + 1 be any random element of GF (32) and D 1 = 2 5. Compute the following elements

169**D 1 = 2 ; (D) = 2 + 1; (D 1) = 2**

: 6. Public key for encryption is (p = 3; (D) = 2 + 1; (D 1) = 2); and private key for decryption is (A = 2 + 2; B = 2): Process of Encryption For encryption following steps are performed (8.62) (8.63) 1. Consider the plaintext be m = 2 + 2 2 GF (32): (8.64) 2. For plaintext P = 2 + 2; choose a random element N = 2 2 GF (pn) and N 1 = 2 + 1 3. De…ne automorphism : D ! (N) 1D(N); for every D 2 GF (32): 4. Compute the following elements ((D 1)) = 2 ; ((D)) = 2 + 1: 5. Select a random unit = + 2 2 GF (pn); 1 = and calculate the ciphertext C = (C1; C2); (8.65) (8.66) (8.67) (8.68) C1 = 1 ((D 1) = 2 + 1; C2 = m ((D)) = 1: (8.69) (8.70) Process of Decryption Now follow the given steps below to decipher the encrypted message: 1. By using the private key compute d = 1((C1)) = 1((1 ((D 1)))) = 2 + 2: (8.71) 2. Calculate the following elements for 0 i k m = C2d = (m ((D)))d = 2 + 2: (8.72) 3. Finally, deciphered message is m = 2 + 2: (8.73) 8.5.4 Example We are now start with a very small example in order to understand the above mechanism for general linear group over prime residue …eld. We have taken i = 2 and j = 3 and calculate

57**T2(x) = 2x 2 1 ; T3(x) = 4x 3 3x** and T6 **(x**) = 32x 6 48x **4** 18x **2 1**

. 1. Transmitter selects p = 7 and h = 6 2 2 34 3 2 GL(2; Z7), 2. Transmitter selects i = 2, 4 5 3. Sender calculates the following values e = T2(h) mod 7 = 65 2 41 3 , 4 5 4. Sender then emails receiver p = 7, h and e, 5. Receiver at the receiving end selects j = 3, 6. Receiver calculates f = T3(h) mod 7 = 5 6 2 2 6 3 ; 7. Receiver emails f; 4 5 8. Sender/Transmitter calculates g = T2(f) mod 7 = 3 6 2 , 2 4 3 4 5 9. Receiver …nd l = T3(e) mod 7 = 3 6 2 . 2 4 3 4 5 8.5.5 Example We pick same integers in order to generate the …rst and second order Chebyshev polynomials. We select i = 2 and j = 3 and compute

57**T2(x) = 2x 2 1 ; T3(x) = 4x 3 3x** , U2 **(x**) = 4x **2 1** ; U3 **(x**) = 8x **3** 4x an U5 **(x**

) = 4x 5+3x 3+6x . The steps for DH key exchange algortihms based on Chebyshev polyno- mails of second kind and GL(2; Z7) are given below: 1. Transmitter selects p = 7 and h = 5 1 2 3 4 3 2 GL(2; Z7), 2. Transmitter selects i = 2, 4 5 3. Sender calculates the following values e = T2(h) mod 7 = 6 5 2 3 , 4 1 4 5 4. Sender then communicates receiver p = 7, h and e = U1(T3(h))U2(h) mod 7 = 2 0 2 3 , 0 2 5. Receiver at the receiving end selects j = 3, 4 5 6. Receiver …nds f = Uj 1(h) mod 7 = 6 4 2 5 2 3 ; 7. Receiver emails f; 4 5 8. Sender/Transmitter calculates g = U1(e)f mod 7 = 2 0 2 0 2 3 , 4 5 9. Receiver calculates l = Uij 1(h) mod 7 = 2 0 2 0 2 3 . 4 5 Similarly we can easily develop two more cases for chebyshev polynomials of second kind over local ring and simple ring. The idea of non-commutative structures along with orthogo- nal polynomials is utilized e¢ ciently in order to improve the DH exchange algorithm. With this improve scheme, we can easily use this design technique in modern cryptosystems while exchange key. 8.6 Conclusion The principal aim of this part of thesis is to device three innovative cryptosystems based on GL2(Zpn); GL2(Zp) and GL2(GF(pn)). We have design all three cryptosystems independently using three different structures inside general linear group. First, cryptosystem uses GL2(Zpn). Second, cryptosystem uses GL2(Zp) and third cryptosystem based on GL2(GF(pn)). The key generation section in cryptosystem III, is based on polynomial extension instead of matrices elements. This modification can easily be used in different multimedia applications. The key exchange issue is the means by which to trade whatever keys or other data are required with the goal that nobody else can get a duplicate. Generally, this required put stock in messengers, discretionary sacks, or some other secure channel. With the appearance of asymmetric/secret key algorithms, the scrambling key (general public/asymmetric key which is in pair) could be made public, since nobody without the decoding key could unscramble the message. Our objective here is to include greater many-sided quality in existing key trade algorithms keeping in mind the end goal to stop interloper to approach the private key. We have supplanted numbers with networks and one term articulation with polynomial of degree n. This change can extremely upgrade the current public key cryptosystems. Chapter 9 Conclusions The basic

