
بسم الله الرحمن الرحيم

Algebraic and Chaotic Schemes to Synthesis S-boxes and their Applications in Multimedia Security

By

Sajjad Shaukat Jamal

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2018

Algebraic and Chaotic Schemes to Synthesis S-boxes and their Applications in Multimedia Security

By

Sajjad Shaukat Jamal

Supervised

By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2018

Algebraic and Chaotic Schemes to Synthesis S-boxes and their Applications in Multimedia Security

A Thesis Submitted to the Department of Mathematics,
Quaid-i-Azam University, Islamabad, in the partial fulfillment of
the requirement for the degree of

Doctorate of Philosophy

in

Mathematics

By

Sajjad Shaukat Jamal

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2018

Author's Declaration

I **Sajjad Shaukat Jamal** hereby state that my PhD thesis titled **Algebraic and Chaotic Schemes to Synthesis S-boxes and their Applications in Multimedia Security** is my own work and has not been submitted previously by me for taking any degree from the Quaid-I-Azam University Islamabad, Pakistan or anywhere else in the country/world.

At any time if my statement is found to be incorrect even after my graduate the university has the right to withdraw my PhD degree.

Name of Student: **Sajjad Shaukat Jamal**

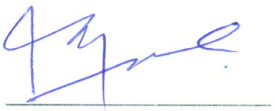
15-08-2018

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Algebraic and Chaotic Schemes to Synthesis S-Boxes and their Applications in Multimedia Security**" is solely my research work with no significant contribution from any other person. Small contribution/help wherever taken has been duly acknowledged and that complete thesis has been written by me.

I understand the zero tolerance policy of the HEC and **Quaid-i-Azam University** towards plagiarism. Therefore, I as an Author of the above titled thesis declare that no portion of my thesis has been plagiarized and any material used as reference is properly referred/cited.

I undertake that if I am found guilty of any formal plagiarism in the above titled thesis even afterward of PhD degree, the University reserves the rights to withdraw/revoke my PhD degree and that HEC and the University has the right to publish my name on the HEC/University Website on which names of students are placed who submitted plagiarized thesis.

Student/Author Signature: 

Name: **Sajjad Shaukat Jamal**

Dedicated

to

My

FAMILY

Acknowledgment

All praise for Almighty **Allah**, the Creator and the Merciful Lord, who guides me in darkness, helps me in difficulties and enables me to reach the ultimate stage with courage. My deepest gratitude to Prophet Mohammad (PBUH) and Ahyl e bait Salam ullah alhe.

I express the deepest gratitude to my respected supervisor **Prof. Dr. Tariq Shah** for his guidance, constant encouragement and suggestions throughout my research work. In short, his tireless work and unique way of research cannot be expressed in words. I am also thankful to the respected Chairman, Department of Mathematics, **Prof. Dr. Tasawar Hayat** for his support and guidance.

I wish to express my heartiest thanks and gratitude to my parents Mr. and Mrs. **Shaukat Hussain**, the ones who can never ever be thanked enough for the overwhelming love, kindness and care they bestow upon me. I am extremely thankful to my brother **Asif Raza** and Sisters **Shazia Shaukat**, **Asia Shaukat**, **Uzma Shaukat and Mehwish Asif.**

I would also like to express my gratitude to my brother in law **Qasim Qadeer**, **Mohammad Ayub** and **Waseem Tabassum**. Special Thanks to my **wife**, **Saima Jamal**, my lovely kids **Ali Raza**, **Wali Raza**, **Shane Shaukat** and **Hussain Shaukat.**

I would like to express my gratitude to all the respected teachers. They are all those people who made me what I am today, they polished me at different stages of my life and taught me whatever I am today.

I enact my heartiest and deepest thanks **to Dr. Iqtadar Hussain**, **Dr. Amir Anees**, **Dr. Attaullah, Mohammad Usman and Dr. Shabieh Farwa** for their brilliant ideas and important contribution in refining my research work. Their professional guidance has nourished my skills and I will always remain thankful to them. I gratefully acknowledge my seniors, my friends **Mohammad Nasir** and **Saad Faisal**.

I am also grateful to the administrative staff of mathematics department for their support at every time.

Sajjad Shaukat Jamal

15-08-2018

Abstract

Rapidly increasing use of international networking offers various new openings for the design and demonstration in the form of digital data. Easy availability and access to digital contents like electronic advertising, video, audio, digital repositories, electronic libraries, web designing etc. arise many security concerns. In this era, digital images are counted as one of the major communication sources as there is excessive application of multimedia knowledge and techniques. Generally, multimedia security is number of methods or techniques which ensures the security of multimedia data. For this reason, many researchers initiated working in developing different security techniques. Although there are certain methods for data security, but lot of improvement is required to guarantee the data security.

The strength of substitution box ensures the strength of block ciphers which have very important role in symmetric key cryptography. The main purpose of Substitution box is to create confusion, secure the original data from cryptanalysis and hide it in cipher text. It is noticed that mostly substitution boxes are constructed on Galois field. The other algebraic structures like groups, finite commutative ring can also be utilized for the construction of substitution box.

The methodologies for two multimedia security techniques i.e., for cryptography and steganography are different but they both are used for information hiding. In cryptography, data is transformed into an unintelligible arrangement called cipher text which is decrypted by receiver end into plaintext. On the other hand, steganography is an art of embedding surreptitious material into an unsuspicious carrier.

Another multimedia security technique is watermarking. Watermarking provides copyright protection of digital content. Copyright violations and plagiarism indicate that current copyright rules are vulnerable to be used for the digital data transfer on Internet. Keeping in view, the importance of copyright protection of digital contents, robustness of watermarking techniques, we in this thesis, initiated working for the construction of algebraic and chaotic high nonlinearity substitution boxes which has strong cryptographic properties.

These Substitution boxes are then utilized in the field of multimedia security specifically in watermarking and steganography (spatial and frequency domain) techniques. The basic purpose is to enhance the security and robustness against malicious attacks.

The first construction of substitution box depends on the action of a projective general linear group over the set of units of the finite commutative ring. The strength of substitution box and ability to create confusion is assessed with different analyses and equated with well-known substitution boxes.

In the next step, we suggest that the choice of the background irreducible polynomial, used for the construction of the Galois field $GF(2^8)$ has a deep influence on the highly desirable features on an Substitution box. We therefore propose that the performance of a substitution box is not just depending on the nature of the bijective Boolean function, however, it is affected by the degree 8 irreducible polynomial $\mu(x)$ as well, which generates the maximal ideal of the principal ideal domain $F_2[x]$. A unique nonlinear combination of two chaotic maps give a chaotic Tent-Sine system. This arrangement of chaotic maps shows brilliant complex chaotic properties. The chaotic range of Tent-Sine system is increased throughout the domain and the output sequences are distributed uniformly. We propose a chaotic substitution box with the help of this chaotic map. This Substitution box is capable of providing confusion ability by

achieving the substitution operation. This Substitution box is helpful against linear and differential attacks.

After that, the chaotic logistic map is employed for locating embedding positions of chaotic watermark generation and a novel watermarking scheme is proposed. Simulation results reveal that the proposed technique is feasible and watermarks are indiscernible.

In the next two frequency domain watermarking techniques, chaotic and algebraic substitution boxes are used. In the first case, the system of non-linear ordinary differential equations which defines a continuous-time dynamical system is used to construct chaotic box. In the second case, the algebraic box which develops one-one correspondence between the multiplicative group of units of the local ring $\mathbb{Z}_{512}$ and the Galois field $\boldsymbol{F}_{256}$. is used. The watermark is substituted with substitution boxes and then embedded into host image which give additional security to our proposed techniques.

For application of substitution box in digital steganography, we engage a specific high nonlinearity Substitution box along with some chaotic systems, possessing enhanced chaotic range, to embed information in the least significant bits of the host image. At the end, we have proposed a high capacity and robust steganographic algorithm based on an effective application of chaos and substitution box. The speciality of the proposed method lies, on one hand, in the process of embedding secret information using some stronger chaotic systems with enhanced chaotic range. While, on the other, high embedding-capacity level and robustness is attained due to the combination of the spatial domain steganography approach along with the frequency domain transform.

Contents

Chapter 1

Introduction and Basic Definitions

The 1st chapter of this thesis has two detailed parts. In the 1st part we represented the introduction, objective and layout of the thesis. The idea of multimedia contents and their security is explained to understand the term multimedia security. A brief description and difference between different information hiding techniques and typical functions are thoroughly discussed. As far as 2nd portion of this thesis is concerned, the basic definitions and theorems are given for better understanding of the later work done in this thesis.

1.1. Introduction

The initiation of the international networking and its effectiveness provide various new opportunities for the design and presentation in the form of digital material. Some of the applications of this digital contents are electronic advertising, video, audio, digital repositories, electronic libraries, web designing and much more. But this easy access to digital content through internet arises the issue of information security. In the recent past, it was quite impossible to side step cracking of original data. This security lapse attracts modern researchers to counterfeit challenges by the express propagation of digital media. Over the last few decades, a lot of researchers worked to develop different methods to secure information integrity, anonymity, authenticity, and confidentiality.

Multimedia security techniques provide integrity of the network, temper proofing, content authentication, copyright protection and broadcast monitoring and also ensure robustness against

any attempt to modify digital substances [1]. Digital watermarking and steganography may shield information, hide secrets, or are used as basic content in digital rights management techniques. We can be categorized multimedia security techniques into three major parts namely: cryptography, steganography and watermarking. The first two types may be considered as information hiding techniques. Initially, we discuss cryptography due to its foundation over Boolean algebra and then rest of two multimedia security techniques will be discussed in detail.

Cryptography provides tools for secure communication of information in the presence of different opponents. It is the science which constructs different algorithms and procedures that avoid any unauthorized use of data. Current cryptography depends on mathematics, electrical engineering and computer science. It covers the three vital areas such as integrity, confidentiality and authentication. The basic purpose of confidentiality is to hide information from whom it was unintended. Integrity ensures that the data cannot be changed from transmitting to receiving end. The transmitter and receiver can confirm the identity of each other with the help of authentication. The encryption and unscrambling of data are recognized as an action in cryptography. Encryption is the process which converts the plaintext or readable information into cipher text or meaningless form. On contrary decryption takes ciphertext as an input and provide the plain text by applying the reverse instructions. The process of enciphering mainly depends on the strong algorithm and key distribution. A cryptosystem is a combination of a finite number of plaintexts, ciphertexts, finite possible keys and the set of instructions for encryption and decryption. Cryptosystems can further be classified into two types which are symmetric and asymmetric cryptosystems. In symmetric cryptosystems, a message is encrypted and decrypted with alike key whereas in asymmetric cryptosystems, public key and the private key are used for encryption and decryption

process respectively. The well-known examples of symmetric key cryptography are block ciphers (blocks of data) and stream ciphers (individual characters).

For security prospective, public key cryptography is considered as more secure as compared to symmetric key cryptography since it permits to convey in a protected way irrespective of no common keys. Shannon [2] gave the concept of confusion and diffusion to attain security in different cryptosystems. The mind-boggling connection between the key and each binary bit of the ciphertext is obtained through confusion. In diffusion, half of the bits in the ciphertext must be changed while changing a single bit of the plaintext.

By keeping all the parameters for strong cryptosystems, it is required that there must be some functions that have characteristics of creating confusion and diffusion to enhance the security level. For this reason, there is a need for functions which hold the above-mentioned properties. It is observed that Boolean functions generate confusion and diffusion which is required for a strong cryptosystem.

Substitution boxes (S-boxes) and Boolean functions are important components of modern cryptosystems. The function quantity is used to link both S-boxes and Boolean functions. In a Boolean function, a single input bit results as a single output bit whereas S-box consists of different output Boolean functions. In block ciphers, the only nonlinear component is S-box which is responsible for confusion.

Normally, Boolean functions are used in the stream ciphers for the construction of secret key stream. In Stream ciphers, single keystream is obtained by joining all the inputs which are in the form of linear feedback shifts registers. In addition to this, the properties of Boolean functions oppose any kind of attacks to secure keystream.

In advanced encryption standard (AES), the S-box produces confusion to hide the plain text [3]. In May 2002, AES is officially accepted by the U.S. government as the Federal Information Processing Standard (FIPS). AES algorithm [3] depends on following steps: Round key addition, Byte Substitution, Shift Row and Mix Column, but the most influential of all these is the byte-substitution step. This step relies on a S-box, which serves as the only nonlinear component in any substitution- permutation network (SPN). It is recognized fact that the S-box is the source to produce nonlinearity in symmetric key cryptography. For this reason, it is frequently used in substitution-permutation network. and in many algorithms for the synthesis of safer and more dependable S-boxes. Moreover, S-boxes can be applied in digital image encryption, watermarking and steganography [4]–[7]. This nonlinear part of substitution process produces confusion and ambiguity. The substitution process is defined as:

$$S: \mathbb{F}^m \rightarrow \mathbb{F}^m$$

S-box provides a technique of substituting different blocks of bits for a totally different set of output bits. It is significant to use secure S-boxes having exceptional encryption properties.

Although the methodologies used in cryptography and steganography are totally different but the theme of both the information hiding techniques is similar, i.e., to obscure the information data. In order to avoid information leakage, many techniques are proposed in steganography and cryptography. It is worth mentioning that cryptography basically deals with changing the information into dummy data, for secure communication as discussed in detail. But steganography is a technique of embedding surreptitious material into an unsuspicious carrier. It is the science that ensures secure communication. The basic theme is to hide the secret information in a carrier. It can be intertwined with two further kinds of security named as cryptography and watermarking.

Plagiarism of copyright contents indicates that present copyright rules are inappropriate for handling digital data on the internet. This violation of copyright laws provides a platform for new protection mechanism of data. Watermarks can be seen on banknotes, passports, stamps and for other security papers. Digital watermarking is an extension lead to ensure the security of digital contents. It is observed that, digital watermarking is counted as one of the top techniques to avoid unlawful replication, altering and restructuring of multimedia data. Due to encryption of multimedia data, an invader has no access to the digital contents without a decryption key. But after decryption, this data can be copied and illegitimately distributed. The main features of digital watermarking are copyright protection, data authentication, content identification and covert communication. A design of bits embedding into audio, digital image and in any video that ascertains the copyright information of the file is named as digital watermarking. The watermark cannot be identified and manipulated easily if it is spread all over the file. This watermark detects the copyright information. The watermark image is noticeably smaller in the size as compared to the host image. that is the difference of size between watermark image and host image should be one-sixteenth [8].

Since the early nineties, the use of chaos theory has been promoted in many fields like physics, biology, engineering, and weather forecasting. The property of creating perplexity and confusion is the central feature of chaotic systems and this is valuable in the study of cryptography. The accessibility/inaccessibility of the initial values describes the certainty/uncertainty of the chaotic system. This nonlinear behaviour of the chaotic system ensures the secure communication through an insecure communication path by creating randomness and perplexity in the plain text. Diffusion is generally developed by the random application of non-linear dynamical structures. A minor alteration in the initial values describes an entirely different behavior of the chaotic structures

which indicate their sensitivity to initial conditions. The idea of using chaos theory for safe communication of data which attracted scholars of a different realm of life to develop chaos-based secure communication theory [2]. The most promising feature in developing novel cryptosystems with the help of chaos theory is their sensitivity to initial conditions.

In this thesis, construction of algebraic and chaotic S-boxes is presented. These S-boxes are then utilized in the field of multimedia security specifically in watermarking and steganography (spatial and frequency domain) methods. The basic purpose is to improve the security and robustness against different attacks.

1.2. Contribution of This Thesis

The foremost objectives of this thesis are discussed in detail as follows.

1- To obtain the strong algebraic and chaotic S-boxes for enhancing the security level of different cryptosystems. In this thesis, algebraic S-box is obtained by using the finite local ring. Here, the selection of the contextual irreducible polynomial, applied for the construction of the Galois field $GF\ (2^8)$, has a deep impact on an S-box.

2- Utilizing two chaotic systems to enhance the chaotic range. This helps to design some novel schemes for construction of chaotic S-boxes. It helps to construct different ciphers for watermarking and steganography.

3- To develop new techniques for watermarking and steganography by using S-boxes constructed in 1 and 2. Similarly, to apply outcomes from 1 and 2 as a substitution process in the proposal of different ciphers for multimedia techniques. The theme is to increase the security level of current multimedia techniques by utilizing the findings and information obtained from different S-boxes constructions. It also motivates to design new ciphers for watermarking and steganography. At this stage, we try to develop few new securities

conspires in this proposal for the application to this errand, notwithstanding trialing known systems through examination.

1.3. Thesis Layout

In this thesis, nine chapters are included, however chapter 2 to chapter 4 are for the construction of S-boxes and chapter 5 to chapter 8 are based on the application of S-boxes in multimedia security. The detail description of each chapter is as follows:

- Introduction and Basic definitions are given in the 1st chapter. The detailed description of Boolean function and theory of S-box are also the part of chapter 1.
- In 2nd chapter, a group action method for structure of strong S-box is presented. In this chapter, S-box is obtained by applying action of a projective general linear group over the set of units of the finite commutative ring. This S-box is cryptographically strong which can be used in multimedia security and data hiding techniques.
- In chapter 3, we suggest that the selection of the background irreducible polynomial, used for the construction of the Galois field $GF\ (2^8)$, has a deep impact on the greatly required features on an S-box. We, therefore, propose that the efficiency of an S-box is not just depending on the nature of the bijective Boolean function, however, it is affected by the degree 8 irreducible polynomial as well, which produces the maximal ideal of the principal ideal domain $\mathbb{F}_2[X]$.
- In chapter 4, the chaotic behavior of the tent-sine map is discussed and a new method to construct different S-Boxes is proposed. The combination of two seed maps give a chaotic map (tent-sine map) which has increased chaotic range and uniformity.

- In chapter 5, the chaotic S-box is designed with the help of system of non-linear ordinary differential equations. This system provides a continuous-time dynamical system that has fractal features of the attractor. The addition of chaos in frequency domain ensures robustness. In frequency domain watermarking, low or middle frequencies are used for embedding watermark so the alterations can be observed throughout the image.
- The algebraic structure of finite local ring is used to synthesize S-box in chapter 6. We use this S-box in a watermarking scheme to make our technique more confusing and secure to provide more support in copyrights protection strategies. The proposed non-blind digital watermarking technique deals with the application of discrete cosine transform (DCT) in the frequency domain which is comparatively more robust than spatial domain techniques.
- Chapter 7 introduces a new scheme for digital steganography in the spatial domain. In this approach, we engage a specific high-nonlinearity S-box along with some chaotic systems, possessing enhanced chaotic range, to insert data in the least significant bits of the original image.
- Chapter 8 presents a high capacity and robust steganographic algorithm based on an effective application of chaos and S-box. The specialty of the proposed method lies, on one hand, in the process of embedding secret information using some stronger chaotic systems with enhanced chaotic range. While, on the other, high embedding-capacity level is attained due to the combination of the spatial domain steganography approach along with the frequency domain technique. For frequency domain, the combination of discrete wavelet transform (DWT) and discrete cosine transform (DCT) is used.
- We have ended this thesis with conclusions and future suggestions.

1.4. Review of S-box Theory

The knowledge of Boolean function and S-box is mandatory for better understanding of this thesis work. It helps to recognize the importance of this research and correlation between this thesis work and study of cryptography. In this chapter, basic concepts, formulae and theorems are given as required contextual.

1.4.1. Boolean Functions

The Boolean function theory is wide-ranging area in itself. We presented a comprehensive classification which is necessary for understanding of this thesis. The cryptographic properties and their inter-relationship is well-defined and discussed in detail.

1.4.2. Properties of Boolean functions for Cryptography

In this section, some basic definitions on Boolean functions are given. Let $GF\ (2^k)$ be the vector space of dimension k over the two-element Galois field *GF(2)*. $GF\ (2^k)$ contains 2^k vectors given in a binary sequence of length k. This vector space has scalar product. $<.,.>: GF\ (2^k) \times GF\ (2^k) \rightarrow GF(2)$

$$< a, b >= \oplus_{j=1}^{q} a_j . b_j, \tag{1.1}$$

where the multiplication and addition $\oplus$ are over $GF(2)$.

Definition 1 [9] A linear Boolean function can be defined as

$$L_\beta(y) = \beta_1 y_1 \oplus \beta_2 y_2 \oplus \ldots \oplus \beta_1 \mathrm{y}_1 \tag{1.2}$$

where $\beta_1 \mathrm{y}_1$ represents the bitwise AND of the $\mathrm{j}-\mathrm{th}$ bits of β, y and $\oplus$ shows bitwise XOR.

Definition 2 [10] Affine Boolean functions is the set of linear Boolean function along with their complements.

$$A_{\beta,c} = L_{\beta}(y) \oplus c, \tag{1.3}$$

where $y \in GF(2^k)$. An affine (linear) sequence is the sequence of affine (linear) functions.

Definition 3 [9] In the form of set, all single valued Boolean function can be given as

$$G_p = \{g | g: GF(2^k) \to GF(2)\}. \tag{1.4}$$

For the space G_k, the subset of all affine and for the space $GF(2^k)$ linear Boolean functions can be given by eq. (1.5) and (1.6) respectively.

$$A_p = \{\gamma | \gamma: \text{is affine and } \gamma \in G_p\}. \tag{1.5}$$

$$L_P = \{\beta | \beta: \text{is linear and } \beta \in G_p\}. \tag{1.6}$$

Remark The set of all affine functions is obtained with the help of linear functions and their negations.

Definition 4 [11] In Boolean function $h: GF(2^k) \to GF(2)$; the Hamming-weight is the total count of 1's in the truth table of h.

Definition 5 [10] The Hamming-distance between two Boolean functions $j, h: GF(2^k) \to GF(2)$; is the total number of arguments where j and h differ, that is

$$d(j,h) = \#\{z \in GF(2^k) / j(z) \neq h(z) \tag{1.7}$$

Or it can be defined as the number of 1's in the truth table of $j \oplus h$. It is established fact that Hamming-distance d is the metric on$GF(2^k)$. So, Hamming-distance can be defined with the help of Hamming weight is $d(j,h) = wt(j \oplus h)$. The $d(k,h)$ equals to the numbers of the values that are required to turn j to h. So, the d(j; h) is zero if and only if $j = h$:

Definition 6 [12] For Boolean function h, the support of h is given as

$$\mathbf{supp}(h) = \#\{z \in GF(2^k) | h(z) = 1 \tag{1.8}$$

Moreover, Hamming-weight can be expressed with the help of Hamming-distance and the support of a Boolean function:

$$\mathbf{wt}(h) = d(h, 0) = \mathbf{supp}(h). \tag{1.9}$$

Definition 7 [12] A $(0,1) - \text{sequence}$ $((1,-1) - \text{sequence})$ holds an equal value of zeros and one (ones and minus ones) then it is named as balanced sequence. If the sequences of function are balanced, then the function is balanced function. $\mathbf{wt}(h) = 2^{k-1}$.

Definition 8 [10] In Boolean function h, the imbalance of function is the difference between the number of inputs that maps to 0 and the number of inputs that maps to 1 divided by 2 The imbalance ranges from -2^k to 2^k. It is denoted by **Imb**(h)

$$\mathbf{Imb}(h) = 1/2\,(\#\{b|h(b) = 0 - \#\{b|h(b) = 1\} \tag{1.10}$$

If the value of imbalance is 0, then that Boolean function is balanced.

Definition 9 [12] The autocorrelation function with a shift $b \in GF\left(2^k\right)$ is denoted by $\hat{\gamma}_h(b)$. It is defined as

$$\hat{\gamma}_h(b) = \sum_{z \in GF\,(2^p)} \hat{h}(z)\,.\,\hat{h}(z \oplus b). \tag{1.11}$$

Definition 10 [10] Let h be a function defined on $GF\left(2^k\right)$. Let $b \in GF\left(2^k\right)$ is named as linear structure of $b \in GF\left(2^k\right)$ if

$$\hat{\gamma}_{\hat{h}}(b) = 2^k; \tag{1.12}$$

i.e., if $\hat{h}(z).\hat{h}(z \oplus b)$ is constant.

A linear subspace of $GF\left(2^k\right)$ is formed with the set of all linear structures of a function h. The dimension provides a measure of linearity. This measure is upper bounded by 2^k. The bound is attainable by the all zero vector in $GF\left(2^k\right)$. A nonzero linear structure is cryptographically undesirable.

Definition 11 [12] To calculate correlation between two Boolean functions j and h, we have

$$C(h,k) = 2\,Pr\big(j(z) = h(z)\big) - 1,$$

$$= 2\left[\frac{2^k - d(j,h)}{2^k}\right] - 1,$$

$$= \left[\frac{2^{k+1} - 2d(j,h)}{2^k}\right] - 1,$$

$$= 1 - \left[\frac{2d(j,h)}{2^{k-1}}\right] \qquad (1.13).$$

The value of correlation is a rational number in the interval $[-1, 1]$. If the Hamming distance between two functions is zero, then the value of correlation is 1.and if the Hamming distance between two functions is equal to 2^k, the result of correlation is -1.

Definition 12 [9] The algebraic degree can be defined as the number of variables in highest order monomial with zero coefficients.

Definition 13 [10] The n-variables Boolean function is algebraic normal form (ANF) which can be given as follows:

$$h(x) = b_0 \oplus b_0 z_0 \oplus b_0 z_0 z_1 \oplus b_{012\ldots.n-1} z_0 z_1 \ldots\ldots z_{n-1,} \qquad (1.14)$$

where the coefficients $b \in GF\left(2^k\right)$ generate the values of the truth table of the ANF of h(z).