121**distinction amongst feeling and reason is that feeling prompts activity, while reason prompts conclusions**

(by Donald Calne). When one thing closes, something else starts. At times finishing something harms, yet a fresh start is constantly worth and agony. To finish up this thesis, we abridge its principle commitments and recommend various headings for additionally look into. 9.1 Impacts of Present Thesis With the help of present thesis, we have examined distinctive parts of symmetric and asym- metric algorithms. After a short talk of the primary standards of symmetric and asymmetric encryption conspire, and a clarification of the method of reasoning behind various sorts of en- cryption algorithms are examined in first section. We have focused on various subjects which are altogether associated by one focal topic: the significance of nonlinear segment in particular nonlinear components of block ciphers in symmetric cryptography, watermarking and steganog- raphy. We have planned new nonlinear components of block ciphers in view of various algebraic structures. The subject of present theory is three crease, one with improvement of mathematical structures for differing interactive media applications, second to use these for advanced medium which incorporates content, picture, sound and video; and last one to approve the proposed algorithms through statistical examinations. The particular commitments made in this thesis are examined underneath: In chapters 2; 3 and 4; we have developed new nonlinear components of block ciphers based on finite Galois fields GF (24), symmetric group S4 and logarithmic permutations. We have not only designed small nonlinear components of block ciphers but also use these proposed nonlinear components of block ciphers for copyright protection and information hiding schemes. We have utilized 3D histogram to analyze the similarities in original and watermarked images. Various types of pixel difference and correlation based statis- tical analyses as well as algebraic analyses were used to testify the proposed copyright protection and information hiding techniques. The trust of new algebraic and statistical analyses plays a vital role in cryptographic algorithms. Several new and modified versions of algebraic and statistical analyses like

77**nonlinearity, strict avalanche criterion, bit independent criterion, linear and** differential **approximation**

probabilities, pixel differencing analyses, correlation based analyses and, human vision system based

110**analyses were** suggested **in order to** test **the strength of**

non- linear component of block cipher. In this sequel, we have proposed new algebraic analyses which include balancedness, nonlinearity, correlation immunity, absolute indicator, sum of square indicator, algebraic degree, algebraic immunity, transparency order, propaga- tion characteristics, strict avalanche criteria, number of fixed points, number of opposite fixed points, composite algebraic immunity, robustness to differential cryptanalysis, delta uniformity, SNR(DPA) and confusion coefficient variance which is main philosophy of chapter 5. There is always room of improvement in every science and technology area. Same hap- pened in cryptographic algorithms, where improvements are going by each instant of time. The algorithms development is very interesting task in information security, where we need different algebraic structures and statistical analyses in order to improve the later one and, validate new algorithms. In this respect, the idea of Galois ring based nonlinear components of block ciphers were projected in chapter 6 which is completely new dimen- sion of developing cryptographically secure new class of Boolean functions having high nonlinearity as compared to existing one. One look is worth a thousand words and images speak louder than words therefore we 200 are in the era of live streaming where video play a significant role. The importance of video in today's world can't be denied by anyone. The video fundamentally comprises of number of frames which means video can speaks millions and billions of worlds. Due to its importance in daily usage, protection of illegal access to video is also an emerging issue in today digital sphere of information age. In this regard, we have developed new nonlinear components of block ciphers which is based on Z257 and action of symmetric group S8 which is responsible to generate a large number of nonlinear components of block ciphers. The idea of video encryption based on mention structure is presented in chapter 7. The

137**idea of public key** cryptography **is to use two** di¤erent **keys for encryption and**

decryp- tion which arouse a new height in cryptography where we utilizing prime factorization and discrete log based algorithms most famous are RSA and Elgamal cryptosystems. Their extensions were developed based on matrix algebra which adds more complexity in sim- ple public key algorithms to cryptanalysis. The idea of subgroup of

199**general linear group** based **on units of local ring**

is use to develop a new cryptosystems in chapter 8. Also, we have extended the Di¢ e Hellman key exchange algorithm which is based on polynomails and general linear group of order 2 over prime residue …eld which is given in chapter 8. The Di¢ e Hellman key exchange algorithm proposed in chapter 8; have a high level of complexity as compared to standard algorithm which is based on discrete log property. 9.2 Future Research The research work of science and art shows people new directions and thinks of the future. Similarly e¤orts are not enough without purpose and future directions. Finally, we suggest some directions for further research. Idea of watermarking with small nonlinear components of block ciphers will further utilize in steganography of audio and also usefulness of these nonlinear components of block ciphers in frequency domains. The combination of encryption and watermarking scheme will be developed in future to provide more privacy in cryptosystems. Extending the algebraic analyses of chapter 5 to nonlinear components of block ciphers based on Galois ring which classifying larger

4**nonlinear components of block ciphers.** The idea **of**

small

4**nonlinear components of block ciphers with**

large number of bits is central point of chapter 6. This theory can easily be extended to other class of …nite chain ring and apply these

4**nonlinear components of block ciphers in**

digital multimedia applications. We apply proposed nonlinear components of block ciphers based on residue prime …eld Z257 and symmetric groups S8 of order 8! which create confusion capability and apply second order texture analyses. We can also add di¤usion layer through any discrete and continuous chaotic systems and, also add some more statistical analyses to con…rm the authentication of proposed algorithm. Finally, the theory of general linear group based algorithm can also be implemented on digital medium. We extend this idea to develop digital signature scheme based on subgroup of general linear group of unit of local ring.

Bibliography [1] C. E. Shannon, A mathematical theory of communication, Bell Labs. Tech. J., 27 (1948) 379–423. [2] C. E. Shannon, Communication theory of secrecy systems, Bell Labs. Tech. J., 28 (1949) 656–715. [3] C. Carlet, Boolean Functions for Cryptography and Error Correcting Codes, Chapter of the monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, (2010) 257-397. [4] C. Carlet, Partially-bent functions, Design Codes Cryptogr., 3(2) (1993) 135-145. [5] M. Matsui, Linear cryptoanalysis method for DES cipher, Lect. Notes. Comput. Sc., 765 (1994) 386-397. [6] R. L. McFarland, A discrete fourier theory for binary functions, R41 Technical paper, 1971. [7] P. K. Menon, On di¤erence sets whose parameters satisfy a certain relation, Proc. Amer. Math. Soc., 13 (1962) 739-745. [8] O. S. Rothaus, On bent functions, J. Combin. Theory Ser. A., 20 (1976) 300-305. [9] T. Siegenthaler, Correlation-immunity of nonlinear combining functions for cryptographic applications, IEEE Trans. Inf. Theory., 30(5) (1984) 776-780. [10] J. Christian, M. Hortmann and G. Leander, Boolean Functions, PhD thesis, (2012). [11] Jean-Pierre Flori. Boolean functions, algebraic curves and complex multiplication, Télé- com ParisTech, 2012. [12] H. Dobbertin, Construction of bent functions and balanced Boolean functions with high nonlinearity, Lect. Notes. Comput. Sc., 1008 (1994) 61-74. [13] Thomas Cusick, Pantelimon Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2009. [14] C. Carlet, A construction of bent functions, Finite Fields Th. App. 233 (4) (1996) 47-58. [15] S. Chee, S. Lee and K. Kim, Semi-bent functions, Lect. Notes. Comput. Sc., 917 (1995) 107-118. [16] Y. Zheng, X. M. Zhang, Plateaued functions, Lect. Notes. Comput. Sc., 1726 (1999) 284-300. [17] C. Carlet, E. Prouf, On plateaued functions and their constructions, Lect. Notes. Comput. Sc., 2887 (2003) 54-73. [18] A. Menezes, P. van Oorschot, S. Vanstone, Applied Cryptography. CRC, Boca Raton, 1996. [19] Seitz J (2005) Digital watermarking for digital media. Idea Group Publishing, Hershey, PA. doi:10.4018/978-1-59140-518-4.ch001 [20] Cox IJ, Miller ML, Bloom JA, Fridrich J, Kalker T (2008) Digital watermarking and steganography, 2nd edn. Morgan Kaufmann Publisher, San Francisco, CA [21] Ruanaidh JJKO, Dowling WJ, Boland FM (1996) Watermarking digital images for copy- right protection. In: IEEE ProcVis. Image Signal Process, vol 143, No 4, pp 250–254 [22] Cox IJ, Kilian J, Leighton T, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687 [23] Alghoniemy M, Tew…k AH (2004) Geometric invariance in image watermarking. IEEE Trans Image Process 13(2):145–153. 204 [24] Yang Z, Campisi P, Kundur D (2004) Dual domain watermarking for authentication and compression of cultural heritage images. IEEE Trans Image Process 13(3):430–448 [25] Ruanaidh