Definition 14 [9] If ANF contains all n variables of a Boolean function h(z), then it is named as non degenerate function. On contrary, if h(z) does not hold every variable in its ANF then the function is degenerate.

Definition 15 [10] The algebraic degree of a Boolean function and the algebraic complexity of the function are directly proportional to each other. Moreover, if the value of degree of a function is on higher side, the greater will be its algebraic complexity.

Definition 16 [10] The algebraic degree of a Boolean function $h(z)$ is the total count of variables in the highest product term of the function's ANF having a non-zero coefficient. It is denoted by deg(h).

Definition 17 [12] For Boolean function, the nonlinearity is represented by N_h and is defined as follows

$$N_h = d(h, A_n) = \min_{\beta \in A_n} d(h, \beta) \tag{1.15}$$

The nonlinearity of an affine function is zero. By definition, for non-affine Boolean function h, the value of nonlinearity is $N_h > 0$. For strong cryptosystem, the high nonlinearity ensures the ability of resistance of any cryptographic system against linear cryptanalysis discussed in [13].

Definition 18 [11] The Walsh transform of a function h on $GF(2^k)$is a mapping Ω: $GF(2^k) \to \mathbb{R}$ given as

$$\Omega(h)(v) = \sum_{z \in GF(2^k)} h(z)\,(-1)^{<v,z>}, \tag{1.16}$$

where $< v, z >$ is the canonical scalar product. The Walsh spectrum of h is the list of 2^k Walsh coefficients as given by Eq. (1.16) as varied.

Definition 19 [14] A Boolean function h in n variables is said to be correlation immune of order m, $1 \leq m \leq n$, if its values are statistically independent of any subset of input variables.

Definition 20 [11] If an average half of the output bits changes due to a single input bit is complemented A function h: $GF(2^k) \to GF(2^k)$ observes the avalanche effect i.e.

$$\frac{1}{2^k} \sum_{v \in GF(2^k)} \mathbf{wt}(g(z^i) - g(z)) = \frac{q}{2}, \text{for all } i = 1,2, \ldots . p. \tag{1.17}$$

Definition 21 [10] A function h: $GF(2^k) \to GF(2^l)$ of k input bits into l output bits is complete, if every single output bit depends on every input bits.

$$\forall\, i = 1, 2, \ldots\ldots k,\ j = 1;\ 2, \ldots\ldots, l, \exists\, z \in GF(2)^k \text{ with } \left(h\left(z^i\right)\right)_j \neq \left(h(z)\right)_j. \tag{1.18}$$

If every ciphertext bit depends on all of the output bits it means cryptographic transformation is complete. Complete cryptographic transformations having complete inverses described as being two-way complete, and if the inverse is not complete then that transformation is only one-way complete.

Definition 22 [11]Whenever a single input bit is complemented and output bit changes with a probability of $1/2$, then the function h: $GF\left(2^k\right) \rightarrow GF\left(2^l\right)$ holds the strict avalanche criterion. i.e.

$$\forall\, i = 1, 2, \ldots\ldots k,\ j = 1;\ 2, \ldots\ldots, l, \text{Prob}\left(h\left(z^i\right)\right)_j \neq \text{Prob}\left(h(z)\right)_j. = \frac{1}{2} \tag{1.19}$$

Definition 23 [12] The autocorrelation function of a Boolean function in k variables is given as

$$r_h(b) = \sum_{i=0}^{2^k-1} h(z_i) \oplus h(z_i \oplus b) \tag{1.20}$$

for all every $b \in GF\left(2^k\right)$.

The autocorrelation function is the summation over all the values of the directional derivatives every $h(z) \oplus g(x \oplus a)$ as z runs through $GF\left(2^k\right)$.

Bent Functions

In [15], Rothaus, introduced a specific class of Boolean functions showing unique features. These functions are named as bent functions. Due to their optimal distance to linear structures, bent functions are named as perfect nonlinear [16].It is observed that the existence of these functions depend on the space of even dimensional Boolean functions. On contrary, for odd dimensional space, Boolean functions are unable to fulfil the required criteria of bent function

.

It is obvious that the Walsh Hadamard spectrum is flat as two-valued Walsh Hadamard spectrum of a Boolean function consists of $\pm 2^{k/2}$ values. The bent function has nonlinearity which can be defined as $(2^k - 2^{k/2})/2$. As Parseval's Theorem hold, so this is the maximum possible nonlinearity for k-dimensional Boolean functions (where k is even). It indicates that there is maximum distance between bent function and linear structures. In addition to this, bent functions have no order of correlation immunity as there does not exist zero-valued entries in the Walsh Hadamard spectrum, bent functions do not show any order of correlation immunity.

For k-variable bent Boolean function (p even), the auto correlation vector is given as $\hat{r}(a) = \{2^k, 0,0, \dots ,0\}$. Here, all entries have value 0 except the first one which has value 2^k.

Even though bent functions display cryptographically optimal characteristics in the form of maximal non-linearity and perfect (minimal) autocorrelation, p-variable bent functions have a Hamming weight of $(2^{k-1} \pm 2^{k/2-1})$. It shows a bias from the balance of constant magnitude $2^{k/2-1}$, bent functions are never balanced. Furthermore, all n-variable bent functions have algebraic degree are cryptographically undesirable for bent functions to be of direct practical use

1.5. S-box Theory

In this section, we will discuss S-boxes (S-boxes). We added some elementary definitions of S-box theory and cryptographic properties to highlight the research work of this thesis.

1.5.1. Definition and Types of S-box

The natural progression of single output Boolean functions to multiple output Boolean functions is the basic feature of S-box. Various type of S-boxes depend upon the connection between the input and output bits. For the sake of better understanding, necessary S-box definitions along with some S-box types are given in detail.

S-box of $k \times l$ is a mapping from p input bits to q output bits, $S: GF(2^k) \times GF(2^l)$. For an $k \times l$ S-box, possible inputs and output are 2^k and 2^l respectively. It is easy to decompose output vector $S(x) = (s_1, s_2, \ldots, s_q)$ into q component functions $S_n: GF(2^k) \times GF(2)$, $i = 1,2, \ldots, q$. The look up table, an $k \times l$ S-box, S, is represented as a matrix of size $2^k \times l$, indexed as $S_{[n]}$ $0 \leq n \leq 2^k - 1$. S-boxes can be classified into three categories: Straight, compressed and expansion S-boxes. If each input entry of $k \times l$ S-box is mapped to a different output OR multiple inputs mapped to the similar output is counted as straight S-box. An injective and surjective $k \times l$ S-box is named as bijective S-box. In bijective S-box, every input maps to a different output value and all likely outputs are present in the S-box. The required condition for bijective S-boxes is $k = l$. They are also known as reversible as there exists a mapping for output distinct values to corresponding input values. This kind of S-box is used in Rijndael cipher.

In data encryption standard [DES] [17], a $k \times l$ compression S-box is used where the sufficient condition is $k > l$. In DES, for 6 input bits but the output for only 4 bits show that it gives back fewer bits as compared to input bits. On contrary with condition that $k < l$, $k \times l$ S-box gives out more bits as compared to input bits. In regular $k \times l$ S-box, all possible 2^l output appears an equal number of times. In addition to this, all possible output values appear 2^{k-l} times in the S-box. It is important to note that all single output Boolean functions including regular S-box (and their linear combinations) are balanced. For all regular S-boxes to be balanced, $k \geq l$ is the required condition. A $k \times l$ S box ($k \geq 2l$ *and* k *is even*) is named as bent provided that every linear combination of its constituent Boolean functions is also a bent function.

In compression and expansion S-boxes there is an issue of reversibility or decryption. In these both type of S-boxes, it is difficult to reverse the process as they alter the total number of bits. Moreover, they have a problem of loss of information, particularly in compression S-boxes. Due to the

complexities associated with compression or expansion S-boxes, straight S-boxes are more commonly used by researchers.

1.5.2. Cryptographic properties of S-boxes

While discussing the cryptographic properties of S-box, it is important to study the cryptographic properties of each component of Boolean functions and all the linear combinations of the component functions. This is explained in the upcoming S-box properties.

For balanced $k \times l$ S-box, it is necessary that its component Boolean functions and their linear combinations are balanced. With this property, an invader is unable to trivially approximate the function or the output.

In [18], Shannon explained that there is a complex relation between the ciphertext and the key material. This concept is named as confusion. In cipher system, confusion is attained by using the nonlinear components. For this reason, S-boxes become the major nonlinear component of any cryptographic cipher systems. The nonlinearity of an $k \times l$ S-box is defined in the later definition.

Definition 24 [19] The minimum nonlinearity of every Boolean function output component and their linear combination is defined as nonlinearity of a $k \times l$ S-box S. It is denoted by $N_{S_{k,l}}$. Let u_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$. Mathematically, the nonlinearity of S can be written as:

$$N_{S_{k,l}} = \min_{u}\{N_{S_{k,l}}(u_j)\} \quad (j = 1, \dots, 2^l - 1) \tag{1.21}$$

where $S = (s_1, s_2, \dots, s_l)$ and s_n $(n = 1, \dots, l)$ are all Boolean functions.

As p and q increases, computationally it is very difficult to calculate the nonlinearity of a $k \times l$ S box. In the next section, we discuss few cryptanalytic attacks to highlight the importance of nonlinearity for the security of cipher systems.

In order to resist a cryptanalytic attack, the algebraic degree of Boolean function and $k \times l$ S-box must be high. It is named as low order approximation [13]. The degree of S-box is given below:

Definition 25 Let $S = (s_1, s_2, \dots, s_l)$ be a $k \times l$ S-box and s_n $(n = 1, \dots, l)$ are all Boolean functions. Let u_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$. The algebraic degree of S which is denoted by deg($S_{k,l}$) can be written as:

$$\deg(S_{k,l}) = \min_{u}\{\deg(u_j)\} \quad \left(j = 1, \dots, 2^l - 1\right) \tag{1.22}$$

In [2], Shannon proposed the idea of diffusion. Diffusion is a method in which data redundancy in a cipher is spread throughout the data to minimize the probability of its statistical structure. The avalanche characteristics of a cipher system are linked with diffusion. These characteristics are achieved by using cipher components which indicate better avalanche characteristics. Following definitions help to measure these characteristics of $k \times l$ S-boxes.

Definition 26 [10] Let $S = (s_1, s_2, \dots, s_l)$ be a $k \times l$ S-box and s_n $(n = 1, \dots, l)$ are all Boolean functions. Let u_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$ having autocorrelation functions as $\ddot{Y}_{u_j}(a)$. Mathematically, maximum absolute autocorrelation value of S can be defined as:

$$|_{AC_{S_{k,l}}}|_{max} = \max_{u} |\ddot{Y}_{u_j}(a)| \tag{1.23}$$

With $a \in \{1, \dots, 2^k - 1\}$ and $(j = 1, \dots \dots\ 2^l - 1)$

Definition 27 [20] Let $S = (s_1, s_2, \dots, s_l)$ be a $k \times l$ S-box and s_n $(n = 1, \dots, l)$ are all Boolean functions. Letu_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$. If every u_j $(j = 1, \dots, 2^l - 1)$ satisfies strict avalanche criterion (SAC) then S is said to satisfy SAC.

Definition 28 [12] Let $S = (s_1, s_2, \dots, s_l)$ be a $k \times l$ S-box and s_n $(n = 1, \dots, l)$ are all Boolean functions. Let u_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$. If every u_j $(j = 1, \dots, 2^l - 1)$ satisfies propagation criteria of order q denoted as PC(q), then S is said to satisfy PC(q).

Definition 29 [21] Let $S = (s_1, s_2, \dots, s_l)$ be a $k \times l$ S-box and s_n $(n = 1, \dots, l)$ are all Boolean functions. Let u_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$. If every l_k $(j = 1, \dots, 2^l - 1)$ satisfies correlation immunity denoted by CI(z), then S is said to be CI(z).

Definition 30 [12] Let $S = (s_1, s_2, \dots, s_l)$ be a $k \times l$ S-box and s_n $(n = 1, \dots, l)$ are all Boolean functions. Let u_j be the set of all linear combinations of s_n $(n = 1, \dots, l)$. If every l_k $(k = 1, \dots, 2^l - 1)$ are z-resilient, then S is said to be z-resilient Boolean functions.

Bit Independent Criterion

In 1985, Webster and Tavares introduced bit independent criterion (BIC) for better understanding of S-boxes [22]. This criterion helps to signify the confusion function. If a single input bit *r* is reversed in BIC, the output bits *m* and *n* must be altered independently for all *i*, *j* and $k \in (1,2, \dots, n)$. The correlation coefficient between m^{th} and n^{th} output bits is required to understand the concept of BIC. The bit independence effects on the m^{th} and n^{th} output bits by changing the r^{th} input bit can be denoted as B^{e_q}:

$$BIC(b_m, b_n) = \max_{1 \le r \le n} |\, \mathbf{corr}\,(b_m{}^{e_r}, b_n{}^{e_r})|. \tag{1.24}$$

For S-box function $g: GF(2^k) \rightarrow GF(2^l)$, the BIC can be defined as:

$$BIC(g) = \max_{\substack{1 \le m,n \le n \\ m \ne n}} \mathbf{BIC}\,(b_m, b_n\,). \tag{1.25}$$

1.5.3. Linear and Differential Cryptanalysis of S-boxes

In 1993, M. Matsui presented the linear cryptanalysis as a theoretical attack on Data Encryption Standard (DES). Later, this linear cryptanalysis is successfully used for cryptanalysis of DES. This cryptanalysis searches "high probability" existences of linear expressions which include plaintext ciphertext, and subkey bits [23]. To determine the value of key bits, different plaintext ciphertext pairs are used in this cryptanalysis.

In 1990, E. Biham and A. Shamir introduced differential cryptanalysis as an attack on DES. In [24], Heys defines the differential analysis as: "Differential cryptanalysis exploits the high probability of certain occurrences of plaintext differences and differences into the last round of the cipher". Linear cryptanalysis is a known plaintext attack whereas differential cryptanalysis is a chosen plaintext attack [25].

Definition 31 [11] The size of XOR table for a vector Boolean function $h: GF(2^k) \rightarrow GF(k)$ is $2^k \times 2^k$. The input vectors in the XOR table for the position (r, m) is given by:

$$|\{P \in GF(2^k): h(P) \oplus h(P + \tau_r) = \tau_m\}| \tag{1.26}$$

for $0 \leq r, m \leq 2^k - 1$. The n-bit binary representation of indices r and m is represented by τ_r and τ_m. The pair (r, m) is an input/output XOR pair, h is the cryptographic function of the S-box and P is the input vector. The S-boxes having low XOR table entries are considered as secured cipher against differential cryptanalysis. In each row, the sum of XOR table entries are equal to 2^k which is equal to a number of total input vector pairs.

Definition 32 [9] The linear approximation table for a Boolean function $h: GF(2^k) \rightarrow GF(2^l)$ is given by

$$LAT_h(c, d) = \#\{y \in GF(2^k) | c.y = d.h(y)\} - 2^{k-1} \tag{1.27}$$

where $c \in GF(2^k)$, $d \in GF(2^l)\backslash\{0\}$.

Lemma [10] For a given vector Boolean function h: $GF(2^k) \to GF(2^l)$ it is defined the linear approximation table which elements are

$$LAT_h(c,d) = 2^k - 1 - d(c.y, d.h), \tag{1.28}$$

where $c \in GF(2^k)$, $d \in GF(2^l)\backslash\{0\}$.

Lemma [10] For a given vector Boolean function h: $GF(2^k) \to GF(2^l)$,

$$N_h = 2^{k-1} - \max_{c,d} |LAT_h(c,d)|, \tag{1.29}$$

where $c \in GF(2^k)$, $d \in GF(2^l)\backslash\{0\}$.

Definition 33 [12] For any given

$\Delta_z,\ \Delta_t, \Gamma_z,\ \Gamma_t \in GF(2^k)$, the linear and differential approximation probabilities for every vector Boolean function (S-box) can be given as:

$$LP^{S_r}(\Gamma_t \to \Gamma_z) = 2\left(\frac{\#\{z \in GF(2^k) | z\Gamma_z = S_r(z)\Gamma_t\}}{2^k}\right) \tag{1.30}$$

$$DP^{S_r}(\Delta_z \to \Delta_t) = \left(\frac{\#\{z \in GF(2^k) | S_r(z) \oplus S_r(z \oplus \Delta_z) = \Delta_z\}}{2^k}\right) \tag{1.31}$$

where, the bitwise product of z and Γ_z is $z\Gamma_z$ (denotes the parity (0 or 1).

Definition 34 [10] For vector Boolean function (S-boxes), the maximum linear and differential approximation probabilities can be defined as:

$$p = \max_i \max_{\Gamma_z, \Gamma_z} LP^{S_i}(\Gamma_z \to \Gamma_z) \tag{1.32}$$

$$q = \max_i \max_{\Gamma_z, \Gamma_z} DP^{S_i}(\Gamma_z \to \Gamma_z) \tag{1.33}$$

The introduction and basic preliminaries are presented in this chapter. In the next chapter, a novel technique for the construction of S-box based on algebraic structure of finite commutative ring is presented.

Chapter 2

Construction of S-box using finite commutative ring

In this chapter, the method to develop cryptographically strong S-box is presented which can be used in multimedia security and data hiding techniques. The algorithm of construction depends on the action of a projective general linear group over the set of units of the finite commutative ring. The strength of S-box and ability to create confusion is assessed with different available analyses. Moreover, the ability of resistance against malicious attacks is also evaluated. The S-box is examined by bit independent criterion, nonlinearity test, strict avalanche criterion, linear and differential approximation probability tests. This S-box is equated with well-recognized S-boxes such as AES [3], Gray [26], APA [27], S8 [28], prime of residue [29], Xyi [30] and Skipjack [31]. The comparison shows encouraging results about the quality of the proposed box. The majority logic criterion is also calculated to analyze the strength and its practical implementation.

2.1. Background

In symmetric key cryptography, block ciphers depends on the strength of S-box and hence these boxes play very important role. The main theme of S-box is to develop confusion, secure the original data from cryptanalysis and hide it in cipher text. In the literature, the construction of S-box is started by Shannon in Shannon theory and then in Fiestal cipher by Fiestal [2], [32]. The different analysis of the properties of S-box like scrambling and creating confusion in data suggests its vital role in encryption schemes and applications. The S-box evaluates the nonlinearity and efficiency of the cryptosystem. The S-boxes used in data encryption standard (DES), advanced

encryption standard (AES) and other designs provide alluring and remarkable properties which are applicable in multiple ciphers.

In an AES, the combination of permutation box and the key based data substitution provide the substitution-permutation network. Several layers of substitution-permutation combination give the cipher text with the application of multiple keys used in each round. The algebraic complexity and better cryptographic properties for encryption are observed in affine power affine (APA) [27]. Similarly, these properties are depicted in S8 AES and Gray S box [3], [28]. The Gray S-box ansd S8 AES S-box are the actions of binary Gray codes and symmetric group S8 and on AES S-box, respectively. In addition to this, Xyi S-box , Skipjack S-box, and Prime S box are also used in certain encryption techniques and best fit for data hiding [29], [31], [33]. The concept of Finite fields and their extensions provide the base of S-boxes as obvious from APA S-box, AES S-box, S8 S-box, Residue Prime S-box, , Skipjack S-box, Gray S-box and Xyi S-box [26], [34]. In the literature, Galois field (2^8) was used to construct S-box. The elements of Galois field were taken in typical ascending order [35], [36]. In our proposed technique, initially finite local ring $\mathbb{Z}_{512}$ is utilized for the structure of S-box. Furthermore, to increase the randomness, inverse map and composition of scalar and inverse map are used. Lastly, group action is applied in the form of linear fractional transformation (LFT) on the permuted elements of Galois field. In this new method, group action method using linear fractional transformation is used to construct S-box depending upon [37]. The algebraic construction is defined with group action of the projective general linear group over the set (group) of units of ring $\mathbb{Z}_{512}$ which is given by K. This group K have 256 unit elements of $\mathbb{Z}_{512}$ develops a bijection with $GF\ (2^8)$. It can be elaborated as:

$$g(2m+1) = \frac{tm+u}{vm+w}, \qquad 0 \leq m \leq 255 \tag{2.1}$$

where t, u, v and w belongs to Galois field which have 256 elements $GF(2^8)$. The elementary subject of the S-box is to scramble data values and produce confusion and perplexity which is used in the encryption scheme. The statistical analyses of S-box not only provide the strength but also give the usage of specific encryption application. As in this encryption procedure, the only nonlinear component is S-box so it is worth finding to notify the values of parameters of linear fractional transform and the nonlinearity manipulated in plaintext. The analyses of S-box are performed by using nonlinearity analysis and analyzing the change effect in output bits by giving a slight variation in input bits. For this, we use bit independent criterion (BIC) and strict avalanche criterion (SAC) [34]. Moreover, the volume of similarity is attained by using the probability of events [17], and these analyses can be done by performing linear and differential probability analysis. The majority logic criterion (MLC) proceeds the outcomes of different analyses and concludes the top-quality S-box with necessary properties [38].

2.2. Algebraic Structure of Proposed S-box

In the literature, algebraic techniques are being applied on the ascending sequence of Galois field having element 0-255. In this novel technique, the sequence is permuted with the help of inverse map and then by applying the composition of inverse and scalar map. Furthermore, the group action is applied to get the enhanced non-linearity of S-box. The work in [39] shows the comparison of previous techniques with proposed technique.

2.2.1. Algorithm for Proposed S-box

Here, the basic phases for evolving the algorithm of new S-box are given as:

A1. In the first step, consider the units from the ring of integers modulo 512 which is denoted by $U(\mathbb{Z}_{512})$.

$$K = U(\mathbb{Z}_{512}) = \{2\mathrm{m} + 1, 0 \leq \mathrm{n} \leq 255\} \tag{2.2}$$

where elements of K and 512 are relatively prime. The multiplicative inverses of elements of K are given in Table 1 using the map γ given in Eq. (2.3).

$$\gamma(y) = y^{-1} \tag{2.3}$$

Table 1: Multiplicative inverses of elements of K (subgroup of $U(\mathbb{Z}_{512})$)

1	171	205	439	57	419	197	239	241	27	317	423	41	19	53	479
481	395	429	407	25	131	421	207	209	251	29	391	9	243	277	447
449	107	141	375	505	355	133	175	177	475	253	359	489	467	501	415
417	331	365	343	473	67	357	143	145	187	477	327	457	179	213	383
385	43	77	311	441	291	69	111	113	411	189	295	425	403	437	351
353	267	301	279	409	3	293	79	81	123	413	263	393	115	149	319
321	491	13	247	377	227	5	47	49	347	125	231	361	339	373	287
289	203	237	215	345	451	229	15	17	59	349	199	329	51	85	255
257	427	461	183	313	163	453	495	497	283	61	167	297	275	309	223
225	139	173	151	281	387	165	463	465	507	285	135	265	499	21	19
193	363	397	119	249	99	389	431	433	219	509	103	233	211	245	159
161	75	109	87	217	323	101	399	401	443	221	71	201	435	469	127
129	299	333	55	185	35	325	367	369	155	445	39	169	147	181	95
97	11	45	23	153	259	37	335	337	379	157	7	137	371	405	63
65	235	269	503	121	483	261	303	305	91	381	487	105	83	117	31
33	459	493	471	89	195	485	271	273	375	93	455	73	307	205	511

A2. Similarly, we define ψ on K by the next equation:

$$\psi(y) = s\, y\, , where\ s \in K \tag{2.4}$$

The composition θ of the maps given in Eq. 2.3 and 2.4 will be

$$\theta = \gamma \circ \psi = s\, y^{-1} \tag{2.5}$$

For our understanding in calculation process, we take $s = 13$ and the result is given in Table 2

Table 2: 16×16 pseudo S-box constructed on a subgroup of $(\mathbb{Z}_{512})$

13	175	105	75	229	327	1	35	61	351	25	379	21	247	177	83
109	15	457	171	325	161	353	131	157	191	377	475	117	87	17	179
205	367	297	267	421	7	193	227	253	31	217	59	213	439	369	275
301	207	137	363	5	359	33	323	349	383	57	155	309	279	209	371
397	47	489	459	101	199	385	419	445	223	409	251	405	119	49	467
493	399	329	43	197	39	225	3	29	63	249	347	501	471	401	51
77	239	169	139	293	391	65	99	125	415	89	443	85	311	241	147
173	79	9	235	389	231	417	195	221	255	441	27	181	151	81	243
269	431	361	331	485	71	257	291	317	95	281	123	277	503	433	339
365	271	201	427	69	423	97	387	413	447	121	219	373	343	273	247
461	111	41	11	165	263	449	483	509	287	473	315	469	183	113	19
45	463	393	107	261	103	289	67	93	127	313	411	53	23	465	115
141	303	233	203	357	455	129	163	189	479	153	507	149	375	305	211
237	143	73	299	453	295	481	259	285	319	505	91	245	215	145	307
333	495	425	395	37	135	321	355	381	159	345	187	341	55	497	403
429	335	265	491	133	487	161	451	477	267	185	283	437	407	105	499

A3. In the last step, we define an action of the Projective general linear group on the set (group) K which is the main theme of this article. This group action of $PGL(2, K)$ on the set K is accomplished by linear fractional transformation. This procedure can be explained as:

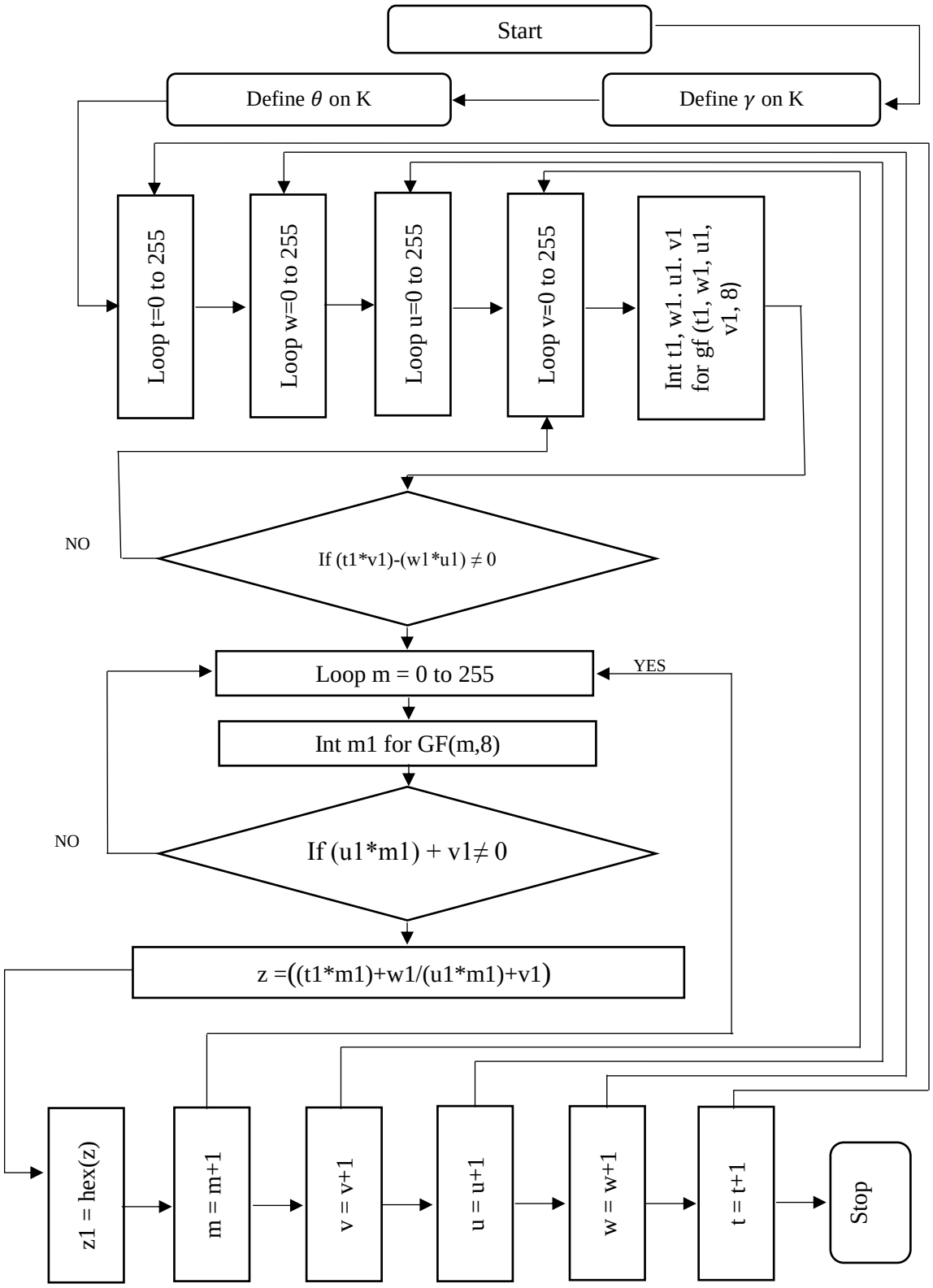


Fig. 1 Algorithm for the structure of constructed S-box

$$g: PGL(2, K) \times K \to K$$

The linear fractional transformation is an invertible map and mathematically it can be defined as:

$$g(2m + 1) = \frac{31m+19}{23m+7},\ 0 \leq n \leq 255 \tag{2.6}$$

where 31, 19, 23 and 7 belongs to Galois field. With the help of this map, Table 2 is converted into a 16×16 table that provides our new S-box. The 256 dissimilar results of the proposed S-box are shown in Table 3. Fig. 1 shows the algorithm for the synthesis of S-box.

Table 3: S-Box constructed by using finite commutative ring

199	24	244	208	226	40	65	32	3	114	172	238	103	25	141	92
44	42	149	77	78	36	104	105	133	52	222	55	247	85	186	87
64	214	171	7	49	164	239	216	35	230	125	168	192	163	246	190
147	116	110	60	107	196	41	228	191	128	176	152	205	51	106	4
86	132	120	20	158	143	167	21	118	173	201	198	210	90	59	112
180	217	0	188	30	88	174	48	27	209	136	17	47	157	140	175
130	177	207	189	181	170	117	73	153	26	204	185	111	8	248	187
71	212	235	67	63	95	102	62	223	184	155	129	200	221	97	38
113	69	16	5	252	234	9	56	254	193	178	75	1	237	160	33
124	84	91	123	119	206	229	115	148	89	220	241	57	31	2	218
165	19	43	28	166	66	54	100	74	127	96	231	243	240	13	68
138	12	98	156	253	93	224	6	11	46	29	139	169	50	232	159
225	202	22	137	179	15	227	122	251	195	23	249	18	61	211	151
213	145	245	79	126	76	70	39	182	80	135	236	34	10	58	250
154	121	146	215	233	197	162	242	94	45	161	83	203	14	72	183
81	82	150	108	109	37	144	142	99	255	101	194	131	219	134	53

It is clear from the algorithm that loop applied in it takes values of t, u, v and w along with values of m from the set $\{0,1,2,\ldots,255\}$. The algorithm moves through the step A3 once it is confirmed that the result of $t \times w - u \times v$ is not equal to 0. Moreover, the condition that $23m + 7 \neq 0 \; \forall \; m$ is also necessary for the iteration of the third step A3 for the structure of our new S-box.

2.3. Statistical results and simulation analysis

This section investigates different characteristics of suggested S-box generated by an algebraic structure which involves group action of the projective general linear group over K (the units of $\mathbb{Z}_{512}$). The valuation of S-box gives assurance of its effectiveness and capability to generate confusion in cipher. The three categories of performance indexes provide the analyses of S-box. The non-linearity of proposed S-box is evaluated in first category. In the second category, the effects of deviation in input bits observed in output bits are observed. The last category is about outcomes of probability of events and differential uniformity. It is observed that the S-box reaches almost all conditions near to ideal results. The subsections concisely designate the analyses linked with the secure S-box.

2.3.1. Nonlinearity

To measure the distance of known Boolean function to all possible affine functions is obtained in nonlinearity analysis. The modification in Boolean function is due to alteration of bits in the truth table. Hence, the outcomes of nonlinearity is the tally of altered bits with the aim of getting the closest affine function. Usually, for S-boxes, the nonlinearity is limited by $N(f) = 2^{m-1} - 2^{m/2-1}$ with optimal value at N=120. Table 4 provides the outcome of non-linearity of our new S-box. This S-box has average nonlinearity value 106.75 which is comparatively better as likened to the residue of Prime, Skipjack, Hussain and Xyi S-box. The proposed S-box non-linearity indicate

the unaffected behavior against cryptanalysis using algebraic attacks. It is observed that the least value of non-linearity is 100, the highest value is 110, and an average value is 106.75 for the proposed S-box.

Table 4: Nonlinearity of basic functions of well-known S-boxes

S-boxes	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	Average
Hussain [15]	104	106	106	106	110	104	100	108	105.5
Prime [29]	94	100	104	104	102	100	98	94	99.5
Skipjack [31]	104	108	108	108	108	104	104	106	105.75
Proposed	106	108	110	110	108	104	100	108	106.75
Hussain [14]	102	104	98	108	104	102	108	106	104
AES [3]	112	112	112	112	112	112	112	112	112
S_8 AES [28]	112	112	112	112	112	112	112	112	112
Xyi [30]	106	104	106	106	104	106	104	106	105

2.3.2. Design of Input/Output Bits

Many methods in the literature assess the changes occurred in output bits due to alteration in input bit patterns. The special effects of these variations can be observed in different rounds of the encryption process. The alterations of input bits and the measure of independence between pair wise avalanche vectors are the significant aspects of BIC. The eight functions used in the construction of S-box and the outcomes of the successive iterations are the major sources of independent features. These iterations are attained when the input bits are altered to recognize the behavior of any two output bits. Table 5 provides the outcomes for the non-linearity of BIC. In Table 6, least values, average values and square deviation of BIC for constructed S-box are given. From this table, it is obvious that average value of our S-box is better as compared to Xyi, Hussain

[35] and prime S-boxes. To understand the characteristics of output bits in detail, the SAC is used. If the particular input difference grounds sequence of variations in the entire network of substitution-permutation, the avalanche result is viewed. It is observed that half of the values have converted values due to this single input variation.

Table 5: Values of Non-linearity of BIC of S-box

----------	108.000	108.000	104.000	104.000	104.000	106.000	106.000
108.000	----------	106.000	108.000	108.000	106.000	106.000	108.000
108.000	106.000	---------	108.000	106.000	106.000	104.000	106.000
104.000	108.000	108.000	----------	108.000	108.000	108.000	106.000
104.000	108.000	106.000	108.000	---------	108.000	104.000	104.000
104.000	106.000	106.000	108.000	108.000	----------	106.000	104.000
106.000	106.000	104.000	108.000	104.000	106.000	----------	108.000
106.000	108.000	106.000	106.000	104.000	104.000	108.000	----------

Table 6: Bit independence criterion of different S-boxes

S-boxes	Least value	Average	Square deviation
New S-box	104	106.27	1.578
Hussain [15]	106	102	2.1381
Hussain[14]	98	103.37	0
Prime [29]	94	101.71	3.53
S8 AES [28]	112	112	0
Xyi [30]	98	103.78	2.743
AES [3]	112	112	0
Skipjack [31]	102	104.14	1.767

When SAC is functional to the nonlinear S-box transformation of proposed algorithm these variations are observed. The outcome assures the confrontation against cryptanalysis and the asset of the cipher. Table 7 demonstrates the outcomes for the SAC. The outcomes for SAC are almost the same as for another designed S-box.

Table 7: SAC of new S-box

0.5000	0.5313	0.5000	0.4531	0.4844	0.5469	0.4844	0.4688
0.5156	0.4844	0.4688	0.5469	0.4531	0.5469	0.4375	0.4844
0.4688	0.5000	0.5156	0.4375	0.5312	0.6094	0.4688	0.5000
0.4844	0.5000	0.4688	0.4844	0.4375	0.5312	0.4688	0.5000
0.5313	0.4688	0.5000	0.5000	0.4844	0.4531	0.5469	0.4844
0.5625	0.5469	0.5000	0.4844	0.5000	0.5312	0.5156	0.5782
0.4375	0.4532	0.4844	0.4688	0.5156	0.4844	0.4531	0.5156
0.5000	0.5000	0.5938	0.5312	0.4844	0.4844	0.5156	0.5000

2.3.3. Approximation Probability Analysis

Here, the probability analysis is discussed for the proposed S-box. Initially, linear approximation probability is used on new S-box to calculate the result of an imbalance of an event [17]. Due to changes in input bits pattern there is an imbalance at output bits. The outcomes of differential uniformity provide strong point to linear approximation analysis. The r_u and r_v are the required masks which are functioned on the equivalence of both input and output bits. We can define it as,

$$LP = \max_{\mathrm{r}_u, \mathrm{r}_v \neq 0} \left| \frac{\#\{u/u \bullet \mathrm{r}_u = S(u) \bullet \mathrm{r}_v\}}{2^l} - \frac{1}{2} \right| \tag{2.7}$$

where all the probable domain results can be given by u and total number of elements are given by 2^l. Table 8 gives the output of this probability of bias. From these values, it is obvious that the

new S-box give extensive confrontation to linear assaults. The maximum result for linear approximation probability is 160.

Table 8: Comparison of Linear approximation probability of proposed and well-known S-boxes

S-boxes	Hussain [15]	Prime [29]	Proposed	Hussain [14]	S_8 AES [28]	Xyi [30]	Skypjack [31]	AES [3]
Max value	160	162	160	160	144	168	156	144
Max LP	0.1328	0.132	0.125	0.140	0.062	0.156	0.109	0.062

Table 9: Results of differential probability of proposed S-box

.0234	.0234	.0234	.0234	.0234	.0234	.0156	.0234	.0234	.0234	.0234	.0234	.0312	.0313	.0156	.0234
.0234	.0234	.0313	.0234	.0234	.0234	.0313	.0234	.0313	.0313	.0234	.0234	.0234	.0234	.0234	.0156
.0234	.0234	.0234	.0234	.0234	.0312	.0234	.0156	.0234	.0313	.0234	.0234	.0156	.0156	.0234	.0234
.0234	.0313	.0156	.0234	.0234	.0234	.0234	.0156	.0234	.0234	.0234	.0313	.0234	.0313	.0234	.0234
.0234	.0234	.0234	.0313	.0234	.0234	.0234	.0156	.0234	.0234	.0156	.0234	.0234	.0234	.0234	.0234
.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.0234	.0234	.0234	.0313	.0312	.0234	.0313	.0313
.0313	.0234	.0234	.0234	.0234	.0312	.0234	.0234	.0156	.0234	.0234	.0391	.0234	.0313	.0234	.0234
.0313	.0156	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.0156	.0234	.0234	.0234	.0234	.0234
.0234	.0156	.0234	.0234	.0234	.0234	.0234	.0234	.0312	.0313	.0234	.0234	.0234	.0234	.0234	.0234
.0234	.0234	.0156	.0234	.0234	.0234	.0312	.0234	.0234	.0234	.0234	.0234	.0156	.0234	.0234	.0313
.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.0234	.0156	.0156	.0234	.0313	.0234	.0234	.0234
.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0156	.0156	.0234	.0156	.0313	.0234
.0313	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234
.0234	.0234	.0234	.0313	.0156	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234	.0234
.0234	.0234	.0234	.0234	.0234	.0234	.1171	.0234	.0156	.0234	.0234	.0234	.0234	.0313	.0234	.0313
.0156	.0234	.0156	.0234	.0234	.0234	.0234	.0234	.0312	.0156	.0234	.0234	.0313	.0313	.0234	-----

The value of Linear approximation probability is 0.125. Secondly, differential uniformity is calculated with the help of differential probability analysis. By plotting the input bits to output bits

the theme is to find and analyze any uniquely plotted differential for input bits. For input differential, Δu is a unique uniform mapping which provides an output of a Δv. It is represented by

$$D_{P^S}(\Delta u \rightarrow \Delta v) = \frac{[\#\{u \varepsilon U / S(u) \oplus S(u \oplus \Delta u) = \Delta y\}]}{2^d} \quad (2.8)$$

The outcomes of this probability scrutiny are given in Table 9 which is the probability of differential by functioning the input and output differentials. Interestingly, the value of differential probability is almost equal to prime, gray, APA and S_8 AES S-boxes.

2.4. Majority Logic Criteria

In MLC, statistical studies are done to assess the statistical strength of the novel S-box for the encryption of data [38]. For analyzing the confusion creating ability of S-box, certain statistical and analytical methods are available in the literature. As encryption process handles data and produces alteration in the image, it is essential to get results of statistical properties. The outcomes of these analyses help us to determine best suited S-box for the whole encryption procedure. In these analyses, homogeneity, contrast, correlation, entropy, energy are evaluated and given in Table 10.

2.4.1. Entropy analyses

In any cryptosystem, measure of the amount of randomness is called entropy. For images, the degree of entropy is linked to the organization of artifacts which supports the individuals to observe the image. In this process of substitution, or application of nonlinear S-box transformation, introduces randomness in the image. The extent of randomness introduced by the encryption process is extremely relevant to the fact that the human eye can perceive the texture in the image.

The lack of randomness may result in partial/full recognition of the encrypted image. Therefore, the measurement of entropy may provide important information about the encryption strength, and is measured as

$$H = \sum_{i=0}^{n} p(x_i) log_b\, p(x_i) \tag{2.9}$$

where $p(x_i)$ indicates the histogram counts.

2.4.2. Energy

Energy analysis is used to determine the energy of the encrypted image. The gray-level co-occurrence matrix is also used in energy analysis. Mathematically it can be given as

$$E = \sum_{i} \sum_{j} P^2[i,j] \tag{2.10}$$

2.4.3. Contrast

The objects in an image are vividly identified to an observer with the help of amount of contrast in the picture. A reasonable amount of contrast levels in the image also saturates the artifacts which enable the identification of the image more precisely. Due to encryption of an image, the amount of randomness rises, which uplifts the contrast, levels to a very high value. The objects in the image completely smudge because of the nonlinear mapping from the substitution of the image data. We can conclude that a higher level of contrast in the encrypted image depicts strong encryption because it is related to the amount of confusion created by the S-box in the original image. The mathematical representation of this analysis is given as

$$C = \sum_{i} \sum_{j} (i-j)^2 p[i,j] \tag{2.11}$$

Here i and j are the pixels in the image, and the number of gray-level co-occurrences matrices is represented by $p(i,j)$.

2.4.4. Homogeneity

The image data have a natural distribution which is related to the contents of that image. We perform the homogeneity analysis which measures the closeness of the distributed elements in the GLCM to GLCM diagonal. This is also known as gray tone spatial dependency matrix (GLCM). The GLCM depicts the statistics of combinations of pixel gray levels in tabular form. The analyses are further extended by processing entries from the GLCM table. The mathematical representation of this analysis is given as

$$H = \sum_{i} \sum_{j} \frac{p(i,j)}{1 + |i - j|} \tag{2.12}$$

2.4.5. Correlation

The correlation analysis is divided into three different types. It is performed on vertical, horizontal, and diagonal formats. In addition to analysis on partial regions, the entire image is also included in the processing. This analysis measures the correlation of a pixel to its neighbor by keeping into consideration the texture of the entire image. The mathematical representation of the correlation analysis is given as

$$K = \sum_{i,j} \frac{(i - \mu i)(j - \mu j)p(i,j)}{\sigma_i \, \sigma_j} \tag{2.13}$$

By considering the significance of the outcomes of above-mentioned analyses, the data are further assessed by MLC to obtain the S-box for different applications.

Table 10: MLC results for S-box over $\mathbb{Z}_{512}$ and different S-boxes

S-boxes	Entropy	Correlation	Homogeneity	Contrast	Energy
Cameraman Image					
Plain Text	7.1025	0.9292	0.8964	0.4785	0.1679
S-box over $\mathbb{Z}_{512}$	**7.9828**	**- 0.0024**	**0.4133**	**8.3936**	**0.0179**
AES	7.2531	0.0554	0.4662	7.5509	0.0202
Hussain [14]	7.3557	0.0473	0.4821	7.2173	0.0209
Prime	7.2531	0.0855	0.4640	7.6236	0.0202
S_8 AES	7.2357	0.1235	0.4707	7.4852	0.0208
Hussain [15]	7.7536	0.1683	0.4924	7.4521	0.0315
Xyi	7.2531	0.0417	0.4533	8.3108	0.0196
Skipjack	7.2531	0.1025	0.4689	7.7058	0.0193
Gold Hill Image					
Plain Text	7.4761	0.9084	0.8700	0.3341	0.1274
Proposed S-box	**7.9385**	**0.0423**	**0.4443**	**7.6225**	**0.0196**
AES	7.2531	0.0554	0.4662	7.5509	0.0202
Hussain [14]	7.5131	0.1473	0.4760	7.9511	0.0199
Prime	7.2531	0.0855	0.4640	7.6236	0.0202
S_8 AES	7.2357	0.1235	0.4707	7.4852	0.0208
Hussain [15]	7.6521	0.0786	0.4223	7.5003	0.0300
Xyi	7.2531	0.0417	0.4533	8.3108	0.0196
Skipjack	7.2531	0.1025	0.4689	7.7058	0.0193

Table 10 indicates that MLC results of proposed S-box are better as compared with Hussain [35], [39], skipjack, prime and xyi. Our proposed S-box is highly recommended for multimedia security

methods and encryption applications. The baboon, cameraman and Gold hill images and their substitution with proposed S-box are given in Fig. 2(a)-c, respectively.

a b c

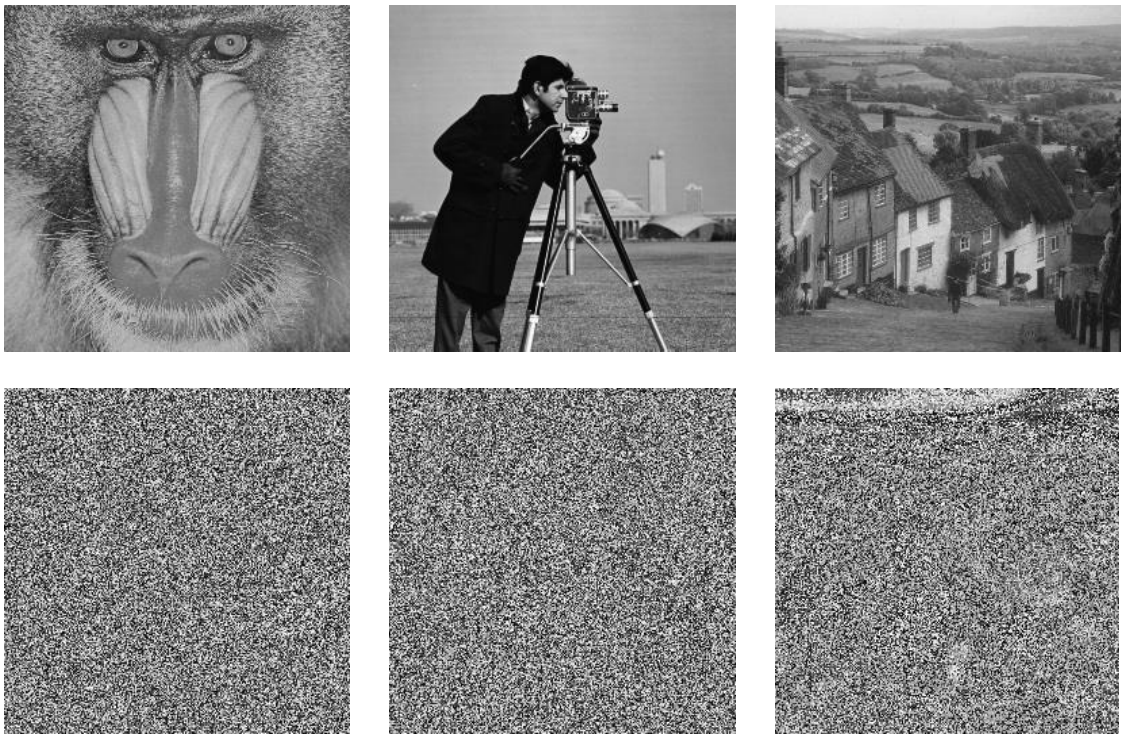
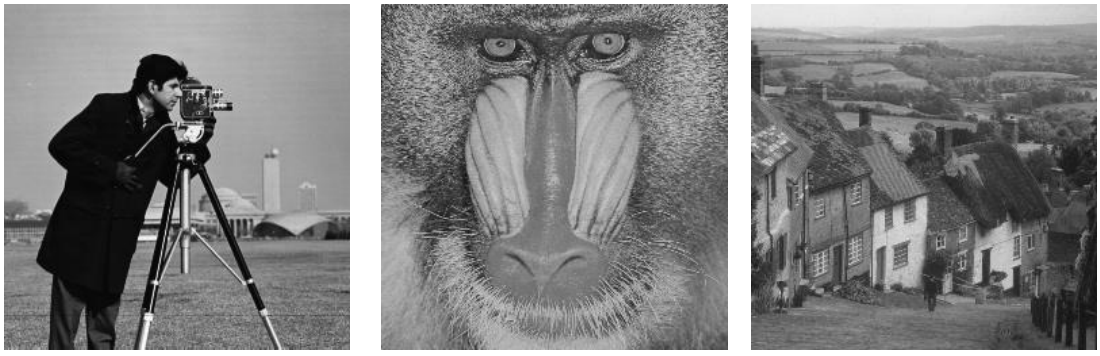


Fig. 2: Host and the encrypted image (a). Baboon. (b). Cameraman. (c). Gold hill.

The encryption of cameraman, baboon and gold hill images with Hussain S-boxes is given in Fig.3a-c respectively.