JJKO, Pereira S (1998) A secure robust digital image watermark. In: Proceed- ings of SPIE 3409, Electronic imaging: processing, printing, and publishing in color, 150. doi:10.1117/ 12.324106 [26] Venkatesan R, Jakubowski M (2000) Image watermarking with better resilience. In: Pro- ceeds ICIP 2000 [27] Barni M, Bartolini F, Piva A (2001) Improved wavelet-based watermarking through pixel- wise masking. IEEE Trans Image Process 10: 783–791 [28] Tefas A, Nikolaidis A, Nikolaidis N, Solachidis V, Tsekeridou S, Pitas I (2001) Statistical analysis of markov chaotic sequences for watermarking applications. In: Proceedings of IEEE international symposium on circuits and systems (ISCAS2001) [29] Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. J Pattern Recognit Soc 37:469–474 [30] Bamatraf A, Ibrahim R, Salleh M, Mohd N (2011) A new digital watermarking algorithm using combination of least signi…cant bit (LSB) and inverse bit. J Comput 3:1–8 [31] Nikolaidis S, Pitas I (2008) Comparison of di¤erent chaotic maps with application to image watermarking. In: Proceedings of IEEE international symposium on circuits and system cryptography based on chaotic random maps with position dependent weighting probabilities Chaos, Solitons & Fractals 35 pp 362–369 [32] Giovanardi A, Mazzini G (2001) Frequency domain chaotic watermarking. In: Proceedings of IEEE Symposium Circuits and System, Sydney, vol 2, pp 521–524 [33] Sujatha SS, Sathik MM (2012) A novel DWT based blind watermarking for image au- thentication. Int J Netw Secur 14(4) : 223–228 205 [34] Hsu CT, Wu JL (1998) DCT-based watermarking for video. IEEE Trans Consum Electron 44(1):206–216 [35] Cox IJ, Miller ML, Bloom JA (2001) Digital watermarking, 1st edn. Morgan Kaufmann Publisher, San Fransisco [36] Kutter M, Jordan F, Digital watermarking technology. AlpVision, Switzerland, pp 1–4 [37] Morimoto Norishige (1999) Digital watermarking technology with practical applications. Inf Sci 2:107–111 [38] Luo H, Chu SH, LuZM(2008) Self-embeddingwatermarking using half toning technique. Circuits Syst Signal Process 27:155–170 [39] Lee YK, Bell G, Huang SY, Wang RZ, Shyu SJ (2009) An advanced least-signi…cant-bit embedding scheme for steganographic encoding. Springer, Berlin [40] Rashi Singh and Gaurav Chawla, A Review on Image Steganography, International Jour- nal of Advanced Research in Computer Science and Software Engineering, 4 (5) (2014) 686-689. [41] Archana.O.Vyas, Sanjay.V. Dudul, An Overview of Image Steganographic Techniques, International Journal of Advanced Research in Computer Science, 6 (2015) 67-72. [42] Z. Wang and A. C. Bovik, A universal image quality index, IEEE Signal Processing letters, vol. 9, no.3, pp. 81-84, March 2002 [43] Chandrasekharappa TGS, Prema KV, Shama K (2011) nonlinear components of block ciphers generated using a¢ ne transformation giving maximum avalanche e¤ect. Int J Comput Sci Eng 3:3185–3193 [44] Cid Carlos, Murphy Sean, Robshaw Matthew (2006) Algebraic Aspects of the advanced encryption standard. Springer, US [45] Khan M, Shah T (2014) A novel statistical analysis of chaotic S-box in image encryption. 3D Res 5:16. doi:10.1007/s13319-014-0016-5 [46] A. Piva, F. Bartolini, M. Barni , Managing copyright in open networks, IEEE Trans. Internet Comput., 6(3) (2002) 18-26. [47] C. Lu, S. Huang, C. Sze, H. Y. M. Liao , Cocktail watermarking for digital image protec- tion, IEEE Trans. Multimedia., 2(4) (2000) 209-224. [48] M. M. Latha, G. M. Pillai, K. A. Sheela, Watermarking based content Security and Multimedia Indexing in digital Libraries, International Conference on Semantic Web and Digital Libraries, (2007). [49] W. Bender, D. Gruhi, N. Morimota, A. Lu, Techniques for Data Hiding, IBM. Syst. J., 35 (3-4) (1996) 313 - 336. [50] Majid Khan, Tariq Shah and Syeda Iram Batool, A color image watermarking scheme based on a¢ ne transformation and S4 permutation, Neural Comput & Applic, Springer, (2014) 25:2037–2045. [51] Ingemar J. Cox, Matt L. Miller and Je¤rey A. Bloom, Watermarking applications and their properties, Int. Conf. on Information Technology'2000, Las Vegas, 2000 [52] Majid Khan, Tariq Shah, An e¢ cient construction of substitution box with fractional chaotic system, Signal, Image and Video Processing, DOI 10.1007/s11760-013-0577-4. [53] Abuelyman ES, Alsehibani AAS (2008). An optimized implementation of the S-Box using residue of prime numbers. Int. J. Comput. Sci. Ntwk. Secur., 8(4): 304-309. [54] Alam GM, Mat Kiah ML, Zaidan BB, Zaidan AA, Alanazi HO (2010). Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. Int. J. Phys. Sci., 5(21): 3254-3260. [55] Cui L, Cao Y (2007). A new S-box structure named A¢ ne- PowerA¢ ne. Int. J. Innov. Comput. I., 3(3): 45-53. [56] Daemen J, Rijmen V (1999). AES Proposal: Rijndael. AES Algorithm Submission, Avail- able: http://csrc.nist.gov/archive/aes/rijndael/ Rijndael-ammended.pdf. [57] Enayatifar R (2011). Image encryption via logistic map function and heap tree. Int. J. Phys. Sci., 6(2): 221:228. [58] Gadelmawla ES (2004). A vision system for surface roughness characterization using the gray level co-occurrence matrix. NDT & E. Int., 37(7): 577-588. [59] Hussain I, Shah T, Mehmood H (2010). A New Algorithm to Construct Secure Keys for AES. Int. J. Cont. Math. Sci., 5(26): 1263-1270. [60] Lui J, Wai B, Cheng X, Wang X (2005). An AES S-box to increase complexity and cryptgraphic analysis. Int. Conf. Infor. Network. Appl.,1: 724-728. [61] Prasadh K, Ramar K, Gnanajeyaraman R (2009). Public key cryptosystems based on chaotic Chebyshev polynomials. Int. J. Phys. Sci., 1(7): 122-128. [62] Shi XY, Xiao Hu You XC, Lam KY (2002). A Method for Obtaining Cryptographically Strong 8 8 nonlinear components of block ciphers. Int. Conf. Infor. Network. Appl., 2(3): 14-20. [63] SKIPJACK (1998). KEA Algorithm. Speci…cations version, 2(29): 1-23. [64] Tran MT, Bui DK, Doung AD (2008). Gray S-box for Advanced Encryption Standard. Int. Conf. Comp. Intel. Secur., 253-256. [65] J.M.H. du Buf, M. Kardan and M. Spann,"Texture Feature Performance of Image Seg- mentation", Pattern Recognition, Vol. 23, pp. 291-309, 1990. [66] JC.C. Gotlieb and H.E. Kreyszig,"Texture Descriptors based on Co-ocurrence Matri- ces",Computer Vision, Graphics, and Image Processing, Vol. 51, pp. 70-86, 1990. [67] R.M. Haralick, K. Shanmugam, and I. Dinstein,"Textural Features for Image Classi… ca- tion", IEEE Trans. on Systems, Man and Cybernetics, Vol. SMC-3, pp. 610-621, 1973. [68] R.M. Haralick and K. Shanmugam, "Computer Classi…cation of Reservoir Sandstones", IEEE Trans. on Geo. Eng., Vol. GE-11, pp. 171-177, 1973. [69] D.C. He, L.Wang, and J. Juibert, "Texture Feature Extraction", Pattern Recognition Letters, Vol. 6, pp. 269-273, 1987. 208 [70] M. Iizulca, "Quantitative evaluation of similar images with quasi-gray levels", Computer Vision, Graphics, and Image Processing, Vol. 38, pp. 342-360, 1987. [71] S. Peckinpaugh,"An Improved Method for Computing Gray-Level Coocurrence Matrix Based Texture Measures", Computer Vision, Graphics, and Image Processing; Graphical Models and Image Processing, Vol. 53, pp. 574-580, 1991. [72] L.H. Siew, R.H. Hodgson, and E.J. Wood, "Texture Measures for Carpet Wear Asess- ment", IEEE Trans. on Pattern Analysis and Machine Intell., Vol. PAMI-10, pp. 92-105, 1988. [73] L.H. Siew, R.H. Hodgson, and E.J. Wood, "Texture Measures for Carpet Wear Asess- ment", IEEE Trans. on Pattern Analysis and Machine Intell., Vol. PAMI-10, pp. 92-105, 1988. [74] M.M. Trivedi, R.M.