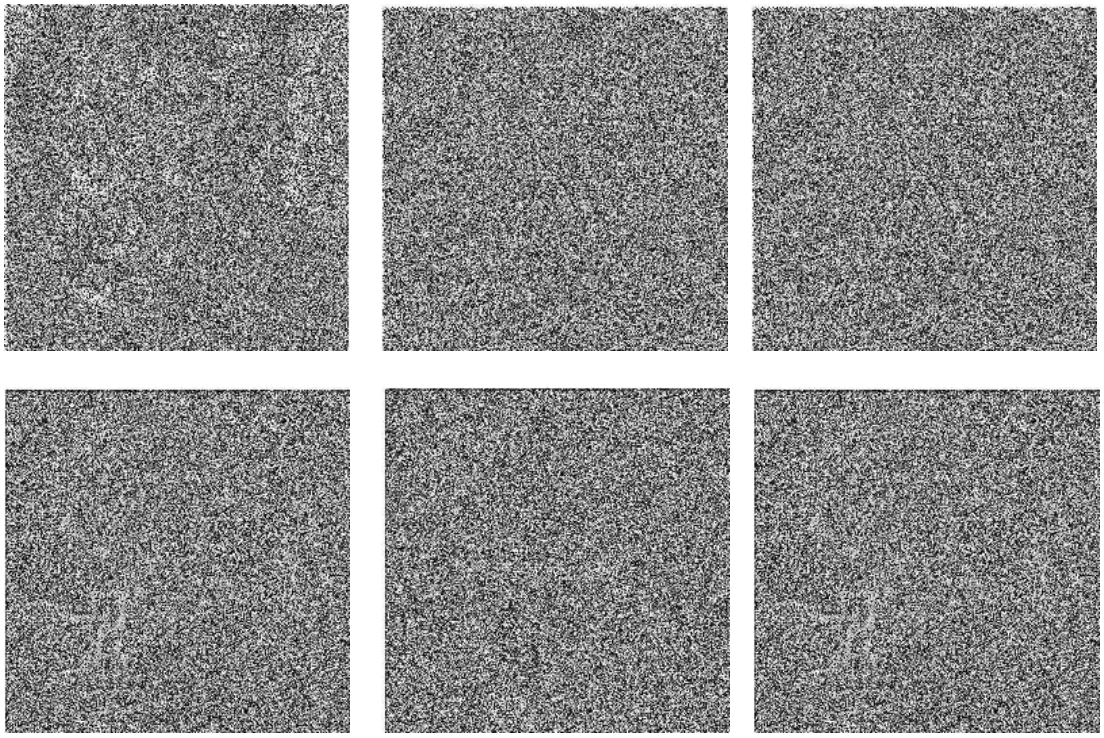


Fig. 3: Host and the encrypted image with Hussain [35], [39] S-boxes respectively

(a). Cameraman (b). Baboon. (c). Gold hill.

This substitution with proposed S-box indicates the complete encryption. MLC outcomes show that the proposed S-box is apposite for encryption and secure transmission of the information.

In this chapter, a scheme for construction of S-box by using group action of the projective general linear group over the unit element of $\mathbb{Z}_{512}$ is presented. The ability of our new S-box to create perplexity in data is quite exceptional. The proposed S-box can be used for information hiding techniques and different encryption process. In the next chapter, we suggest that the choice of the background irreducible polynomial, involved in the structure of the Galois field $GF\ (2^8)$, has a critical influence on the highly desirable features on an S-box

Chapter 3

Construction of S-Box Using Different Irreducible Polynomial

Keeping in view the importance of the S-box, many designs are recently presented by researchers to synthesize cryptographically stronger S-boxes. In this chapter, we suggest that the selection of the background irreducible polynomial, has a deep influence on the highly desirable features on an S-box such as nonlinearity, bit independence, strict avalanche, linear and differential approximation probability etc. We therefore propose that the capacity of an S-box is not just depending on the nature of the bijective Boolean function, however, it is affected by the degree 8 irreducible polynomial $\mu(X)$ as well, which generates the maximal ideal of the principal ideal domain $\mathbb{F}_2[X]$. We discuss a detailed example to support our proposition and show practically that the same algorithm produces a different output when the generating polynomial is changed.

3.1. Statement of the problem

The study of innovation in design algorithms for S-boxes witnesses that the change of model and the selection of Boolean function etc. contribute little to the performance indices of an S-box. We in this chapter propose that the performance of an S-box is highly related with the background Galois field. The fact that finite fields of the same order are isomorphic is of worth but the scrambling effect of a nonlinear Boolean function applied on two different fields of the same order might vary. Since in cryptography, an S-box is the salient component used to produce confusion

in the data, it is worth-studying that the confusion creating ability is associated with the choice of the irreducible polynomial used to form the background Galois field.

In [35], Hussain et. al. presented an algorithm for generating S-box through the application of a linear fractional transformation on the Galois field $GF(2^8)$, structured by the polynomial $X^8 + X^4 + X^3 + X^2 + 1$. We in the proposed work show that the same algorithm used for a different polynomial exhibits highly improved results. By comparing the numerical results of these tests, we prove that different polynomials produce significantly different results. This observation leads us to revise the existing models by choosing different background polynomials as it could be more influential in the improvement of ideas rather changing the whole scheme.

3.2. Generating Polynomial and the Galois Field

For any prime p, Galois field $GF(P^n)$ is expressed as the factor ring $F_P[X]/(\mu(X))$ where $\mu(X) \in \mathbb{F}p[X]$ is an irreducible polynomial of degree n. For $GF(2^8)$ we select an irreducible polynomial of degree-8 that becomes the maximal ideal of the principal ideal domain $\mathbb{F}_2[X]$. It is quite obvious, that the multiplicative group of this field $GF(2^8)$ is cyclic in nature and therefore, power of the generator α = 00000010 can be used to express every nonzero element of this field. In this section, we take two irreducible polynomials μ_1 and μ_2 of degree 8, to construct Galois Field $\mathbb{F}_1$ and $\mathbb{F}_2$ respectively, where we choose $\mu_1 = X^8 + X^6 + X^5 + X^4 + 1$ and $\mu_2 = X^8 + X^4 + X^3 + X^2 + 1$, as used in [35]. Let G_i represents the multiplicative group of the Galois field, $\mathbb{F}_i$.The exponential form of elements of the multiplicative group G_1, along with their inverses, is represented in Table 1, however the elements of G_2 are presented in Table 2 of [35]. In the upcoming section, we use these calculations to construct the corresponding S-boxes.

3.3. Algorithm for S-box

An $n \times n$ S-box can be given as:

$$S_n(v) = (s_1(v), s_2(v), \dots, s_n(v),$$

where $v = (v_1, v_2, \dots, v_2^n) \in \mathbb{F}_2^n$ and each of $S_i's$ is regarded as a component Boolean function.

For a field $\mathbb{F}$, the general linear group $GL(n, \mathbb{F})$ is a group constructed by all $n \times n$ invertible matrices. A projective general linear group of degree n over a field $\mathbb{F}$ is defined to be the quotient group of $GL(n, \mathbb{F})$ by its center. For this chapter, we form the 8×8 S-box by considering the action of the Galois field $GF(2^8)$ on the projective linear group $PGL(2; GF(2^8))$, i.e. we take a function

$$\sigma: PGL\big(2, GF(2^8)\big) \times GF(2^8) \to GF(2^8)$$

Table 1: Exponential representation and the multiplicative inverses of elements of G

$x \in G$	α^n	x^{-1}	$x \in G$	α^n	x^{-1}	$x \in G$	α^n	x^{-1}
1	α^{255}	1	87	α^{240}	193	172	α^{223}	47
2	α^{1}	184	88	α^{157}	99	173	α^{220}	9
3	α^{231}	208	89	α^{116}	163	174	α^{241}	216
4	α^{2}	92	90	α^{243}	54	175	α^{31}	41
5	α^{207}	159	91	α^{128}	149	176	α^{158}	137
6	α^{232}	104	92	α^{253}	4	177	α^{65}	166
7	α^{59}	134	93	α^{205}	158	178	α^{117}	233
8	α^{3}	46	94	α^{33}	86	179	α^{250}	32
9	α^{35}	173	95	α^{18}	192	180	α^{244}	27

10	α^{208}	247	96	α^{236}	190	181	α^{10}	25
11	α^{154}	139	97	α^{163}	235	182	α^{129}	242
12	α^{233}	52	98	α^{214}	162	183	α^{145}	146
13	α^{20}	48	99	α^{98}	88	184	α^{254}	2
14	α^{60}	67	100	α^{247}	113	185	α^{230}	209
15	α^{183}	117	101	α^{55}	123	186	α^{206}	79
16	α^{4}	23	102	α^{136}	42	187	α^{58}	125
17	α^{159}	252	103	α^{102}	89	188	α^{34}	43
18	α^{36}	238	104	α^{23}	6	189	α^{153}	103
19	α^{66}	83	105	α^{82}	135	190	α^{19}	96
20	α^{209}	195	106	α^{43}	160	191	α^{182}	234
21	α^{118}	204	107	α^{177}	169	192	α^{237}	95
22	α^{155}	253	108	α^{13}	45	193	α^{15}	187
23	α^{251}	16	109	α^{169}	199	194	α^{164}	205
24	α^{234}	26	110	α^{141}	74	195	α^{46}	20
25	α^{245}	181	111	α^{89}	155	196	α^{215}	81
26	α^{21}	24	112	α^{63}	122	197	α^{171}	213
27	α^{11}	180	113	α^{8}	100	198	α^{99}	44
28	α^{61}	153	114	α^{228}	215	199	α^{86}	109
29	α^{130}	121	115	α^{151}	237	200	α^{248}	128
30	α^{184}	130	116	α^{132}	66	201	α^{143}	170
31	α^{146}	73	117	α^{72}	15	202	α^{56}	133
32	α^{5}	179	118	α^{76}	221	203	α^{180}	59
33	α^{122}	232	119	α^{218}	36	204	α^{137}	21

34	α^{160}	126	120	α^{186}	152	205	α^{91}	194
35	α^{79}	141	121	α^{125}	29	206	α^{103}	230
36	α^{37}	119	122	α^{192}	112	207	α^{29}	164
37	α^{113}	220	123	α^{200}	101	208	α^{24}	3
38	α^{67}	145	124	α^{148}	78	209	α^{25}	25
39	α^{106}	248	125	α^{197}	187	210	α^{83}	251
40	α^{210}	217	126	α^{95}	34	211	α^{26}	228
41	α^{224}	175	127	α^{174}	140	212	α^{44}	80
42	α^{119}	102	128	α^{7}	200	213	α^{84}	197
43	α^{221}	188	129	α^{150}	171	214	α^{178}	236
44	α^{156}	198	130	α^{71}	30	215	α^{27}	114
45	α^{242}	108	131	α^{217}	72	216	α^{14}	174
46	α^{252}	8	132	α^{124}	58	217	α^{45}	40
47	α^{32}	172	133	α^{199}	202	218	α^{170}	219
48	α^{235}	13	134	α^{196}	7	219	α^{85}	218
49	α^{213}	53	135	α^{173}	105	220	α^{142}	37
50	α^{246}	226	136	α^{162}	167	221	α^{179}	118
51	α^{135}	84	137	α^{97}	176	222	α^{90}	245
52	α^{22}	12	138	α^{54}	246	223	α^{28}	57
53	α^{42}	49	139	α^{101}	11	224	α^{64}	61
54	α^{12}	90	140	α^{81}	127	225	α^{249}	64
55	α^{140}	148	141	α^{176}	35	226	α^{9}	50
56	α^{62}	244	142	α^{168}	255	227	α^{144}	85
57	α^{227}	223	143	α^{88}	71	228	α^{229}	211

58	α^{131}	132	144	α^{39}	249	229	α^{57}	250
59	α^{75}	203	145	α^{188}	38	230	α^{152}	206
60	α^{185}	65	146	α^{110}	183	231	α^{181}	165
61	α^{191}	224	147	α^{239}	243	232	α^{133}	33
62	α^{147}	156	148	α^{115}	55	233	α^{138}	178
63	α^{94}	68	149	α^{127}	91	234	α^{73}	191
64	α^{6}	225	150	α^{204}	77	235	α^{92}	97
65	α^{70}	60	151	α^{17}	241	236	α^{77}	214
66	α^{123}	116	152	α^{69}	120	237	α^{104}	115
67	α^{195}	14	153	α^{194}	28	238	α^{219}	18
68	α^{161}	63	154	α^{52}	75	239	α^{30}	82
69	α^{53}	157	155	α^{166}	111	240	α^{187}	76
70	α^{80}	254	156	α^{108}	62	241	α^{238}	151
71	α^{167}	143	157	α^{202}	69	242	α^{126}	182
72	α^{38}	131	158	α^{50}	93	243	α^{16}	147
73	α^{109}	31	159	α^{48}	5	244	α^{193}	56
74	α^{114}	110	160	α^{212}	106	245	α^{165}	222
75	α^{203}	154	161	α^{134}	168	246	α^{201}	138
76	α^{68}	240	162	α^{41}	98	247	α^{47}	10
77	α^{51}	150	163	α^{139}	89	248	α^{149}	39
78	α^{107}	124	164	α^{226}	207	249	α^{216}	144
79	α^{49}	186	165	α^{74}	231	250	α^{198}	229
80	α^{211}	212	166	α^{190}	177	251	α^{172}	210
81	α^{40}	196	167	α^{93}	136	252	α^{96}	17

82	α^{225}	239
83	α^{189}	19
84	α^{120}	51
85	α^{111}	227
86	α^{222}	94

168	α^{121}	161
169	α^{78}	107
170	α^{112}	201
171	α^{105}	129

253	α^{100}	22
254	α^{175}	70
255	α^{87}	142

Table 2: S-box S_1

3	214	37	74	126	4	18	26	219	62	45	226	50	136	104	148
154	38	200	199	185	228	170	245	177	114	137	231	139	35	8	134
158	27	223	232	17	157	217	49	83	141	171	42	47	206	64	194
106	29	30	110	14	40	72	236	105	221	202	87	241	41	11	71
186	28	253	175	67	31	23	33	66	189	117	118	94	149	135	252
235	43	124	125	90	229	204	215	218	100	101	249	243	54	173	166
138	234	244	201	167	44	250	25	16	187	207	246	107	103	161	1
183	99	179	240	129	123	188	193	20	143	155	174	7	220	213	239
108	84	113	184	5	57	208	153	75	112	223	178	180	150	65	24
224	248	102	89	70	111	59	172	95	131	198	163	93	164	55	209
86	132	6	225	51	79	53	34	97	48	197	142	182	210	91	247
195	15	10	144	85	63	168	238	196	162	98	32	251	254	203	156
80	152	237	24	127	78	165	12	52	222	122	58	211	36	140	191
216	146	109	96	147	73	116	190	128	68	56	77	115	160	19	92
69	2	192	121	145	21	76	61	60	181	133	151	159	0	88	205
13	230	22	82	39	119	9	255	120	46	81	212	227	130	176	169

defined as;

$$\sigma(v) = \frac{\alpha v+\beta}{\gamma v+\delta} \tag{3.1}$$

In Eq. (3.1), σ is known as a linear fractional transformation (LFT) with α, β, γ and $\delta \in GF(2^8)$ satisfying the non-degeneracy condition $\alpha\delta - \beta\gamma \neq 0$. The ease of implementation, lesser computational labour and high algebraic complexity of an LFT are the prime features that give the incentive to employ this map for byte substitution. For the presented calculations, in particular, we choose $\alpha = 35, \beta = 15, \gamma = 9$ and $\delta = 5$.

Table 3: S-box S_2

198	214	241	163	130	165	217	127	179	123	111	197	43	141	237	3
168	201	17	121	142	101	232	174	11	249	16	156	10	50	183	65
72	184	200	132	58	47	27	159	231	189	8	18	206	194	177	31
193	92	122	192	85	137	243	49	178	170	36	135	230	95	100	128
13	109	227	0	224	144	208	78	173	32	139	234	107	82	172	81
51	233	12	154	94	161	244	55	7	34	251	225	153	93	254	138
102	240	115	242	110	134	124	79	157	160	90	238	73	53	169	250
136	118	112	48	40	114	22	246	46	131	23	69	52	235	248	2
116	91	117	26	166	25	219	59	54	229	120	245	89	185	99	226
105	45	60	199	164	191	228	202	37	104	143	209	220	147	44	186
145	125	203	29	38	41	215	108	64	88	119	74	213	96	211	83
218	146	196	205	67	152	129	175	84	158	207	176	80	62	150	86
57	155	195	216	75	19	1	87	33	68	71	236	239	255	35	212
148	188	133	15	204	187	42	182	97	56	24	221	252	30	77	181
4	247	167	21	9	222	180	190	151	140	39	171	14	126	66	253
103	223	70	98	28	20	63	162	61	113	149	210	106	5	6	76

The images of the map σ, when applied on $\mathbb{F}_1$ and $\mathbb{F}_2$ produce our S-boxes S_1 and S_2 respectively, as shown in Table 2 and 3 respectively.

3.4. Performance Analysis of S-boxes

The cryptographic strength of the S-boxes, generated in the foregoing section, is examined through nonlinearity, strict avalanche, bit independence, linear and differential approximation probabilities etc.

As it is mentioned before, non-linearity criterion outlines the total number of bits that must be altered in the truth table of a Boolean function to get close to the nearby affine function [40]. Table 4 shows that for S_1, the average nonlinearity measure is 112., which is the highest Fig. attained by the AES S- box. Fig. 1 shows the comparison which clearly depicts outstanding performance of S_1 as compared to S_2.

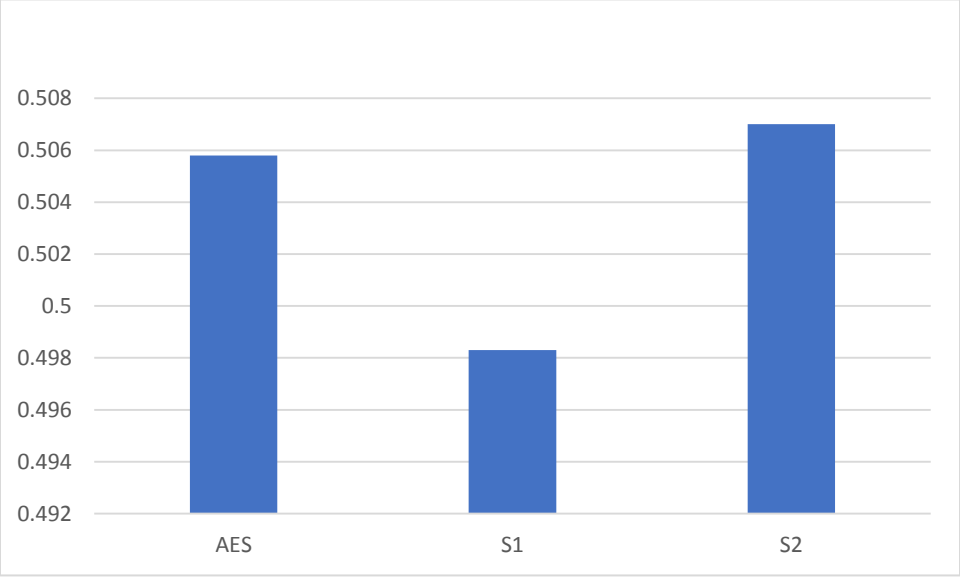


Fig. 1: Nonlinearity of different S-boxes

Table 4: Performance Indices for new S-box

Analysis	**Max.**	**Min.**	**Average**	**Square deviation**	**DP**	**LP**
Nonlinearity	113	111	**112**			
SAC	0.546875	0.429688	**0.498291**	0.0157537		
BIC		111	**111.751**	0.6227		
DP					**0.015625**	
LP						**0.064063**

Numerical outcomes presented in Table 5 and compared in Fig. 2 show that the linear approximation probability of S_1 is much better than S_2.

For further analysis, we utilize the differential approximation probability that gives the differential uniformity established by an S-box.

Table 5: Comparison of performance indices for various S-boxes

S-box	**Nonlinearity**	**SAC**	**BIC**	**DP**	**LP**
AES	112	0.5058	112	0.0156	0.062
S_1	112	0.498291	111.751	0.015625	0.064063
S_2	105.5	0.507	106	0.0242	0.140

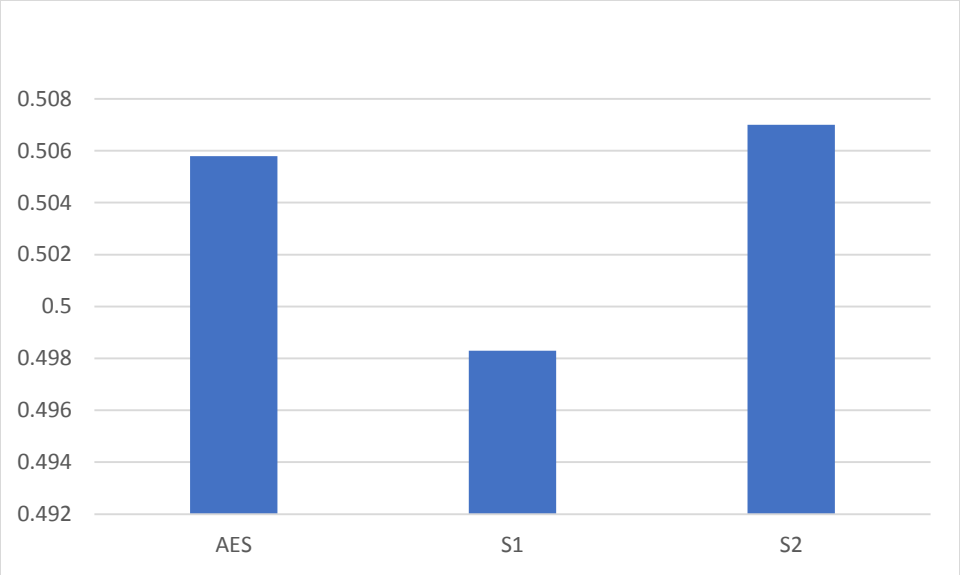


Fig. 2: LP of different S-boxes

Table 5 and Fig. 3 show that in terms of the differential approximation probability S_1 is much stronger than S_2

An S-box is said to fulfil strict avalanche criterion if for a change in an input bit, the probability of change in the output bit is 1/2. The outcomes are given in Table 5 and Fig. 4.

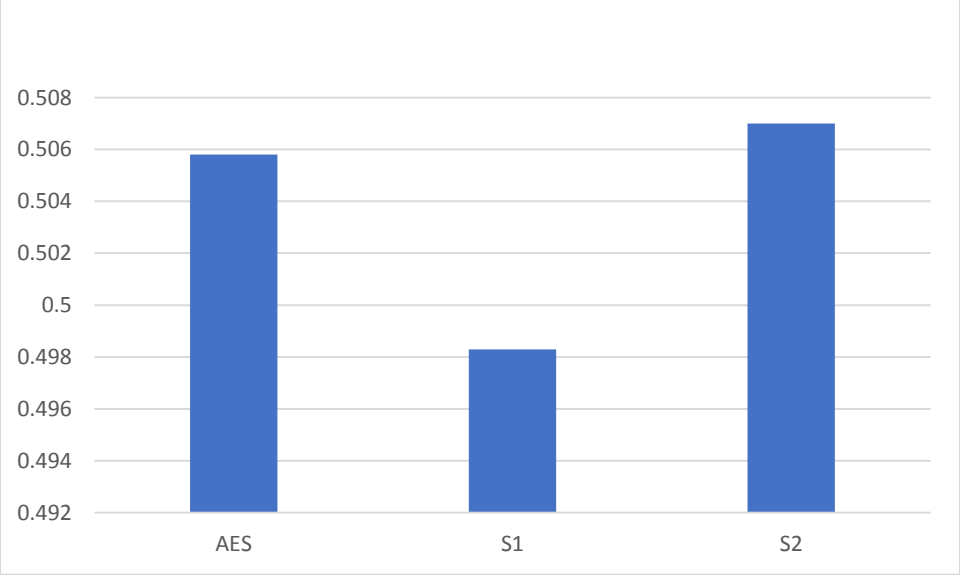


Fig. 3: DP of different S-boxes

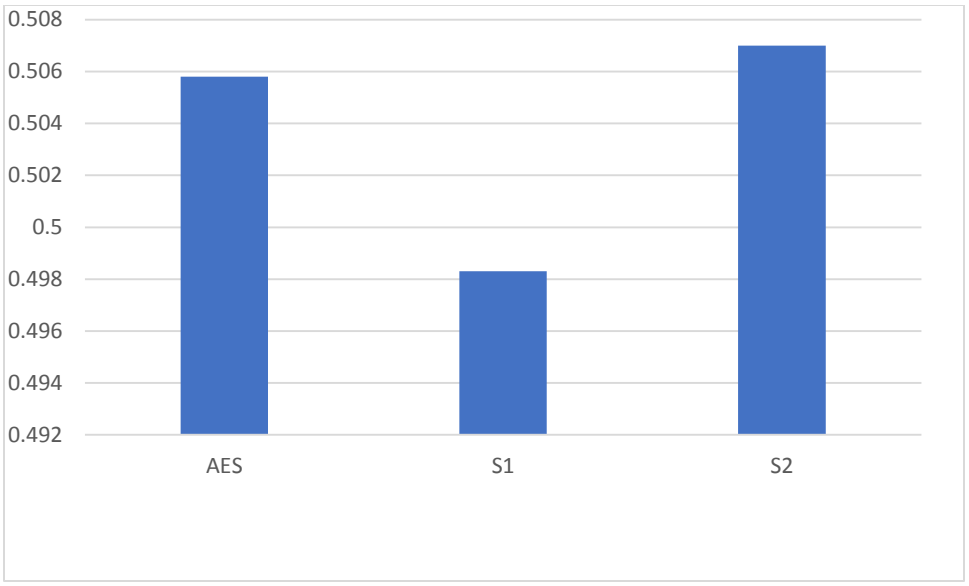


Fig. 4: SAC of different S-boxes

In BIC, input bits are transformed exclusively, and then output results are scrutinized for their independency [22]. The numerical results of BIC when applied to the proposed S-box are given in Table 5 and are compared in Fig. 5. It can be observed that according to these results our S-box S_1 is pretty like the AES S-box and is much better than S_2.