Haralick, R.W. Conners, and S. Goh, ”Object Detection based on Gray Level Coocurrence”, Computer Vision, Graphics, and Image Processing, Vol. 28, pp. 199-219, 1984. Albregtsen : Texture Measures Computed from GLCM-Matrices 14 [75] M Unser, ”Sum and Di¤erence Histograms for Texture Classi…cation”, IEEE Trans. on Pattern Analysis and Machine Intell., Vol. PAMI-8, pp. 118-125, 1986. [76] J.S. Weszka, C.R. Dyer, and A. Rosenfeld, “A comparative Study of Texture Measures for Terrain Classi…cation”, IEEE Trans. on Systems, Man and Cybernetics, Vol. SMC-6, pp. 269-285, 1976. [77] JC-M. Wu, and Y-C. Chen, “Statistical Feature Matrix for Texture Analysis”, Computer Vision, Graphics, and Image Processing; Graphical Models and Image Processing, Vol. 54, pp. 407-419, 1992. [78] T. Shah, N. Mehmood, A.A. Andrade and R. Palazzo Jr., Maximal cyclic subgroups of the groups of units of Galois rings: A computational approach, Computational and Applied Mathematics- (40314/CAM) DOI 10.1007/s40314-015-0281-9 [79] Bart Preneel’, Werner Van Leekwijck, Luc Van Linden, Rem Govaerts and Joos Vandewalle, Propagation characteristics of Boolean functions, Advances in Cryptology - EU- ROCRYPT ’90, LNCS 473, pp. 161-173, 1991. 0 Springer-Verlag Berlin Heidelberg 1991. [80] W. Meier, Othmar Sta¤elbach, Nonlinearity criteria for cryptographic functions, Ad- vances in Cryptology — EUROCRYPT ’89, Volume 434 of the series Lecture Notes in Computer Science pp 549-562. [81] X.-M. Zhang and Y. Zheng. Autocorrelations and new bounds on the nonlinearity of Boolean functions. Advances in Cryptology – EUROCRYPT, 96, no. 1070 in Lecture Notes in Computer Science, Springer-Verlag, pp. 294-306, 1996. [82] D. Olejar and M. Stanek. On cryptographic properties of random Boolean functions.” Journal of Universal Computer Science, vol. 4, No.8, pp. 705-717, 1998. [83] Y. Zheng, X.-M. Zhang, and H. Imai. Restriction, terms and nonlinearity of Boolean functions. Theoretical Computer Science, 226(1-2),pp. 207-223, 1999. [84] P. Sarkar and S. Maitra. Nonlinearity Bounds and Constructions of Resilient Boolean Functions. CRYPTO 2000, LNCS, vol. 1880, ed. Mihir Bellare, pp. 515-532, 2000. [85] P. Sarkar and S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. Advances in Cryptology - EUROCRYPT 2000, no. 1807 in Lecture Notes in Computer Science, Springer Verlag, pp. 485-506, 2000. [86] A. Canteaut, C. Carlet, P. Charpin and C. Fontaine. Propagation characteristics and correlation-immunity of highly nonlinear Boolean functions. Proceedings of EURO- CRYPT’2000, Advances in Cryptology, Lecture Notes in Computer Science n 187, pp. 507-522 (2000). [87] E. Pasalic, T. Johansson, S. Maitra and P. Sarkar. New constructions of resilient and cor- relation immune Boolean functions achieving upper bounds on nonlinearity. Proceedings of the Workshop on Coding and Cryptography 2001, published by Electronic Notes in Discrete Mathematics, Elsevier, vo. 6, pp. 425-434, 2001. 210 [88] S. Maitra. Highly nonlinear balanced Boolean functions with very good autocorrelation property. Proceedings of the Workshop on Coding and Cryptography 2001 published by Electronic Notes in Discrete Mathematics, Elsevier, vo. 6, pp. 355-364, 2001. [89] J. Clark, J. Jacob, S. Stepney, S. Maitra, W. Millan, Evolving Boolean functions satisfying multiple criteria, in: INDOCRYPT 2002, Lecture Notes in Computer Science, vol. 2551, Springer, Berlin, 2002, pp. 246–259. [90] C. Carlet. A larger Class of Cryptographic Boolean Functions via a Study of the Maiorana- McFarland Construction. Advances in Cryptology - CRYPT0 2002, no. 2442 in Lecture Notes in Computer Science, pp. 549-564, 2002. [91] P. Charpin. Normal Boolean functions, Journal of Complexity 20, pp. 245-265, 2004. [92] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. Fast Software Encryption, Second International Workshop, Lecture Notes in Computer Science 1008, pp.61-74, 1995. [93] A. Canteaut and M. Videau. Symmetric Boolean functions. IEEE Transactions on Infor- mation Theory 51(8), pp. 2791-2811, 2005. [94] D. K. Dalai, K. C. Gupta and S. Maitra. Cryptographically Signi…cant Boolean functions: Construction and Analysis in terms of Algebraic Immunity. Fast Software Encryption 2005, Lecture Notes in Computer Science 3557, pp. 98-111, 2005. [95] A. Braeken and B. Preneel, On the algebraic immunity of symmetric Boolean functions, in INDOCRYPT 2005, Lecture Notes in Computer Science. Berlin, Germany: Springer- Verlag, 2005, pp. 35-48. [96] C. Carlet, D. Dalai, K. Gupta and S. Maitra. Algebraic Immunity for Cryptographi- cally Signi…cant Boolean Functions: Analysis and Construction. IEEE Transactions on Information Theory, vol. 52, no. 7, pp. 3105-3121, July 2006. [97] Li, N., Qi, W.-Q.: Construction and analysis of Boolean functions of 2t + 1 variables with maximum algebraic immunity. In: Lai, X., Chen, K. (eds.) ASIACRYPT 2006. LNCS, vol. 4284, pp. 84–98. Springer, Heidelberg (2006). 211 [98] Sihem Mesnager, Improving the Lower Bound on the Higher Order Nonlinearity of Boolean Functions With Prescribed Algebraic Immunity, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 54, NO. 8, AUGUST 2008, [99] Wei Guo Zhang, Member, IEEE, and GuoZhen Xiao, Constructions of Almost Optimal Resilient Boolean Functions on Large Even Number of Variables, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 55, NO. 12, DECEMBER 2009 [100] Qichun Wang, Jie Peng, Haibin Kan, Member, Constructions of Cryptographically Sig- ni…cant Boolean Functions Using Primitive Polynomials, IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. 56, NO. 6, JUNE 2010. [101] Enes Pasalic and Yongzhuang Wei, On the Construction of Cryptographically Signi…-cant Boolean Functions Using Objects in Projective Geometry Spaces, IEEE TRANSAC- TIONS ON INFORMATION THEORY, VOL. 58, NO. 10, OCTOBER 2012 6681 [102] B. Chor, O. Goldreich, J. Hastad, J. Freidmann, S. Rudich, and R. Smolensky, The bit extraction problem or t resilient functions, In Foundations of Computer Science, 1985, 26th Annual Symposium, 396-407. [103] J. F. Dillon, A survey of bent functions, The NSA technical journal, (1972) 191-215. [104] R. Forre, The strict avalanche criterion: Spectral properties of boolean functions and an extended de…nition, Lect. Notes. Comput. Sc., 403 (1990) 450-468. [105] M. Matsui, Linear cryptoanalysis method for DES cipher, Lect. Notes. Comput. Sc., 765 (1994) 386-397. [106] Preneel, V. Leekwijk, V. Linden, Govaerts and Vandewalle, Propagation characteristics of boolean functions, Lect. Notes. Comput. Sc., 473 (1991) 161-173. [107] A. F. Webster and S. E. Tavares. On the design of nonlinear components of block ciphers, Lect. Notes. Comput. Sc., 218 (1986) 523-534. [108] Y. Zheng, X. M. Zhang, Plateaued functions, Lect. Notes. Comput. Sc., 1726 (1999) 284-300. 212 [109] Y. Zheng, M. Zhang, Improved upper bound on the nonlinearity of high order correlation immune functions, Lect. Notes. Comput. Sc., 2012 (2001) 262-274. [110] M. Matsui, The …rst experimental cryptanalysis of the Data Encryption Standard, Lect. Notes. Comput. Sc., 839 (1994) 1–11. [111] H. M. Heys, A tutorial on linear and di¤erential cryptanalysis, Technical Report CORR 2001-17, Centre for Applied Cryptographic Research, Department of Combinatorics and Optimization, University of Waterloo, March 2001. [112] E. Biham, A. Shamir, Di¤erential cryptanalysis of DES like cryptosystems, Lect. Notes. Comput.