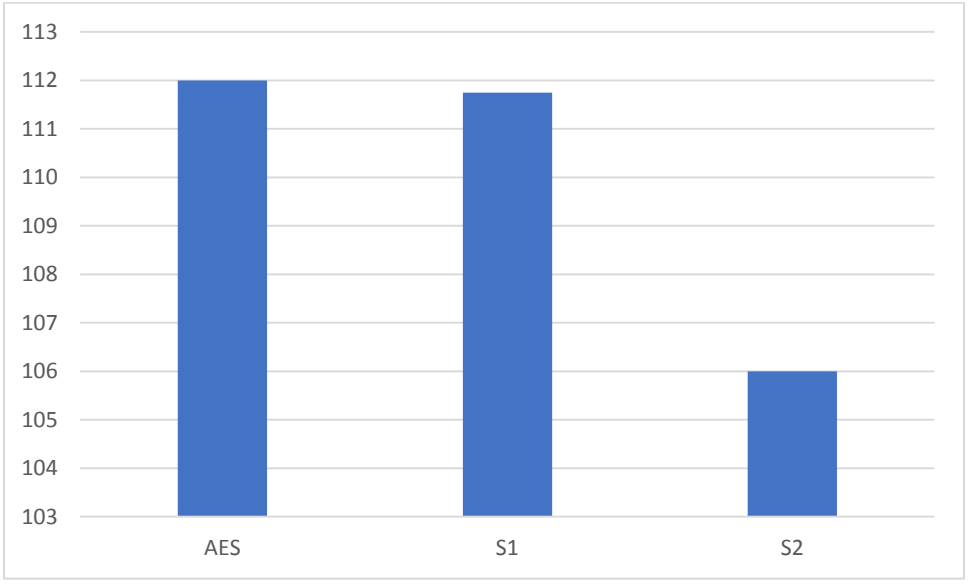


Fig. 5: BIC of different S-boxes

One can observe that overall performance of S_1 is much better than that of S_2. The performance parameters for S_1 seem to be pretty close to that of AES S-box. The algorithm used for both S_1 and S_2 is same but the primitive polynomial selected to generate the Galois field is different, which really contributes to the outputs.

The kernel of the presented work lies in the fact that the choice of the background Galois field and its generating primitive polynomial matters to the function and performance of the S-boxes. This fact leads to the fascinating idea that rather the development of new algorithms, the improvement of the existing algorithms is worth-studying as its least laborious but most effective. We propose, based on the example discussed, that the effect of the choice of generating polynomial may lead to an intensive research in future to modify the design models of S-boxes. In the next chapter, a new method for construction of S-boxes based on chaotic tent-sine map is proposed.

Chapter 4

Chaos Based Construction of S-Box

Over the last few decades**,** different mediums of secure communication use chaos which is demonstrated by some nonlinear dynamical systems. Chaos shows unpredictable behavior and this characteristic is quite helpful in different encryption techniques and for multimedia security. In this work, the chaotic behavior of the tent-sine map is discussed and a new method to make a S-Boxes is proposed. Moreover, S-box is evaluated with the help of certain algebraic tests which include nonlinearity, bit independence criterion, strict avalanche criterion, linear approximation probability and differential approximation probability. In addition to this, proposed S-box shows very good statistical properties like correlation, Homogeneity, energy, entropy, contrast, PSNR and MSE. The comparison of proposed S-box with some of privileged S-boxes, like AES, gray, APA S8 and Lui J depict the strong point of anticipated technique.

4.1. Introduction

The value and capability of producing confusion are measured by variations in output bit pattern. The selected S-box must be robust and shows opposition against any attempt of cryptanalysis. Nonlinearity is considered as a foremost performing criterion of the S-box in any encryption method. Over the years, researchers are keen to get algebraically strong and cryptographically robust S-boxes. In addition to this, chaos-based S-boxes also have their importance for secure communication of data. These S-boxes exhibit different striking properties and offer interesting results to various ciphers.[41].

S-box holds one to one and onto relations which makes it a bijection mapping and hence its inverse is possible. A text symbol is replaced with one element of S-box. By elaborating equation (4.1), *a* × *b* S-box takes *a* bit as the input and gives *b* bits as the output. It can be seen as

$$y1 = y2 \Rightarrow f(y1) = f(y2) \tag{4.1}$$

Some of the privileged S-boxes are AES, [42], gray [26], Lui J [43] and S8 [44]. In this work, the proposed technique for the synthesis of S-box is using a different chaotic maps to improve their chaotic range. Moreover, the group action of a projective general linear group is performed on the elements of GF (2^8). The distinct 256 values of our anticipated S-box are then compared with some of the existing S-boxes

4.2. Review of Various Chaotic Maps

In the past, various chaotic maps are applied for encryption schemes and for multimedia security. The background of Tent map and sine map is discussed in this section. By the combination of these two maps a Tent-Sine system (TSS) is formed which gives new chaotic S-box.

4.2.1. Chaotic Tent Map

It is obvious from bifurcation diagram of chaotic tent map; the map name is due to its tent map like shape. The interval of chaotic behavior of tent map is $[2, 4]$. The Lyapunov Exponent and bifurcation diagrams are shown in fig 1(a). It can be expressed as:

$$y_{n+1} = \begin{cases} \tau\frac{y_n}{2} & z_i < 1/2 \\ \frac{\tau(1-y_n)}{2} & z_i > 1/2 \end{cases} \quad 0 < \tau \leq 4;\ y_n \in [0,1] \tag{4.2}$$

The behavior of tent map is chaotic and uniform for the specific interval as depicted in bifurcation and Lyapunov Exponent diagrams. It shows the limitations of this chaotic map.

4.2.2. Chaotic Sine Map

The behavior of Logistic map and Sine map is similar to each other. This can be seen in both bifurcation and Lyapunov Exponent diagrams of sine map. Fig 1(b) describes the sine map graphical interpretation. It can be expressed as:

$$y_{n+1} = \frac{\sigma sin(\pi y_n)}{4}, 0 < \sigma \leq 4; y_n \in [0,1] \tag{4.3}$$

As both maps have identical behavior so they have the common problems as well. The range of chaos in sine map is limited as depicted in bifurcation diagram. Moreover, the non-uniformity of data combine with limited chaotic range makes application of sine map limited.

4.2.3. Chaotic Tent-Sine System

As the chaotic range of both tent map and sine map is limited so there is a demands of a chaotic map whose chaotic range is much greater as compared to two seed maps. A unique nonlinear combination of tent map and sine map give a chaotic Tent-Sine system (TSS). This arrangement of chaotic maps shows brilliant complex chaotic properties. The output range of data remains in interval $[0,1]$ due to mod 1 operator. The assimilation of parameters of both chaotic maps, the mathematical expression will take a form

$$y_{n+1} = \begin{cases} (\sigma \frac{y_n}{2} + (4-r)\sin(\pi y_n)/4) mod 1 & z_i < 1/2 \\ (\sigma (1-y_n)/2 + (4-r)\sin(\pi y_n)/4) mod 1 & z_i > 1/2 \end{cases} \tag{4.4}$$

where $0 < \sigma \leq 4$. The chaotic range of Tent-Sine system is increased remarkably well and the output sequences are distributed uniformly which can be seen in Fig 1(c).

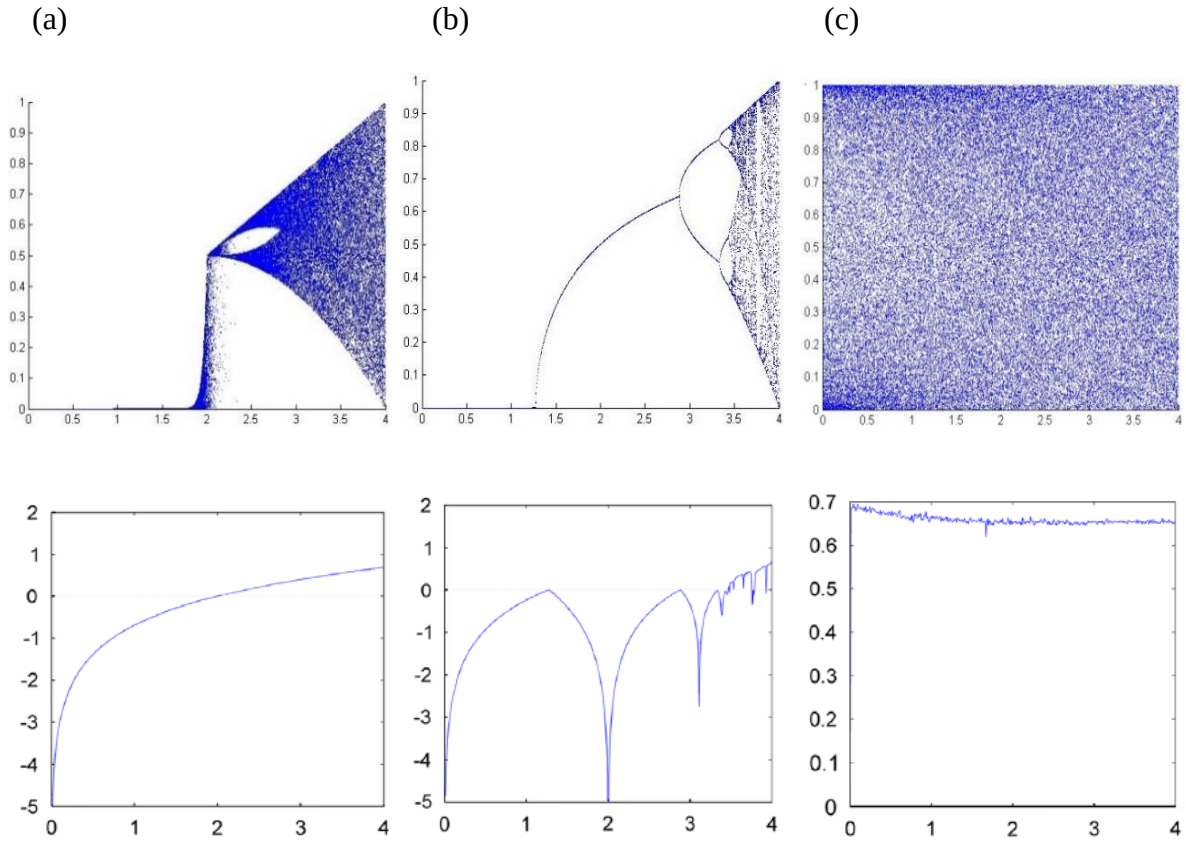


Fig. 1. Lyapunov and bifurcation diagrams of (a) Tent, (b) Sine and (c) TSS

4.3. Construction of chaotic S-box using Mobius Transformation

The careful selection of S-box provides support to confront any linear and differential cryptanalysis. With a higher chaotic range and complex properties, Tent-Sine system is considered for the structuring of proposed S-boxes. The flow chart given in fig 2 indicates that the primary input for the structure of S-box is taken from chaotic Tent-Sine map.

The mathematical foundation of the scheme is defined by using the concept of group action of a projective general linear group (linear fractional transformation) over a finite field (2^8). The choice of four random values, allocated to linear fractional transformation is selected from the chaotic Tent-Sine system. Further, we can explain it as:

$$g: PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8)$$

$$g(m) = \frac{ix+j}{kx+l},\ 0 \leq m \leq 255 \tag{4.5}$$

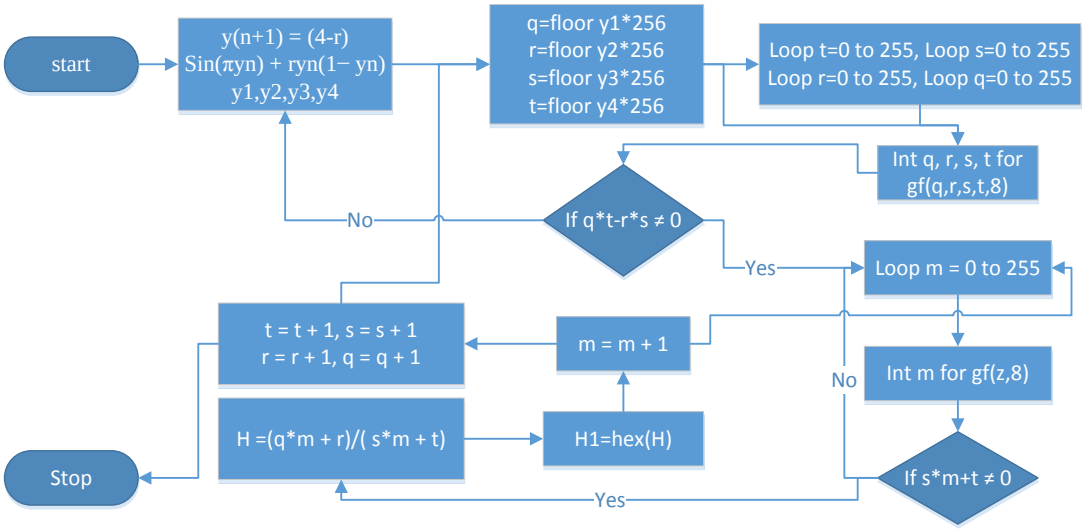


Fig. 2. Algorithm for the construction of proposed S-box

where, finite field (2^8).provides four chaotic values i, j, k and l. The products of this new scheme provide new chaotic S-box and values are given in Table 1. The algorithm depicts that loop applied in it takes values of i, j, k, l and m from interval 0-255.

4.3.1. Proposed S-boxes

S-boxes are constructed by using various powers of chaotic TSS. The detailed description of the map relates to first S-box is specified in equation (4.4) and the maps of rest of the four S-boxes are given in equations (4.6) to (4.9). The exponent in the equation of TSS is used as a parameter. The tabular form of proposed chaotic S-boxes is given in Tables (1) to (5).

$$y_{n+1} = \begin{cases} \left(\sigma \frac{y_n}{2} + (4-r)\sin(\pi {y_n}^{8/9})/4\right) mod 1 & z_i < 1/2 \\ \left(\sigma\,(1-y_n)/2 + (4-r)\sin(\pi {y_n}^{8/9})/4\right) mod 1 & z_i > 1/2 \end{cases} \tag{4.6}$$

$$y_{n+1} = \begin{cases} \left(\sigma \frac{y_n}{2} + (4-r)\sin(\pi {y_n}^{4/5})/4 \right) mod 1 & z_i < 1/2 \\ \left(\sigma \, (1-y_n)/2 + (4-r)\sin(\pi {y_n}^{4/5})/4 \right) mod 1 & z_i > 1/2 \end{cases} \quad (4.7)$$

Table 1. Chaotic S-box corresponds to the TSS by equation (6), $\beta = 1$

83	27	78	85	30	124	26	239	153	109	48	57	154	38	191	46
118	7	73	230	201	213	94	144	41	250	216	9	242	121	101	127
50	63	234	252	126	199	174	225	217	52	21	233	86	88	135	3
106	180	238	223	18	214	28	95	205	227	240	162	105	37	49	131
31	29	237	114	155	65	96	139	246	173	198	147	67	54	138	120
12	80	68	241	167	145	132	210	99	158	89	22	11	192	134	149
218	79	181	71	219	8	69	60	87	248	91	133	34	90	39	32
130	251	16	245	76	122	156	108	171	159	23	228	254	110	44	142
19	169	148	189	58	6	35	123	72	200	194	36	222	116	64	186
232	10	17	188	236	202	14	168	229	176	2	212	4	129	74	42
215	195	104	207	221	92	5	235	77	208	47	187	20	119	193	197
226	220	166	163	255	141	182	128	93	211	102	66	125	62	61	33
97	253	179	175	40	164	70	185	151	25	112	137	157	177	13	165
247	55	56	84	24	161	15	51	117	231	190	244	146	152	206	209
150	1	53	0	45	172	178	81	59	111	82	249	98	203	224	183
113	243	43	75	143	196	115	160	136	170	103	204	140	107	100	184

Table 2. Chaotic S-box corresponds to the TSS by equation (8), $\beta = 8/9$

112	80	53	200	68	242	11	3	72	46	89	136	114	224	78	166
174	120	176	65	73	163	204	95	30	23	107	197	32	217	128	215
1	214	33	6	154	180	75	158	143	173	169	161	185	116	92	0
164	12	115	137	221	245	19	51	44	8	195	59	181	142	160	41
237	190	110	189	29	35	213	129	148	127	24	18	208	171	56	119
252	134	186	126	232	183	109	246	162	25	203	222	34	211	27	111
170	60	2	202	98	206	64	133	177	130	225	22	250	233	251	228
49	104	71	238	201	149	90	152	105	150	20	97	184	47	94	255
223	52	199	118	66	48	147	17	145	124	74	153	231	240	132	117
40	39	139	36	7	81	212	103	155	101	219	187	102	62	21	113
125	144	249	106	196	121	167	83	168	138	209	227	151	10	191	37
188	63	100	69	77	254	179	84	178	57	247	239	15	28	135	220
205	216	198	42	175	13	5	9	244	50	79	182	141	165	58	243
207	96	193	76	31	99	146	226	87	70	93	234	194	236	253	230
218	159	55	235	122	14	4	16	229	248	241	88	38	192	157	61
43	131	156	67	26	45	172	108	91	140	85	82	123	86	210	54

Exponents used for the construction of these S-boxes are written with tables. Fig. 1 (c) give the bifurcation and Lyapunov diagram of TSS. The bifurcation diagrams of S-boxes having different exponents are shown in Fig. 3.

$$y_{n+1} = \begin{cases} (\sigma \frac{y_n}{2} + (4-r)\sin(\pi {y_n}^{6/7})/4) mod 1 & z_i < 1/2 \\ \left(\sigma (1-y_n)/2 + (4-r)\sin(\pi {y_n}^{6/7})/4\right) mod 1 & z_i > 1/2 \end{cases} \quad (4.8)$$

Table 3. Chaotic S-box corresponds to the TSS by equation (9), $\beta = 4/5$

51	188	63	187	122	179	183	101	24	1	55	147	254	111	211	62
226	66	225	189	250	169	39	120	213	108	82	215	204	84	58	96
95	253	75	22	30	159	127	228	28	85	117	121	57	232	25	13
4	103	19	99	136	78	5	202	7	10	64	114	243	23	90	61
129	67	148	138	139	182	170	80	42	155	110	91	145	115	151	68
43	105	0	245	16	252	89	171	178	227	222	153	162	164	168	231
104	247	210	251	35	165	27	69	37	249	2	191	40	156	207	208
41	83	32	199	74	205	152	125	220	94	234	17	8	255	123	106
229	132	11	244	175	79	36	15	100	87	190	157	52	173	137	59
48	65	167	236	18	146	72	192	38	246	216	12	238	174	131	235
112	26	154	130	161	6	20	172	98	107	212	50	73	77	116	185
119	224	31	181	197	109	166	209	180	46	124	242	53	186	214	128
218	184	21	150	140	86	92	102	240	237	60	143	163	221	195	194
56	158	93	54	160	3	126	134	49	29	47	217	70	97	141	206
113	248	200	9	177	233	198	76	203	142	71	241	230	45	144	239
196	81	193	133	223	118	34	176	33	201	149	135	88	44	219	14

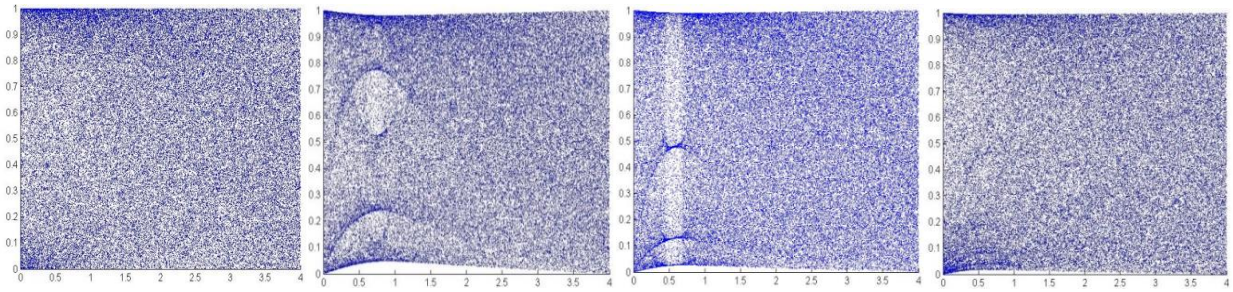


Fig. 3. Bifurcation diagrams for the expressions given in (a) Equ.(4.6), (b) Equ.(4.7), (c) Equ.(4.8), (a) Equ.(4.9).

$$y_{n+1} = \begin{cases} (\sigma \frac{y_n}{2} + (4-r)\sin(\pi {y_n}^{10/9})/4) mod 1 & z_i < 1/2 \\ \left(\sigma\,(1-y_n)/2 + (4-r)\sin(\pi {y_n}^{10/9})/4\right) mod 1 & z_i > 1/2 \end{cases} \quad (4.9)$$

Table 4. Chaotic S-box corresponds to the TSS by equation (10), $\beta = 6/7$

232	166	125	1	10	184	148	152	143	192	196	237	118	208	204	7
211	36	223	173	44	156	239	108	3	12	112	134	210	115	214	76
249	142	60	104	67	0	102	128	56	171	114	121	73	93	22	14
250	219	97	172	50	207	254	47	199	151	34	203	99	225	24	11
244	246	113	18	58	64	168	52	187	96	138	15	19	130	202	127
234	154	123	53	227	215	139	31	61	98	33	157	101	40	158	229
235	169	253	9	178	92	120	82	129	20	65	163	85	245	39	160
141	212	135	54	68	186	13	221	57	6	147	78	165	35	21	194
80	79	81	41	176	226	137	87	133	161	164	195	198	200	62	136
8	149	77	48	122	174	222	117	109	231	188	177	159	89	51	30
`233	100	205	4	181	119	32	182	243	86	71	213	209	185	45	75
106	111	220	228	124	90	251	72	91	17	224	230	59	94	206	43
247	23	216	238	74	162	144	16	193	183	28	201	170	37	167	84
189	69	150	105	236	131	83	255	155	179	29	242	95	140	153	145
110	240	88	116	107	146	63	252	26	42	197	103	46	27	66	126
241	132	25	217	5	175	70	180	248	190	218	2	38	55	191	49

4.4. Analysis of S-boxes

The assessment of S-box defines its utilization in any cryptosystem and for multimedia security [45] For this purpose, different theoretic and statistical approaches are being utilized to evaluate the characteristics of S-boxes [46]. A comprehensive demonstration of such techniques, involving differential properties of the block cipher is explained in [17]. This category of cryptanalysis is

used in DES algorithm, multiple ciphers and on different S-boxes. The cipher can be scrutinized by using information theory approach [46]. Different tests like the evaluation of nonlinearity, a scheme of input and output bits (strict avalanche criterion and bit independence criterion) that give features and connection of input and output bits and approximation probability (linear and differential approximation probabilities) which give the probability of events and differential uniformity to get an iterative method.

Table 5. Chaotic S-box corresponds to the TSS by equation (11), $\beta = 10/9$

51	244	119	243	122	179	183	45	80	1	55	147	254	111	155	118
170	10	169	245	250	225	39	120	157	108	26	159	204	28	114	40
95	253	75	22	86	215	127	172	84	29	61	121	113	232	81	69
4	47	19	43	192	78	5	202	7	66	8	58	187	23	90	117
129	11	148	194	195	182	226	24	98	211	110	91	145	59	151	12
99	105	0	189	16	252	89	227	178	171	222	209	162	164	224	175
104	191	154	251	35	165	83	13	37	249	2	247	96	212	207	152
97	27	32	143	74	205	208	125	220	94	234	17	64	255	123	106
173	132	67	188	231	79	36	71	44	31	246	213	52	229	193	115
48	9	167	236	18	146	72	136	38	190	216	68	238	230	131	235
56	82	210	130	161	6	20	228	42	107	156	50	73	77	60	241
63	168	87	181	141	109	166	153	180	102	124	186	53	242	158	128
218	240	21	150	196	30	92	46	184	237	116	199	163	221	139	138
112	214	93	54	160	3	126	134	49	85	103	217	14	41	197	206
57	248	200	65	177	233	142	76	203	198	15	185	174	101	144	239
140	25	137	133	223	62	34	176	33	201	149	135	88	100	219	70

Table 6 represents the nonlinearity of new S-boxes and other reputed S-boxes. The tables of S-boxes made by an upgraded range of chaotic maps and group action of a projective general linear

group is given in Tables 1, 2, 3, 4, 5. Moreover, the results of bit independence criterion, strict avalanche criterion, linear approximation probability and differential approximation probability are also calculated.

Table 6. Nonlinearity of proposed and well-known S-boxes

S-boxes	0	1	2	3	4	5	6	7	Ave
S-box-1	108	106	108	110	110	108	104	100	106.75
S-box-2	108	106	108	104	104	104	108	104	105.75
S-box-3	112	112	112	112	112	112	112	112	112
S-box-4	112	112	112	112	112	112	112	112	112
S-box-5	112	112	112	112	112	112	112	112	112
S8 AES	112	112	112	112	112	112	112	112	112
Jakimoski[4]	98	100	100	104	104	106	106	108	103.2
Tang[5]	100	103	104	104	105	105	106	109	104.5
Gray	112	112	112	112	112	112	112	112	112
Prime	94	100	104	104	102	100	98	94	99.5
Chen[6]	100	102	103	104	106	106	106	108	104.3
Skipjack	104	108	108	108	108	104	104	106	105.75
Wang [7]	104	106	106	102	102	104	104	102	103.7
APA	112	112	112	112	112	112	112	112	112
AES	112	112	112	112	112	112	112	112	112
Xyi	106	104	106	106	104	106	104	106	105

Moreover, the results of strict avalanche criterion, bit independence criterion, linear and differential approximation probabilities are depicted in Table 7.

Table 7. Results of algebraic analysis for the proposed S-boxes

S-box	BIC	SAC	BIC/SAC	DP	LP
S-box-1	106.286	0.500	0.500	0.1171	158/0.125
S-box-2	103.429	0.492	0.505	0.0391	162/0.133
S-box-3	112	0.504	0.504	0.0156	144/0.0625
S-box-4	112	0.504	0.504	0.0156	144/0.0625
S-box-5	112	0.504	0.504	0.0156	144/0.0625

4.5. Simulation Results and Statistical Analysis

The encryption quality of the S-box is analyzed by substituting the pepper image with five different proposed S-boxes.

Table 8. Comparison of Majority Logic Criterion results

Images	Contrast	Correlation	Entropy	Energy	Homogeneity
Plain Text	0.2668	0.9365	7.5498	0.1477	0.9191
Proposed I	**8.4388**	**0.0167**	**7.9876**	**0.0175**	**0.4152**
Proposed II	**8.5848**	**0.0056**	**7.9814**	**0.0174**	**0.4119**
Proposed III	**8.6736**	**0.0101**	**7.9829**	**0.0173**	**0.4104**
Proposed IV	**8.7232**	**0.0159**	**7.9767**	**0.0170**	**0.4121**
Proposed V	**8.4380**	**0.0275**	**7.9749**	**0.0175**	**0.4170**
AES	7.5509	0.0554	7.2531	0.0202	0.4662
APA	8.1195	0.1473	7.2531	0.0183	0.4676
Prime	7.6236	0.0855	7.2531	0.0202	0.4640
S8_AES	7.4852	0.1235	7.2357	0.0208	0.4707
Gray	7.5283	0.0586	7.2531	0.0203	0.4623
Xyi	8.3108	0.0417	7.2531	0.0196	0.4533
Skipjack	7.7058	0.1025	7.2531	0.0193	0.4689

Fig 4 gives the pictorial representation of the host and encrypted images. In addition to this, the results of histogram of the host and encrypted images is given in Fig. 5. The different analyses are performed to assess the S-box for encryption techniques and multimedia security purposes. The comparison of the results of these analyses for proposed technique with some of the existing S-boxes which include S8, AES, gray, APA, Lui J and is given in Table 2. The outcomes of our proposed technique are quite better as compared to existing techniques.

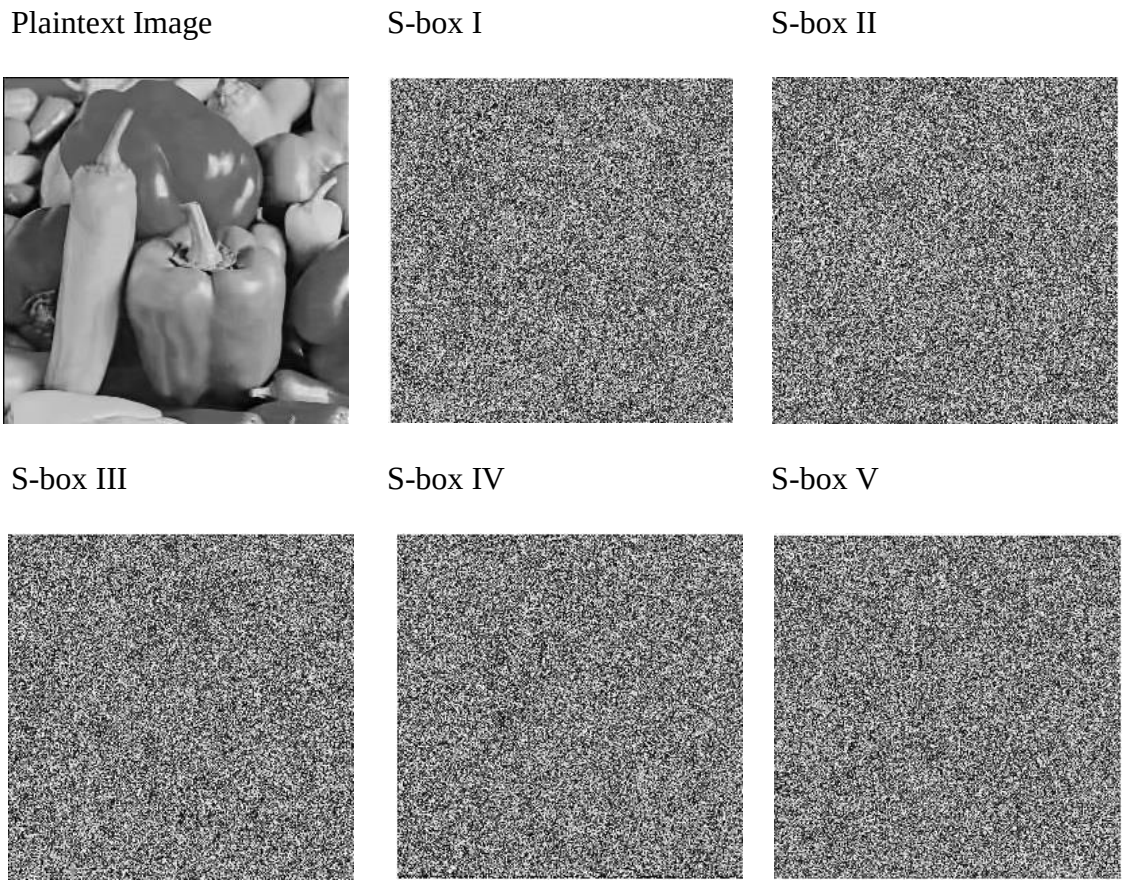


Fig. 4. Pepper image and its two rounds encrypted images with chaotic S-boxes

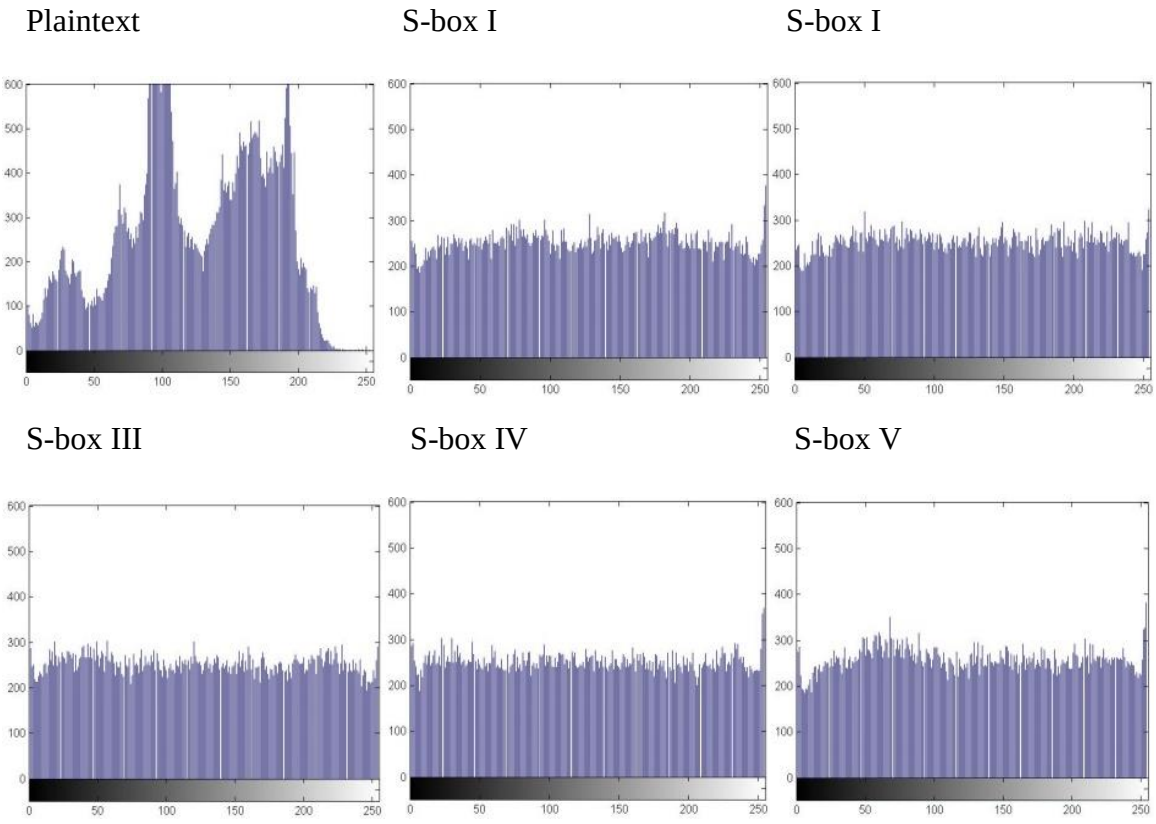


Fig. 5. Histograms of images known in Fig. 4.

In this chapter, the chaotic tent-sine system is applied for the structure of different S-boxes. The linear fractional transformation is used on random values of the chaotic map and provides 256 different values of S-box. The randomness produced with the inclusion of chaos not only increases the unpredictability of the cipher but also helps to resist any attempt of cryptanalysis. The chaotic S-box based frequency domain watermarking technique is presented in chapter 5. The issue of robustness is addressed by using chaos and frequency domain.

Chapter 5

A Watermarking Technique with Chaotic S-Box Transformation

In this chapter, the system of non-linear ordinary differential equations which describes a continuous-time dynamical system are applied to develop chaotic S-box. In this new digital watermarking technique, robustness problem is addressed by using chaos and frequency domain. In frequency domain watermarking, watermark is embedded into the low or middle frequencies which help to spread changes all over the image. Moreover, the fractional S-box is assessed by using algebraic and statistical analyses. In addition to this, some security analyses are done for the strength of proposed watermarking scheme. The confidence measure suggests the resistance of proposed technique against malicious attacks like noise, cropping and compression

5.1.

5.2. Introduction

In this proposed technique, S-box is constructed and employed for a new digital watermarking technique using frequency domain. Diffusion and confusion are the features of cryptographic structures and chaotic sequences. The unarranged behavior exhibited by non-linear dynamical systems may be considered as a basis of diffusion [41]. Chaotic communication which uses chaos theory having a feature of unpredictability planned to give security in the communication of data attained through broadcasting tools. The S-boxes is one of the applications of chaotic systems in

block cryptosystems and an application of chaotic cryptology [47]. The chaotic systems approach to utilize uncertainty makes it a striking choice in generating mix-up and additional in execution nonlinear alterations among various approaches to uncertainty.

Certain examples of chaotic maps constructed block ciphers are revealed in literature. Resistance to cryptanalysis is mainly due to chaotic maps for generation of strong block ciphers. We may use diverse types of chaotic maps to develop strong block cipher [48]. Three-dimensional baker's maps and heuristic approach for S-box is being used by Chen et. al. [49]. The idea to use the chaotic differential equation for generating the S-boxes is proposed by Özkaynak et al. and Khan et al [50]. The chaotic algorithms have shown numerous benefits like reasonable computational overheads, speed, computational power over the conventional algorithms and high security.

For the last three decades, different techniques for watermarking are developed and categorized into two main types named as spatial domain [51] and frequency domain techniques. In the first technique, the process of watermarking replaces the pixels of the host image with the watermark image. However, in the later technique, the watermark is embedded into the coefficients values of the host image. The main feature of both these techniques is to provide digital data the integrity, authentication, copyright protection, broadcast monitoring and most important robustness against malicious attacks [52]. In this proposed algorithm, strong cryptographic properties of fractional chaotic Rössler system help us to generate a S-box having the ability to create confusion and capability of adding randomness [53], we employed this chaotic S-box to propose a novel watermarking technique which embed watermark by using discrete Fourier cosine transform. Simulation results statistical analysis for host and watermark image depict good results. The robustness of proposed algorithm is analyzed by several image processing operations.

5.3. Mathematical Model of Chaotic System

Rössler was motivated by the geometry of flows in dimension three and, specifically, by the reinjection principle, which consists of relaxation-type systems to often present a Z-shaped slow manifold in their phase space. In dimension three, the reinjection can persuade chaotic behavior if the motion is spiraling out on one branch of the slow manifold. In this way, Rössler invented a series of systems which is applied for construction of chaotic system [54]. Mathematically, system of differential equations can be represented as|:

$$\frac{dx}{dt} = -y - z$$

$$\frac{dy}{dt} = x + ay \tag{5.1}$$

$$\frac{dz}{dt} = b - cz + zx$$

This dynamical system is basically for creating confusion in the plaintext to accomplish secure transmission. Comparatively, Rössler system and Lorenz attractor produce chaotic attractor with a single lobe and two lobes respectively.. The chaotic behavior of Rössler system is depicted in Fig. 1. In Eq. (1), three variables (x, y, z) that develop in the continuous time t and having three parameters (a, b, c). Figs 2, 3 and 4 represent the graphs of x, y and z variables of Rossler system, respectively. Initial conditions are given as:

$$x(0) = x_o, y(0) = y_o, z(0) = z_o$$

where x_o, y_o, z_o are constants.

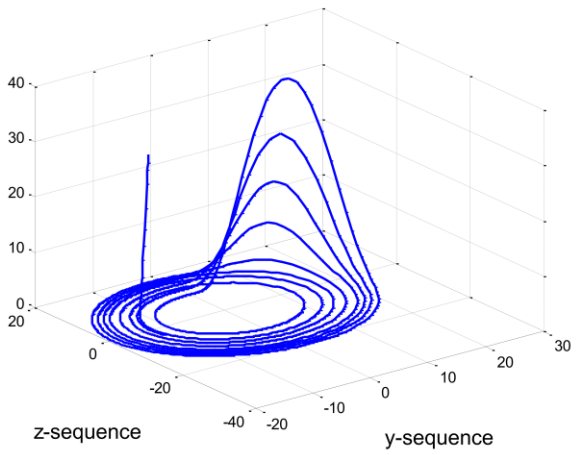


Fig. 1: The Rössler system with values of parameters a=0.1, b=0.1, c=14.

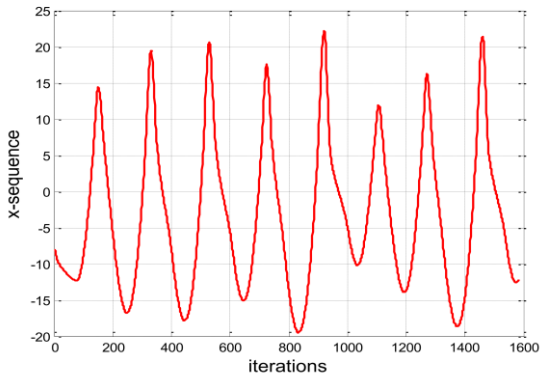


Fig. 2: The Rössler system for x along t-axis for a=0.1, b=0.1, c=14.

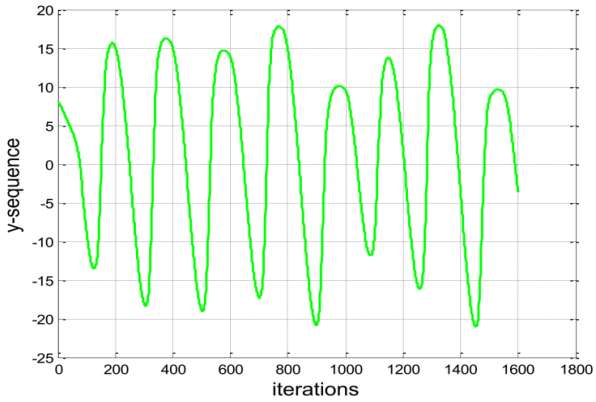


Fig. 3: The Rössler system for y along t-axis for b=0.1, c=14.

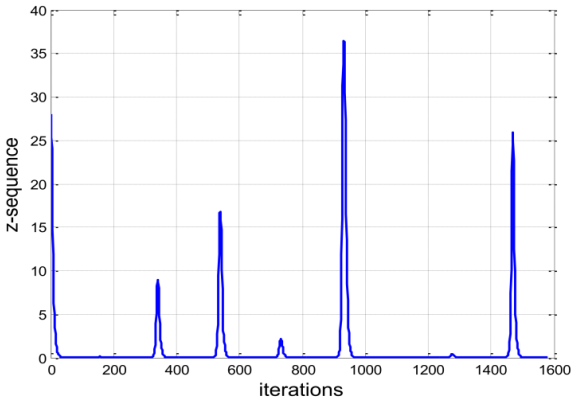


Fig. 4: The Rössler system for z along t-axis for a=0.1, a= 0.1, b=0.1, c=14.

The space plots obtained from the equations represented in (1) are given in Fig.s 1, 2, 3 and 4. Here the parameters are a=0.1, b=0.1 and c=14. The intervals range in the state of the system are $0 \leq x \leq 1600$, $0 \leq y \leq 1600$ and $0 \leq z \leq 1600$. The Rossler system shows chaotic performance for the particular parameters and intervals.

5.4. Construction of Fractional Chaotic S-box and Watermarking Algorithm

In Fig. 5 the algorithm of the chaos based S-box design and watermarking by using frequency domain is presented. In symmetric key cryptography, S-box is counted as one of the basic components. In all-purpose, an S-box takes p input bits and convert them into q output bits. We say it as $p \times q$ S-box and is shown in Table 1. These S-boxes are vigilantly selected to defend against linear and differential cryptanalysis. The outcome of Rössler's system creates the trajectories and dimension of the system indicate the total number of orbits. The sensitivity of initial conditions is of great importance to produce chaos. MATLAB is operated to get the solution of the chaotic system equations. In order to construct the fractional S-box which alternate 8 bits of data, every trajectory is sampled at 8-bit resolution and in this way, we achieve 256 different values whose range is from 0 to 255. Table 1 represents the values of S-box attained by the proposed fractional system. The behavior of chaotic trajectories of the Rössler system in $\boldsymbol{xy}$ plane is depicted in Fig. 1. By making codes in Matlab the answers of S-box are achieved from the preferred trajectories having specific initial conditions. As we know, the dynamical systems sensitivity to initial conditions, we selected conditions with immense effort to get chaos. The trajectories are attained from 1000 data samples. By substituting watermark image values with the help of chaotic fractional S-box we obtain the altered watermark image. Now to embed altered watermark image in host image we have options in the form of spatial and frequency domain. Because of not as much of robustness ability of spatial domain against dissimilar attacks it may not be capable to protect image processing attacks although it has the capacity of hiding data around 6.25%.

Table 1: S-box obtained with the help of chaotic fractional S-box

224	25	191	122	65	3	219	61	12	134	157	26	149	39	181	229
216	18	186	118	62	28	158	150	179	58	139	127	30	235	29	99
208	11	182	115	56	80	209	87	9	20	121	21	199	123	6	100
201	5	177	112	53	197	55	1	225	239	117	188	10	97	174	204
194	254	173	108	51	228	109	222	147	203	113	232	27	24	43	178
167	248	169	105	49	4	163	183	32	166	116	67	85	176	120	7
144	242	164	101	47	37	217	142	250	131	119	211	255	82	227	143
124	237	160	98	45	141	14	75	212	61	136	213	90	40	244	170
107	231	156	94	44	253	72	2	135	218	145	13	19	15	187	153
93	226	152	91	60	36	185	180	95	155	165	233	38	54	175	104
81	220	148	88	79	76	240	96	17	238	221	42	241	128	151	193
69	215	140	84	92	202	48	16	234	162	0	172	70	190	130	243
59	210	137	78	103	246	110	189	154	138	63	245	46	223	64	8
50	205	133	74	195	34	132	146	114	206	86	247	23	73	106	77
41	200	129	71	214	125	52	102	35	192	111	89	184	230	83	207
33	196	126	68	236	171	159	57	252	168	251	22	66	31	249	198

On contrary, in the spectrum- (or frequency) domain watermarks are inserted in coefficients of the transformed image. We have the options of discrete Fourier transform (DFT) discrete cosine transform (DCT), discrete wavelet transform (DWT) and so on. The embedding scheme of watermarking into the low or middle frequencies, the whole image examines the change due to all over the allocation of the watermark as greater part of the energy lies in the low-frequency components. Here, we will apply discrete Fourier transform on the host image and then embed the watermark in the frequency coefficients of the image.

5.4.1. Discrete Fourier Transform

An image is counted as a spatially varying function which is decomposed into orthogonal functions with the help of Fourier transform so spatial intensity image may transform into the frequency domain. For phase modulation between watermark image and its carrier, we may use discrete Fourier transform (DFT) visual effect along with robustness against noise attack. Mathematically, the pair of equations (5.2) and (5.3) given below represents DFT and inverse DFT respectively**.**

$$F(u,v) = \frac{1}{MN}\sum_{X=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)exp\left[-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right] \tag{5.2}$$

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)exp\left[j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)\right] \tag{5.3}$$

Where $F(u,v)$ and $f(x,y)$ are named as Fourier transform pair.

Algorithm

A.1: By using initial conditions and chaotic parameters, S-box is obtained from the solution of the Rössler system by mapping each output of x values of numerical solutions in the range from 0 to 255.

A.2: From the values of watermark image pixels, we generate the indices of the S-box. Values from these indices location are replaced with corresponding original values of image pixels.

A.3: The chaotic y-sequence of Rössler system identify the embedding positions of S-box

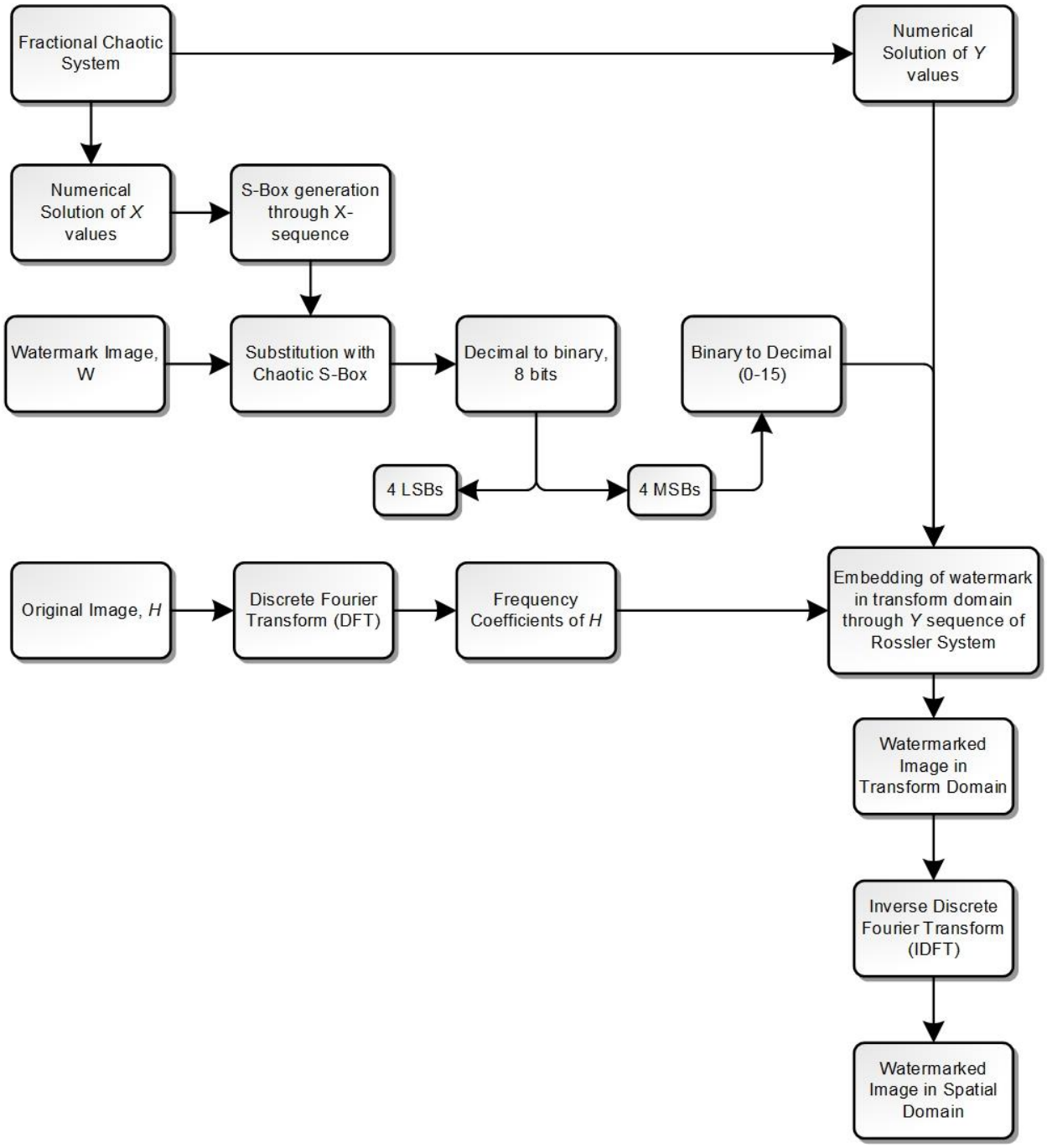


Fig. 5 Flow chart of algorithm

substituted watermark into frequency coefficients (obtained by discrete Fourier transform) of the Host image.

A.4: Lastly, the watermark image is attained by using inverse Fourier transform.