Sc., 537 (1991) 2–21. [113] T. Siegenthaler, Correlation-Immunity of Nonlinear Combining Functions for Crypto- graphic Applications, IEEE Transactions on Information Theory 30 (5) (1984) 776–780. [114] L. L. Bartosov, Linear and di¤erential cryptanalysis of reduced-round AES, Tatra Mt. Math. Publ., 50(1) (2011) 51-61. [115] G. Chen, Y. Chen, X. Liao, An extended method for obtaining nonlinear components of block ciphers based on three-dimensional chaotic Baker maps, Chaos Solitons Fract., 31(3) (2007) 571–577. [116] F. Özkaynak, A. B. Özer, A method for designing strong nonlinear components of block ciphers based on chaotic Lorenz system, Phys. Lett. A., 374(36) (2010) 3733–3738. [117] Y. Wang, K. W. Wong, X. Liao, T. Xiang, A block cipher with dynamic nonlinear compo- nents of block ciphers based on tent map, Commun. Nonlinear Sci. Numer. Simul., 14(7) (2009) 3089-3099. [118] Y. G. Chen, X. Liao, An extended method for obtaining nonlinear components of block ciphers based on three-dimensional chaotic Baker maps, Chaos Solitons Fract., 31(3) (2007) 571-577. [119] T. Guoping, L. Xiaofeng, C. Yong, A novel method for designing nonlinear components of block ciphers based on chaotic maps, Chaos Solitons Fract., 23(2) (2005) 413-419. 213 [120] G. Jakimoski, L. Kocarev, Chaos and cryptography: Block encryption ciphers based on chaotic maps, IEEE Trans. Circuits Syst., 48(2) (2001) 163-170. [121] C. Adams, S. Tavares, Good nonlinear components of block ciphers are easy to …nd, Lect. Notes. Comput. Sc., 89 (1989) 612–615. [122] A. F. Webster, S. Tavares, On the design of nonlinear components of block ciphers, Lect. Notes. Comput. Sc., 85 (1986) 523–534. [123] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, An e¢ cient method for the construction of block cipher with multi-chaotic systems, Nonlinear Dynam., 71(3) (2013) 489–492. [124] J. P. Pieprzyk, Non-linearity of Exponent Permutations, Lect. Notes. Comput. Sc., 434 (1990) 80-92. [125] C. Carlet and K. Feng, An in…nite class of balanced functions with optimal algebraic immunity, good immunity to fast algebraic attacks and good nonlinearity," in Advances in Cryptology-ASIACRYPT 2008 (Lecture Notes in Computer Science), Springer-Verlag, 2008, vol. 5350, pp. 425-440. [126] Z. Tu and Y. Deng, nA conjecture on binary string and its applications on constructing boolean functions of optimal algebraic immunity," Designs, Codes Cryptogr., 2010. Online First Articles. DOI 10.1007/s10623-010-9413-9. [127] Q. Wang, J. Peng, H. Kan, and X. Xue, Constructions of cryptographically signi…cant Boolean functions using primitive polynomials," IEEE Trans. Inf. Theory, vol. 56, no. 6, pp. 3048-3053, 2010. [128] Xiaohu Tang, Deng Tang, Xiangyong Zeng and Lei Hu, Balanced Boolean Functions with (Almost) Optimal Algebraic Immunity and Very High Nonlinearity. [129] P. Stanica, Nonlinearity, local and global avalanche characteristics of balanced Boolean functions, Discr. Math., vol. 248, pp. 181-193, 2002. [130] P. Stanica, S. H. Sung, Improving the nonlinearity of certain balanced Boolean functions with good local and global avalanche characteristics, Inf. Process. Lett., vol. 79, pp. 167- 172, 2001. [131] P. Stanica, S. H. Sung, Boolean functions with …ve controllable cryptographic properties, Des., Codes Cryptogr., vol. 31, no. 2, pp. 147-157, 2004. [132] W. Di¢ e and M.E. Hellman, New directions in cryptography, IEEE Transactions on Information Theory 22 (1976), 644-654. [133] R.L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM 21 (1978), pp. 120-126. [134] H.C. Williams, A Modi…cation of the RSA Public-Key Encryption Procedure, IEEE Transactions on Information Theory, IT No.6 (26), 1980, pp. 726-729. 1.1 [135] Z. Cao, Conic analog of RSA cryptosystem and some improved RSA cryptosystems, Journal of Natrual Science of Heilongjiang University, 16 (4), 1999. 1.1 [136] Z. Cao, The multi-dimension RSA and its low exponent security, Science in China (E Series), 43 (4): 349-354, 2000. [137] M.O. Rabin, Digitized signatures and public-key functions as intractible as factorization, MIT Laboratory for Computer Science Technical Report, LCS/TR-212 (1979). [138] P. Smith and M. Lennon, LUC: A newpublic key system, Proceedings of the IFIP TC11 Ninth International Conference on Information Security, IFIP/Sec 93, 103-117, North- Holland, 1993. [139] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete loga- rithms, IEEE Transactions on Information Theory, 31 (1985), pp. 469-472. [140] K. Komaya, U. Maurer, T. Okamoto and S. Vanston, New public-key schemes bases on elliptic curves over the ring Zn, Int. J. Feigenbaum (Ed.): Crypto'91, LNCS 576, Springer-Verlag (1992), pp. 252-266. [141] P. K. Shau, R. K. Chhotray, Gunamani Jena, S Pattnaik, An Implementation of Elliptic Curve Cryptography, Int. J. Eng. Res. Tech. 2 (2013) 1-8. [142] C. Cid, S. Murphy, and M.J.B. Robshaw Small Scale Variants of the AES, Proceedings of FSE 2005, LNCS, 2005, 145-162. Springer-Verlag. [143] Jorge Nakahara Jr, Daniel Santana de Freitas, Mini ciphers: a reliable testbed for crypt- analysis?, "Symmetric Cryptography", Seminar 09031, 2009. Dagstuhl Seminar Proceed- ings. 1862-4405. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (eds.), Germany. [144] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher", The 9th International Workshop on Cryptographic Hardware and Embedded Systems - CHES 2007, LNCS 4727, P. Paillier and I. Verbauwhede (eds.), Berlin, Germany: Springer- Verlag, pp. 450-466, 2007. [145] Mihajloska, H., Gligoroski, D.: Construction of Optimal 4-bit nonlinear components of block ciphers by Quasigroups of Order 4. In: The Sixth International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2012, Rome, Italy (2012). [146] Raphael Chung-Wei Phan; Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students, Published in Cryptologia, XXVI (4), 2002. [147] Hanem M. El-Sheikh, Omayma A. El-Mohsen, Talaat Elgarf, and Abdelhalim Zekry, A New Approach for Designing Key-Dependent S-Box De…ned over GF (24) in AES, International Journal of Computer Theory and Engineering Vol. 4, No. 2, April 2012. [148] J.C. Interlando, R. Palazzo Jr., M. Elia, On the decoding of Reed-Solomon and BCH codes over integer residue rings, IEEE Trans. Inform. Theory, IT-43 (1997) 1013–1021. [149] Richard Klima, Neil Sigmon, Ernest Stitzinger, Applications of Abstract Algebra with Maple and MATLAB, Chapman and Hall/CRC; 2 edition (July 12, 2006). [150] Kocarev L., Tasev Z., Public-key encryption based on Chebyshev maps, The 2003 IEEE International Symposium on Circuits and Systems Proceedings, 2003, 28-31. 216 [151] Pina Bergamo, Paolo D'Arco, Alfredo De Santis, et al., Security of public key cryptosys- tems based on Chebyshev polynomials, http://citebase.eprints.org, 2004. [152] D Xiao, X Liao, G Tang, Chuandong Li. Using Chebyshev chaotic map to construct in…nite length hash chains, Circuits and Systems, 1 (2004) 11-12. [153] Xiao Di Liao Xiaofeng Wong K.W. An e¢ cient entire chaos-based scheme for deniable authentication. Chaos, Solitons and Fractals, 23 (2005) 1327-1331. [154] Kohda Tohru Fujisaki Hirohi. Jacobian elliptic Chebyshev rational maps, Physica D 148 (2001) 242-254. 0.5000 0.5313 0.4609 0.5234 0.4688 0.5391 0.5000 0.4531 0.5469 0.5000 0.4922 0.5391 0.5000 0.4453 0.4609 0.5078 0.5000 0.4688

0.5000 0.4453 0.5469 0.5156 0.5156 0.4688 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111 112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127 128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143 144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159 160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175 176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191 192 193 194 195 196 197 198 199 201 202 203 206 207 209 214 215 217