5.5. Analysis of S-box

The evaluation of fractional S-box evaluates its efficiency and strength [55], [56]. We analyze proposed chaotic system generated with the help of Rössler system in section 3. Among different available tests, we selected nonlinearity, strict avalanche criterion, bit independence criterion (BIC), linear approximation probability (LP), and differential approximation probability (DP). Different results indicate that the S-box approximately fulfill all the parameters near to optimal values.

The avalanche effect is viewed if more or less half output bits have changed results due to single input deviation and owing to this output bits transform the entire substitution-permutation system view the series of variations [57]. The outcomes of the strict avalanche criterion are shown in Table 2.

Table 2 Strict avalanche criterion analysis of chaotic fractional S-box

0.5078	0.5234	0.5000	0.5078	0.4609	0.5000	0.5000	0.5313
0.5000	0.5234	0.4766	0.5078	0.5000	0.5000	0.5313	0.4688
0.5000	0.5234	0.5000	0.5078	0.5000	0.5078	0.5000	0.5000
0.5000	0.5000	0.5234	0.5078	0.4609	0.4922	0.4688	0.5000
0.5000	0.4766	0.5000	0.4922	0.5000	0.5078	0.5000	0.5000
0.5000	0.5234	0.5234	0.5000	0.4609	0.4922	0.5313	0.4688
0.5000	0.5234	0.5000	0.5078	0.5000	0.5078	0.5313	0.5000
0.5000	0.5000	0.4766	0.5078	0.4609	0.5000	0.5000	0.5000

The BIC is analyzed if some of its input bits remain unchanged. This adjustment of input bits and the avalanche vectors independent performance of pair wise variables are the assets of this

criterion. Non-linearity represents the bits which are modified in the truth table to attain the least distance from the set of affine function. The value of nonlinearity of new S-box is 102.5.

Table 3 The nonlinearity of BIC of chaotic fractional S-box

0	106	106	104	104	102	108	98
106	0	106	106	104	106	100	100
106	106	0	104	104	104	104	100
104	106	104	0	102	106	102	102
104	104	104	102	0	106	104	108
102	106	104	106	106	0	104	104
108	100	104	102	104	104	0	102
98	100	100	102	108	104	102	0

Table 4 BIC of SAC analysis of chaotic S-box

0.5123	0.5011	0.5190	0.5145	0.5056	0.5011	0.5045	0.4911
0.5246	0.5000	0.5022	0.4955	0.4754	0.4955	0.5078	0.4900
0.4911	0.4888	0.4911	0.4955	0.4911	0.5000	0.4989	0.5123
0.4922	0.5056	0.4922	0.4989	0.4944	0.5033	0.5000	0.4911
0.5089	0.4978	0.4911	0.4821	0.4911	0.5000	0.4944	0.4944
0.5067	0.5067	0.4866	0.5067	0.5045	0.4955	0.5089	0.5112
0.5145	0.5011	0.5033	0.4989	0.4900	0.4967	0.4944	0.4833
0.5112	0.5089	0.5134	0.5000	0.4933	0.5045	0.5011	0.4810

The highest value of the disproportion of an event between input and output bits is enumerated by linear approximation probability. Differential approximation probability is a unique uniform

mapping which gives output of yi for input differential Δxi.From Table 5 we observed the values of differential approximation probability of proposed S-box.

Table 5: Differential approximation probability of chaotic fractional S-box

6	6	8	6	6	8	8	6	6	6	6	6	8	6	6	8
6	6	6	6	8	6	6	8	6	8	8	6	8	6	8	8
8	8	10	8	6	6	6	6	6	6	6	6	8	8	8	6
6	6	6	10	6	6	6	6	8	6	6	6	6	8	6	6
8	8	6	6	6	8	8	8	6	6	8	6	6	8	6	8
6	6	6	6	6	8	6	6	6	8	6	6	8	6	8	8
6	10	6	8	6	6	8	6	8	6	8	8	8	6	8	10
6	8	6	6	6	6	8	6	6	6	6	6	6	8	6	6
6	6	6	8	8	6	6	6	6	6	8	8	6	10	6	8
6	8	6	4	8	8	8	8	6	6	6	6	8	8	8	8
6	8	4	6	6	6	8	8	6	6	8	6	8	6	8	8
8	8	8	6	8	4	6	8	10	8	8	6	8	6	10	6
8	6	6	10	6	6	8	8	6	6	6	8	8	8	6	6
6	6	8	8	6	6	8	8	6	6	6	6	6	6	8	6
6	6	6	8	8	6	6	6	6	8	6	6	6	6	8	6
6	8	6	8	8	8	6	6	6	6	8	6	6	6	8	256

5.6. Simulated Results and Statistical Analysis

It is essential to judge the both original image and watermarked image by using available statistical analyses. In this chapter, we look at images with the help of homogeneity, correlation, energy, contrast, entropy, mean square error and peak signal to noise ratio. To find out the security of

images the analyses are made on 256×256 Host images of Lena, baboon and pepper and 50×50 watermark image.

5.6.1. Comparison of Statistical Analysis

The proposed technique employed chaos with the frequency domain embedding of the watermark. This approach is new and has certain advantages over the previous works. Moreover, the proposed work has been compared with one of the states of art techniques that uses almost the same methodology [54].The comparison is given in Table 6

Table 6 Statistical Analysis Original Image and Watermarked Image

Statistical Analysis	**Pepper**			**Lena**			**Baboon**		
	Host	**Proposed**	**Ref.** [54]	**Host**	**Proposed**	**Ref.** [54]	**Host**	**Proposed**	**Ref.**
Homo.	0.8902	0.8902	0.8901	0.8651	0.8811	0.8601	0.7294	0.7294	0.7298
Contrast	0.3311	0.3311	0.3318	0.4141	0.3371	0.4221	1.0004	1.0004	0.9993
Energy	0.1330	0.1330	0.1317	0.0942	0.1130	0.0920	0.0817	0.0817	0.0825
Entropy	7.5612	7.5613	7.4105	7.7021	7.7023	7.5121	7.3903	7.3903	7.4602
Corr.	0.9207	0.9207	0.9219	0.9444	0.9443	0.9383	0.6607	0.6607	0.6593

The results of MSE and PSNR tests for pepper, lena and baboon images are given in Table 7. Moreover, Fig.6 represents the host image, watermark, substituted watermark (substituted with S-box) and watermarked image respectively.

Table 7 MSE and PSNR values of proposed watermarking technique

Image	**MSE**	**PSNR**
Pepper	15.7216	81.9777
Lena	10.5413	86.2234
Baboon	4.8876	91.4512

Host image Watermark substituted watermark watermarked image

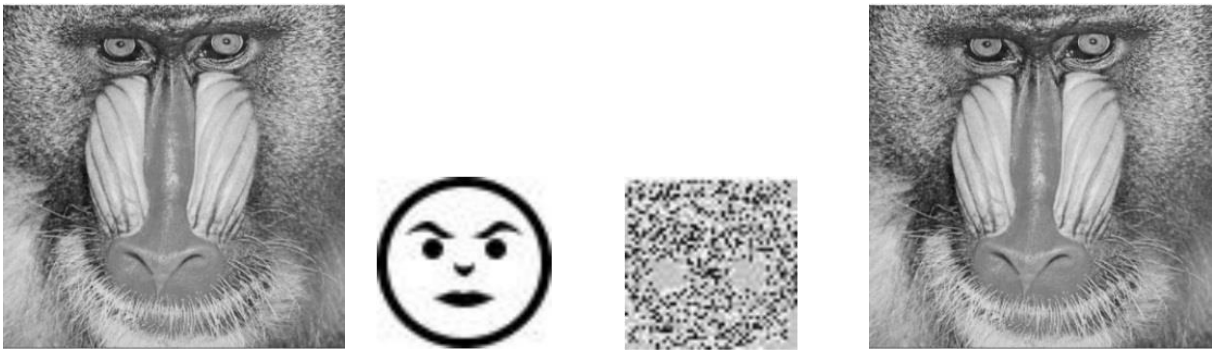


Fig.6 Pictorial results of proposed Embedding and Extraction of Watermarking Technique

5.6.2. Extraction of watermark

The basic idea of inverse proposed watermark algorithm is authentication. Watermarked image shown in Fig. 7 follows the inverse process and the watermark image is extracted. Moreover, inverse substitution is on the card because the extracted watermark image is substituted by the proposed chaotic S-box to attain original watermark**.**

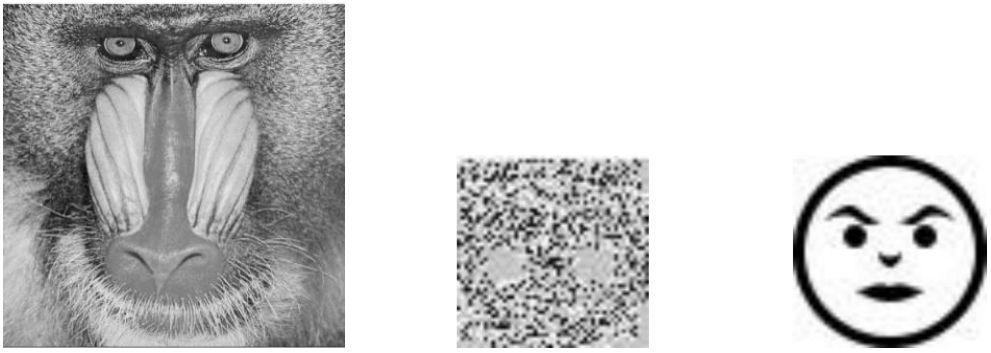


Fig. 7: Pictorial representation of the extracted image, substituted watermark and watermark images.

5.7. Robustness Test Based on Image Processing Operations

The numerical estimate of two watermarks is the similarity of extracted and original watermark, Cox et.al. [58]. The High correlation between two watermark images guarantees the robustness of the watermarking algorithm. In addition to this, if the value is on the higher side, it represents the more correlation between two watermark images. It is given as:

$$Sim = \frac{\sum t_i . s_i}{\sqrt{\sum t_i^2 . \sum s_i^2 .}} \qquad qa$$

where $\boldsymbol{t_i}$ and $\boldsymbol{s_i}$ represent the corresponding $\boldsymbol{ith}$ element of extracted and original watermark respectively. The perfect correlation between extracted and original watermark is observed by seeing the numerical value of confidence measure which is 98.09. With the help of certain image processing operations on the watermarked image and on the extracting watermark we may have the better idea of similarity.

We consider and add salt and pepper noise to check the noise attack on our watermarked image. Among different compression attack, we consider the Joint Photographic Experts Group (JPEG)

for our proposed algorithm. If extracted image is disfigured or giving fewer information then this is count as an example of cropping attack. Fig. 8 depicts compression, noise and cropping attack on our scheme and outcomes are given in Table 8.

Table 8 Confidence measure values of selected images against different image processing attacks

Attacks	**Pepper**	**Lena**	**Baboon**
Compression	71.5691	71.2982	69.2561
Noise	75.9812	76.1256	74.3253
Cropping	41.3694	44.5197	42.1582

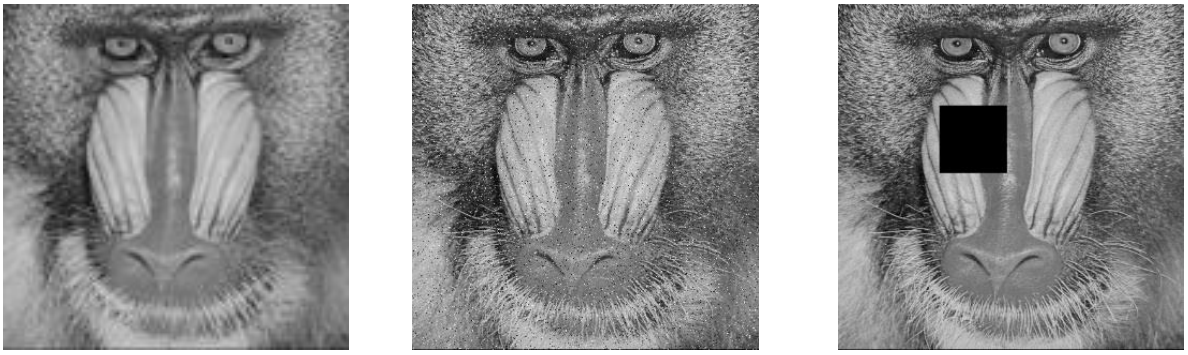


Fig. 8: Image Processing Effects on Baboon image.

This new idea shows the importance of utilization of the chaotic system of differential equation for synthesis of S-box in watermarking. The embedding of the watermark (secret signature) has been done in the frequency domain of the original image whose copyrights must be protected. The embedding positions are defined by the random values generated with the help of chaotic map. We use the algebraic S-box in a watermarking scheme to make our scheme robust in the next chapter.

Chapter 6

Frequency domain watermarking based on algebraic S-box

This chapter presents a new and comparatively secure watermarking technique, in the frequency domain. Our scheme deploys a local ring-based S-box. The algebraic algorithm used to synthesize S-box basically exploits one-one correspondence between the multiplicative group of units of the local ring $\mathbb{Z}_{512}$ and the Galois field $\mathbb{F}_{256}$. This S-box has high confusion creating capability due to the structural properties of the local ring and fulfills the necessary requirements to be reliably used in multimedia applications. We use this S-box in a watermarking scheme to make our technique more confusing and secure to provide more support in copyrights protection strategies. The proposed non-blind digital watermarking technique deals with the application of discrete cosine transform (DCT) in the frequency domain which is comparatively more robust than spatial domain techniques. In the proposed scheme, first the watermark image is substituted through the S-box, and the scrambled watermark is then embedded in the DCT-transformed host image. To measure the strength of the proposed technique, simulation results and statistical analyses are made. Most significant analyses techniques including measures of homogeneity, energy, contrast, entropy, correlation, Mean squared error (MSE) and peak signal to noise ratio (PSNR) are applied which show coherent results.

6.1. Introduction

Among the aforementioned types of watermarking, spatial domain algorithms offer more capacity to insert watermark but as far as robustness is concerned, frequency domain watermarking is a preferably used technique (see [59] for more details).

Several methods for digital watermarking in the frequency domain are available in literature including Discrete Fourier Transform (DFT) [60], Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fractional Fourier Transform (DFRFT) [61]. We, in the proposed framework, apply the Discrete Cosine Transform method to get robust watermarking. It is safe from annoying blocking artifacts as it is not a block-based transform and offers a high degree of freedom for embedding due to its multi-resolution property. DCT may be used with the combination of other transforms to obtain maximum advantages of the properties of other transforms [62], [63].

DCT-based watermarking algorithms have been widely studied [64], [65]. Recently Zhang et. al. [66] anticipated a digital watermarking scheme using DCT, that involves two preprocessing steps (before watermark embedding); changing the size of the watermark and scrambling it. However, our proposed method achieves the security targets by using a comparatively simple, direct and more secure approach as compared to [66]. This algorithm is distinguished from the previous work in two senses; firstly, it enhances the security level by utilizing the S-box, secondly, the structural properties of the used local ring contribute to elevating the imperceptibility level of our technique. Construction of stronger S-boxes is considered as a major focus of recent research as in the last few years S-boxes gained attention in further multimedia applications as well [7], [67].

In this chapter, we introduce an application of S-box in digital watermarking in the frequency domain using DCT method. For the construction of our S-box, we utilize the structure of a local

ring $\mathbb{Z}_{512}$ of size 512 which has a multiplicative subgroup of cardinality 256, formed by the unit elements. The bijection between the group of units and the Galois field $\mathbb{F}_{256}$ leads us to formulate a new S-box by applying a specific map in the corresponding field. This values of S-box are substituted with watermark before the embedding process. By the involvement of S-box, our technique becomes highly secured against any plagiarism and copyright violations. The substituted watermark image is embedded in the DCT- transformed host image, and the watermarked image is achieved by utilizing the inverse DCT. The algorithm for the extraction of the watermark is also discussed which shows non-blind watermark technique.

6.2. Construction of S-Box

In this section, the algebraic algorithm used to structure new S-box. In chapter 2 of this thesis, a construction method of an 8×8 S-box over the elements of units of the integer modulo ring $\mathbb{Z}_{512}$ is given. The construction of proposed S-box with different parameters as of reference depends on 3 major's steps; calculation of multiplicative inverses of the elements of the group of units $U(\mathbb{Z}_{512})$, then the construction of pseudo S-box based on $U(\mathbb{Z}_{512})$ and in the last step defining the one-one correspondence between $U(\mathbb{Z}_{512})$ and $\mathbb{F}_{256}$. Consequently, 256 distinct values of S-box are obtained [68].

We define bijective correspondence between $U(\mathbb{Z}_{512})$ and $\mathbb{F}_{256}$ by

$$l(2t+1) = \frac{33t+23}{12t+9}, \tag{6.5}$$

where $0 \leq t \leq 255$. The fraction on the left side of Eq. (6.5) is evaluated by expressing each number in 8-bits format such as 33=00100001, 23=00010111, 12=00001100 and 9=00001001. Table 1 gives the 256 values of proposed S-box.

Table 1: Proposed S-box

95	228	190	139	255	0	175	241	43	8	66	70	125	62	245	119
250	181	158	214	96	100	44	53	192	73	178	17	187	135	246	161
122	206	234	149	106	99	133	235	51	212	211	170	7	93	91	27
205	86	89	67	63	243	182	13	87	77	16	160	41	20	237	167
117	15	24	146	252	216	166	200	213	46	196	152	113	115	42	209
137	111	147	1	2	31	206	194	3	240	148	164	239	21	184	154
189	281	84	143	110	35	220	253	132	61	108	244	247	9	50	208
39	10	112	236	54	126	199	203	33	159	186	72	11	165	222	28
140	155	0	59	30	58	174	79	251	157	142	34	45	6	105	173
151	83	40	101	215	231	123	130	121	59	207	36	204	202	116	62
82	248	78	180	185	176	14	198	22	193	226	156	127	75	218	94
109	12	134	57	76	150	232	230	163	224	177	183	179	32	10	223
141	128	120	48	47	254	153	103	52	69	85	5	238	201	25	197
145	90	107	74	64	249	60	131	18	38	97	168	124	210	104	136
71	162	92	217	169	98	227	129	81	65	37	191	219	68	188	19
242	49	88	23	55	29	229	171	144	149	233	221	138	56	190	114

6.3. Performance Analysis of the Proposed S-box

In this section, the essential performance parameters are inspected for the newly generated S-box. The assessment of the projected S-box guarantees its competence and strength [18]. In this article, best available tests are selected to assure the perfomance of the S-box. It includes bit independence criterion (BIC), linear approximation probability (LP), differential approximation probability (DP), nonlinearity, bit independence criterion (BIC) and strict avalanche criterion. It is proved that

the new S-box fulfills all the requirements to be used in further applications. The subsections below describe the required properties in detail.

It is the highly-desired property of an S-box that single input deviation produces series of variations in the substitution- permutation network [22], [69].

Table 2: Results of algebraic analysis for the new S-boxes

S-box	BIC	SAC	BIC/SAC	DP	LP	Bijective
Proposed S-box	103.25	0.503906	0.504	0.046875	160/0.1406	yes

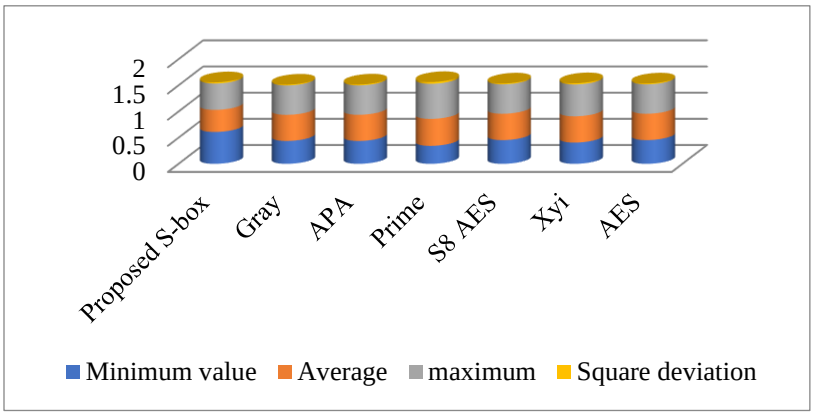


Fig. 1: Comparison of Strict avalanche criteria for various S-boxes

Table 2 shows the results of strict avalanche criterion and Fig. 1 provides the comparison of the new S-box with the prevailing S-boxes such as Gray, APA, residue prime, S8, Xyi and state of the art, AES S-box. The average value of the strict avalanche criterion comes out to be 0.5039.

The independent behavior of the pair of variables and the variations of input bits are considered as important factors of bit independence criterion. In bit independence criterion, input bits are transformed exclusively, and then output results are studied for their independency [22], [55], [69]. Table 1 presents bit independence of nonlinearity and Fig. 2 is a pictorial representation of the comparison of numerical results of BIC applied on different S-boxes.

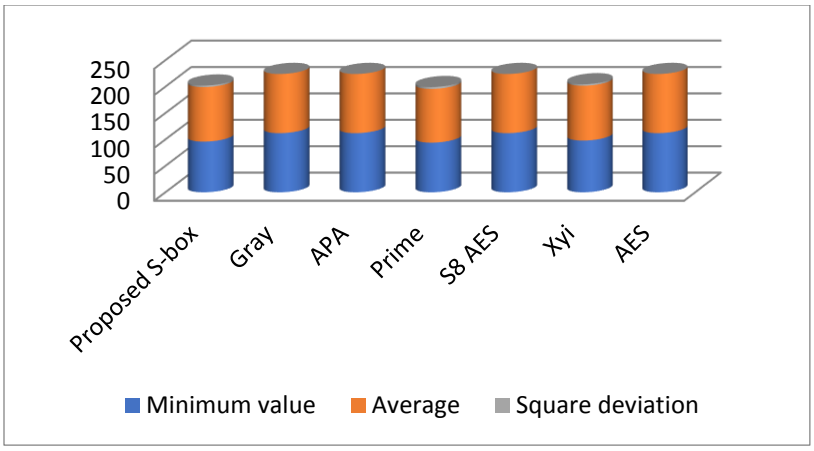


Fig. 2 Bit Independence Criterion of various S-boxes

Nonlinearity analysis measures the distance of the reference function from all of the affine functions. For more details and calculation process see[70]. The average nonlinearity of our S-box is 103.25 that is reasonably acceptable. Fig. 3 is the graphical representation of the nonlinearity comparison.

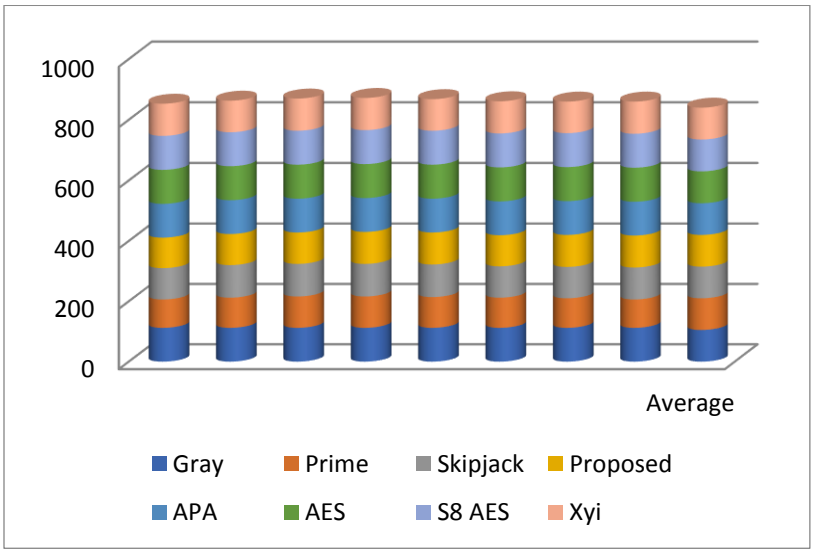
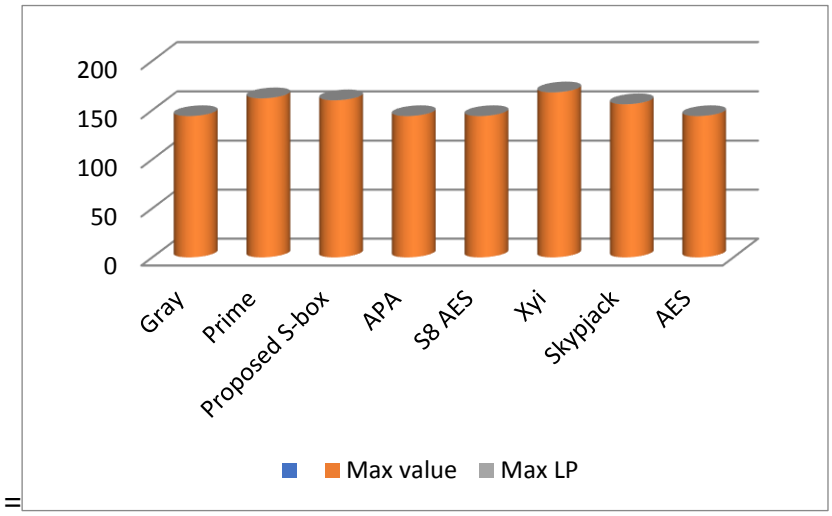


Fig. 3: Nonlinearity of proposed and other S-boxes

The unevenness of an event is calculated in linear approximation method. The Linear approximation probability of the proposed S-box is 0.1094. It is evident from these results that our

S-box gives confrontation to different linear attacks. In fig 4, the graphical representation of the linear approximation of proposed S-box and different S-boxes is given.



=

Fig. 4: Comparison of Linear approximation probability

We depend on the differential approximation probability test which concludes the differential uniformity confirmed by an S-box.

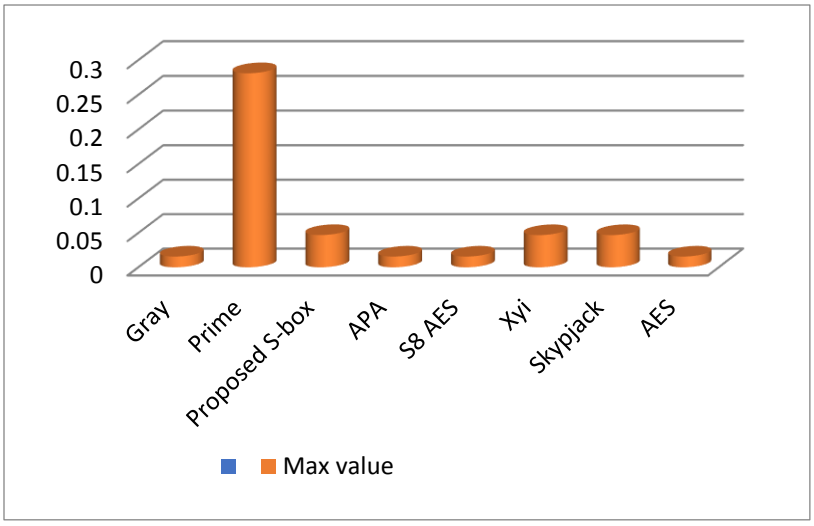


Fig. 5: Comparison of differential probability of different S-boxes

The results of odds of differential by applying input and output differentials are given in Table 1. The graphical analyses of proposed S-box and some well-known S-boxes are also shown in Fig. 5.

6.4. Algorithm of Frequency domain Watermarking Technique

The flow chart of the new technique of watermarking using S-box and frequency domain watermarking is depicted in Fig. 1. By utilizing the multiplicative subgroup of unit elements $U(\mathbb{Z}_{512})$ of the local ring $\mathbb{Z}_{512}$, a new S-box which depends on the special algebraic structure of a local ring and its relationship with the Galois field. The newly developed S-box possesses reasonably acceptable performance indices as discussed in the previous section. By the help of this S-box, we substitute the watermark image first. This altered and secured watermark is embedded into the DCT-transformed version of the original image. In the frequency domain, almost all portions of image observe the change as the watermark is inserted in low or middle frequencies and low-frequency components contain the larger portion of energy. Due to special features of discrete cosine transform, we are applying the frequency domain technique using DCT.

Fourier series provides us the establishment of various transforms including discrete cosine transform (DCT). DCT converts an image to the frequency domain by compression which is obtained through data quantization. This transform only uses the real part of the Fourier complex kernel and neglect complex part. The information of the original image is concentrated into the smallest low-frequency coefficient with the help of 2D-DCT. Moreover, due to this transformation, the effect of image blocking is minified, which shows the good interaction between the information centralizing and the computing complications. The embedding process is strengthened with the help of secure S-box and this altered watermark is then embedded into the DCT-converted host image. For extraction of the watermark, the original host image is needed as it is the non-blind

technique of frequency domain. Fig. 6 and 7 represent the process of embedding and extraction of the watermark respectively.

6.4.1. Embedding and Extraction of Watermark

Let the host image is of size $H1 \times H2$ and is given by $H = \{h(x,y), 1 \leq x \leq H1, 1 \leq y \leq H2\}$ whereas, the watermark image is of size $W1 \times W2$ be denoted as $W = \{w(i,j), 1 \leq i \leq w1, 1 \leq j \leq W2\}$ and (x,y), (i,j) show the pixel coordinates of original host image and gray watermark image respectively, If P denotes the total number of binary bits of gray level image pixels than $h(x,y)$ and $w(i,j)$ is given by $\{0, 1, \ldots, 2L-1\}$. The substitution of the frequency domain is almost same as that in spatial domain with an exception that the watermark is embedded into frequency coefficients of the transformed image. In this article, the scheme becomes more secure as the watermark is substituted with algebraic S-box.

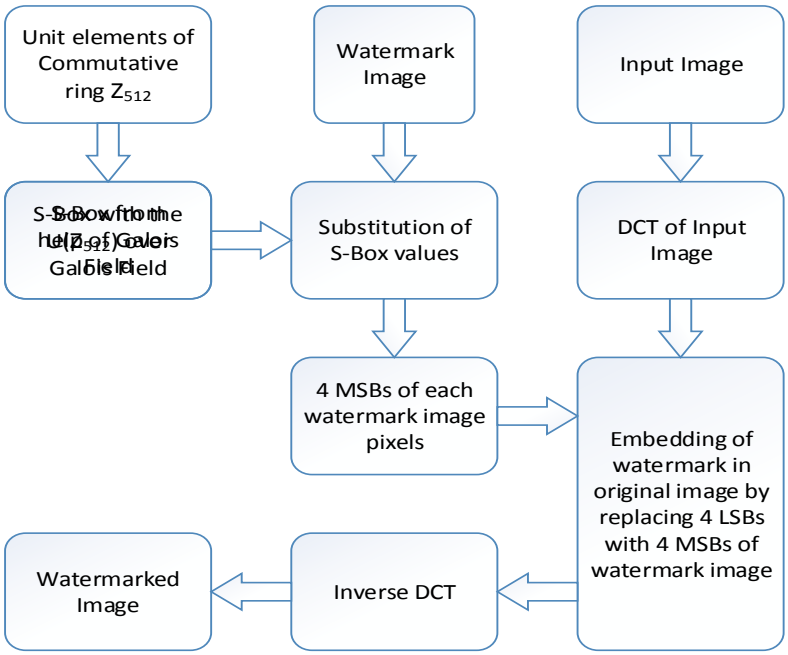


Fig. 6: Embedding of S-box substituted watermark in original image

This provides more strength to our technique and copy right protection to support our claim at any forum. The watermark is then inserted into DCT-transformed image where we consider positive integral parts of DCT coefficients (neglecting the sign of negative DCT coefficients) and replace the LSBs of DCT coefficient with MSBs of the altered watermark. After applying IDCT on the result we attain the final watermarked image.

In embedding scheme, the S-box is another hidden truth to counterfeit any plagiarism attempt. Moreover, this provides a strong mathematical foundation to our technique**.** The pictorial representation of embedding and extraction procedure of this novel scheme is given in Fig. 8. The gray level images of Lena, Baboon and Peppers respectively are selected as host images. The watermark is substituted with proposed S-box and depicted in fig 9. After embedding the substituted watermark into host images (DCT is applied on host image), the watermarked images of Lena, Baboon and Peppers, are given in Fig 8. The visual results witness that the final watermarked images have the identical appearance as in Fig. 8 of the original images. Following the inverse process of embedding, it is possible to extract the watermark image from the host image. The watermarked image is then subjected to DCT and extraction of the original image is done by replacing 4 LSBs of DCT watermarked image with original values. By this process, we can remove the watermark from the original image. The extraction procedure requires the inverse S-box algorithm as well. Fig. 11 represents the extracted S-box substituted image and successfully extracted watermark. The extracted original images of Lena, baboon and Peppers are represented in Fig. 10.

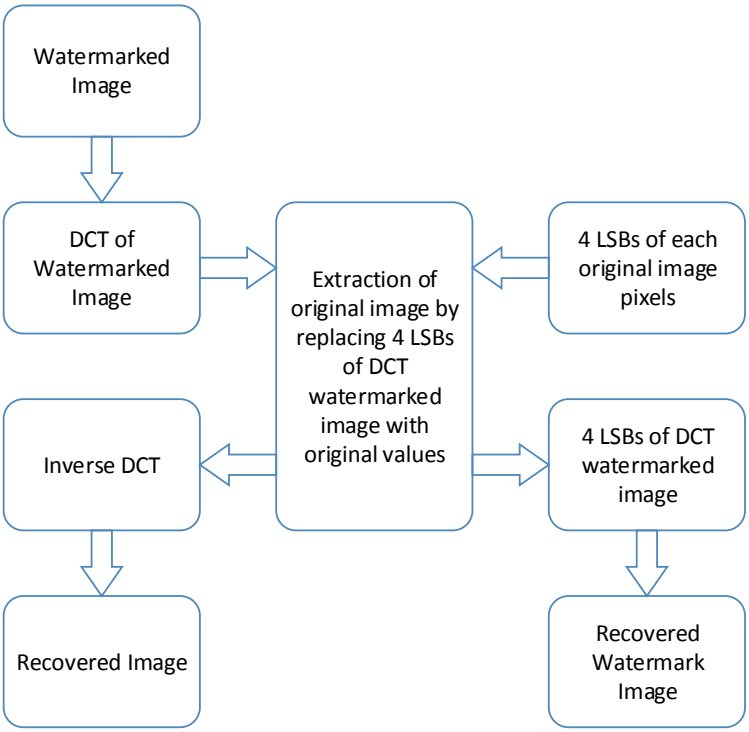
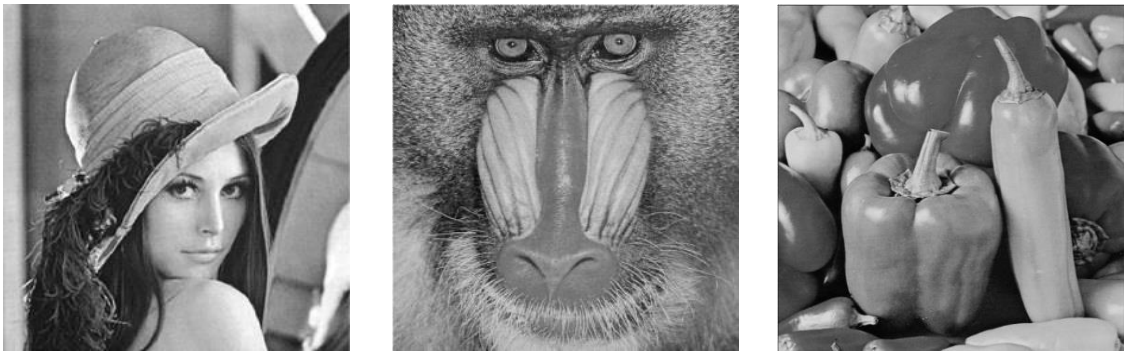


Fig. 7: Extraction of watermark from watermarked image

Host Images

(a) Lena (b) Baboon (c) Pepper



Watermarked images

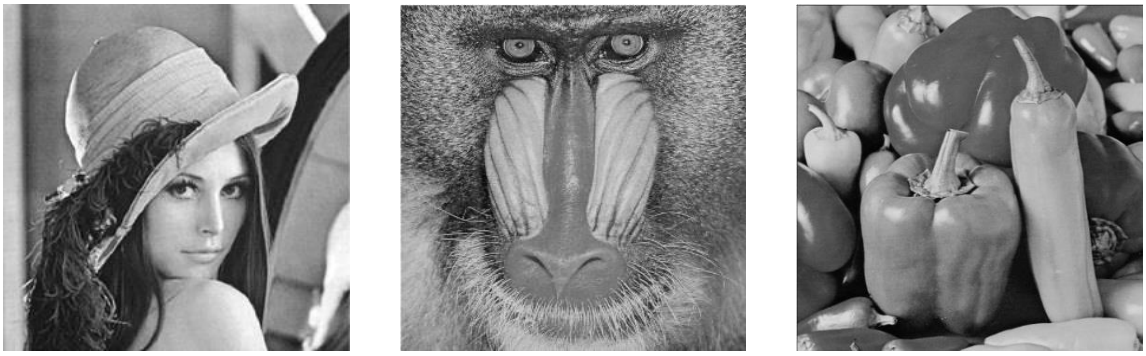
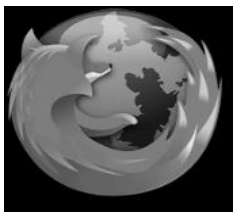


Fig. 8 Host and the watermarked images

watermark



Substituted watermark

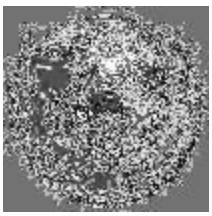


Fig 9: Original and the substituted watermark

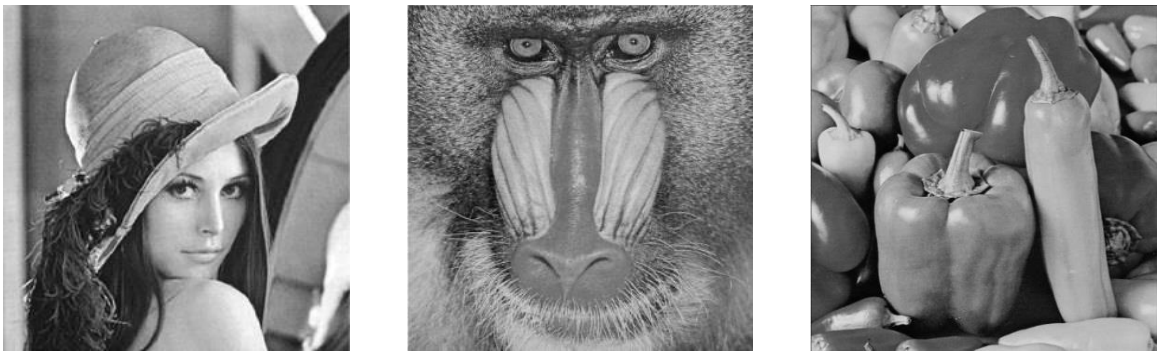
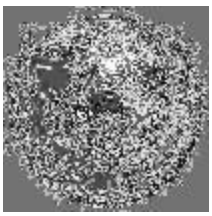


Fig. 10: Extracted images of Lena, Baboon and Pepper

Substituted watermark



Extracted watermark

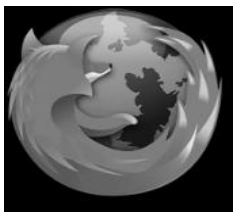


Fig. 11: Substituted and the Extracted watermark

6.5. Simulation Results and Statistical Analysis

The assessment of both the host image and the S-box substituted, watermarked image with certain statistical tests is performed in this section. We perform frequently used tests including

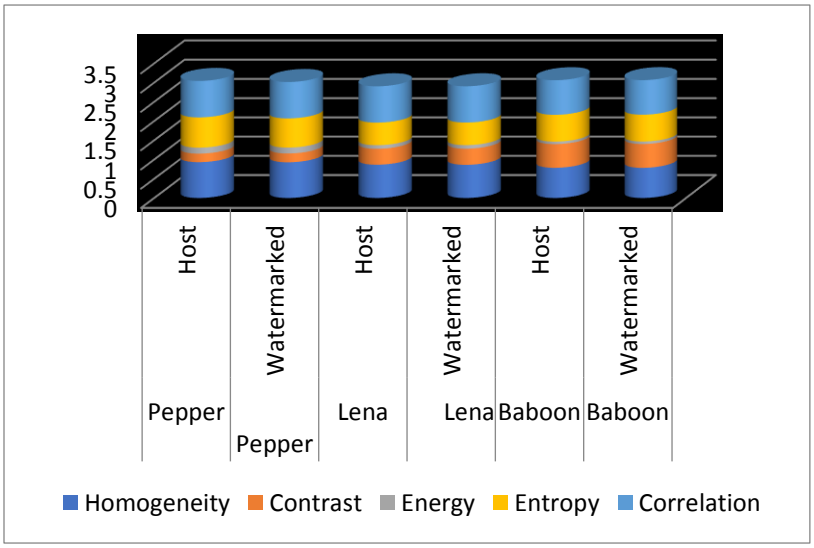


Fig. 12: Comparison of MLC for different Images

homogeneity, contrast, correlation, entropy, energy, mean square error and peak signal to noise ratio on both the images. The outcomes of above-mentioned analyses are presented in Table 3 and Fig. 12.

Table 3: Statistical Analyses of Host Image and Watermarked Image

Statistical	Pepper	Pepper	Lena	Lena	Baboon	Baboon
	Host	Watermarked	Host	Watermarked	Host	Watermarked
Homogeneity	0.9317	0.9279	0.8651	0.8625	0.7848	0.7839
Contrast	0.2219	0.2295	0.4141	0.4194	0.6159	0.6194
Energy	0.1560	0.1537	0.0942	0.0934	0.0655	0.0653
Entropy	0.7856	0.7579	0.5859	0.5859	0.6962	0.6962
Correlation	0.9484	0.9467	0.9444	0.9437	0.8994	0.8989

These analyses are made on 256 x 256 image of Lena, baboon and pepper along with 50 x 50 watermark image.

The dissimilarity between two digital images is calculated with the help of the mean squared error. The logarithm of the ratio between the signal strength and difference between the images (MSE) gives peak signal to noise ratio Table 4 gives the result of MSE and PSNR results.

Table 4: MSE and PSNR values of proposed watermarking technique

Image	MSE	PSNR
Pepper	1.4786	46.4814
Lena	1.4665	46.5741
Baboon	1.4644	46.4742

6.5.1. Complexity Analysis

For the application of the proposed technique, the most important factors are the improved security and the embedding, extraction speed of watermark along with the space complexity. In this regard, speed analysis is performed with the help of MATLAB 7.9.0 (R2009b) on a laptop having Windows 7 working structure, Intel(R) Core(TM) i5-2520M, CPU@ 2.50GHz and RAM of 4GB. One can see that the speed of our embedding and extraction process is pretty close to the other DCT-based schemes, however the security level attained by the proposed scheme is highly improved than the recently known techniques. The sequence of operations used for the proposed algorithm requires no additional space. Table 5 provides elapsed time for embedding and extraction of the watermark with different image sizes and picture qualities.

Table 5: Elapsed time for Embedding and Extraction of watermark

Serial No	Size	JPEG			PNG		
		Baboon	**Pepper**	**Lena**	**Baboon**	**Pepper**	**Lena**
01	**512*512**	5.3631 sec	5.3579 sec	5.6291 sec	5.4792 sec	5.4385 sec	5.6820sec.
02	**256*256**	1.7309 sec	1.2096 sec	1.7533 sec	1.6618 sec	1.9459 sec	1.9154

6.6. Robustness Test Based on Image Processing Operations

The mathematical approximation of two watermarks is the similarity between the extracted and the original watermark [58]. The numerical value for confidence measure in our simulation results is 99.92. It demonstrates the ideal correlation between extracted and original watermarks. The watermarked image and extracted watermark are gone through well-known image processing operations which are given in the following subsections. Similarity analysis of different images is given in Table 6.

Table 6: Similarity analysis of different Images

Image	SIM
Pepper	0.9964
Lena	0.9937
Baboon	0.9987

Table 7: Confidence measure values against different image processing attacks

Attacks	Pepper	Lena	Baboon
Compression	33.0563	36.4937	22.5401
Noise	18.5720	18.3259	18.7559
Cropping	30.1589	32.4309	28.0296

Compression Attack Salt and Pepper Attack Cropping Attack

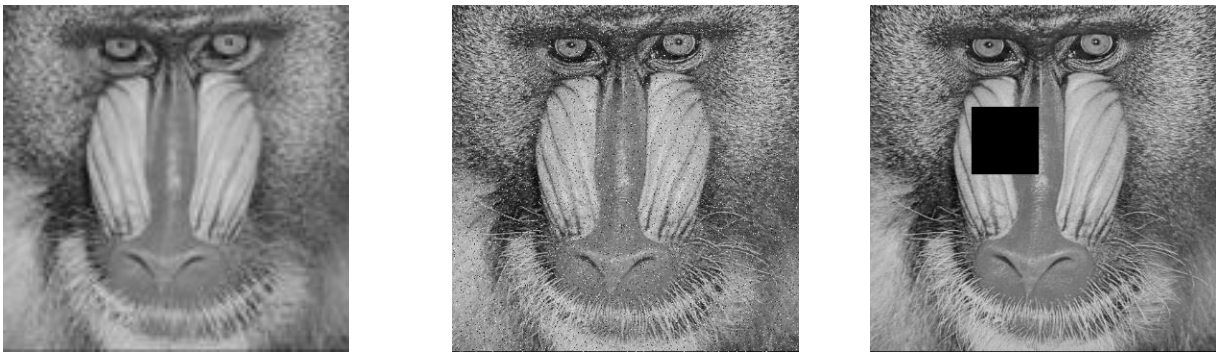


Fig. 13 Image Processing Effects on Baboon image.

In this technique**,** for noise attack**,** we add salt and pepper noise. Joint Photographic Experts Group (JPEG) is measured for compression attack. In cropping attack either extracted image is distorted or offers fewer information than the original image. The outcomes of all image processing attacks are given in Table 7 and Fig.13 represents the compression, noise and cropping attacks respectively.

In this chapter, a new idea is presented for watermarking that mainly relies on a newly designed 8×8 S-box from a local ring instead of a Galois field. The involvement of S-box in the scheme, where we substitute the values of the watermark image, not only develops confusion in understanding the used scheme but also provides more security and support to our argument for copy right protection of digital data. This technique of watermarking is based on frequency domain Discrete Cosine Transform. The complexity of the algebraic structure of the S-box and then

frequency domain technique makes almost impossible to identify watermark. In the next chapter, steganography techniques based on S-boxes are presented in the spatial domain.

Chapter 7

Steganography Technique with Enhanced Security Based on a High-Nonlinearity S-box

This chapter introduces a new scheme for digital steganography in the spatial domain. In this approach, we engage a specific high-nonlinearity S-box along with some chaotic systems, possessing enhanced chaotic range, to embed data in the least significant bits of the original image. An effective application of chaos in secure communication is presented in the proposed work. We determine the statistical strength of our steganographic algorithm through various analyses. We further evaluate the robustness of our technique against several image processing attacks. The outcomes of these analysis techniques depict that our scheme is significantly secure and can be reliably used in confidential communication applications.

7.1. Introduction

When secret information is transferred electronically, the main problem is to avoid unauthorized way to get the information. To achieve the essential security in this process many methods such as cryptography, watermarking, steganography etc. have been the major focus of research for past few years [71]–[73].

The word steganography is a combination of two Greek words, steganos and graphein, which mean "covered writing". In steganography, secret information is embedded into an unsuspecting carrier (any digital media), to avoid the unwanted attention during communication. Evidence for the use

of steganographic methods, for secret communication, are available in ancient Greek history [74], [75]. With the passage of time, more advanced techniques have been developed for steganography[71], [76]–[80]. Particularly, the advent of modern computer technology remarkably polished the skills of surreptitious communication [73], [76], [81], [82]. The wide-ranging applications of steganographic methods in computer forensics, copyright protection, broadcast monitoring, circumvention of web-censorship etc. made it an absolutely ascendant strategy in communication security [77], [80], [82], [83].

In the last decade, chaos has gained incredible importance as the most authentic source to elevate the level of security in confidential communication. Chaotic systems possess some extra ordinary features such as, irregularity and sensitivity to the initial conditions, unpredictability, speed and computational strength which distinguish these nonlinear dynamical systems in security applications [84]–[86].

7.1.1. Previous Work

Due to the exceptional properties of the chaotic maps, the study and analysis of chaos-based steganographic techniques have been quite popular. Recently it has been identified that some algorithms are susceptible to the statistical analysis [87], [88]. Steganalysis (the inverse proof steganography) seems to have increased significance [89]–[91]. This necessitates an acute evolution in steganographic methods. Recently in [72], Amir et. al. presented an effective application of one-dimensional chaotic systems in digital steganography. The authors engaged three chaotic maps; the logistic map, TD-ERCS and NCA to embed information in a spatial domain. The strategy is quite simple and efficient (for further details see section 3 of [72]). Zhou et. al.[92] proved that the combinations of one dimensional chaotic maps have enhanced chaotic

range. The authors applied these systems in image encryption applications but in literature, such systems have not been applied in steganographic methods as yet.

7.1.2. Contribution of This Work

We, in the proposed framework, ameliorate the algorithm discussed in [72] in two ways. Firstly, we increase the complexity by involving a highly nonlinear S-box to substitute information bits. Secondly, rather plain one-dimensional chaotic maps, we employ the nonlinear combinations of the chaotic maps with enhanced chaotic range as described in [92]. These two steps contribute to increase the security of the anticipated method and the analysis thus performed shows outstanding results when compared with the method discussed in [93].

7.2. Algebraic Algorithm for S-box

For better understanding of the structural properties of an S-box, it is necessary to understand few basic facts. For the convenience of our readers, the algebraic structure of the Galois field are thoroughly explained to construct an S-box. For the underlying synthesis of 8×8 S-box, we use

$$GF(2^8) = \mathbb{F}_2[x]/< p(X) >$$

with $p(X) = X^8 + X^4 + X^3 + X + 1 \in \mathbb{F}_2[x]$. is an irreducible polynomial of degree 8. It is our option that we can use any degree 8 irreducible polynomial for constructing the background field $GF(2^8)$ but this affects our calculations as the binary operations are carried modulo the used polynomial [68].

For a field $\mathbb{F}$, the general linear group $GL\ (n, \mathbb{F})$ is a group made by all $n \times n$ invertible matrices. A projective general linear group of degree n over a field $\mathbb{F}$ is defined to be the quotient group of $GL\ (n, \mathbb{F})$ by its center. For this chapter, we form the 8×8 S-box by considering the action of the

aforementioned Galois field $GF(2^8)$ on the projective linear group $PGL(2; GF(2^8))$, i.e. we take a function f : $PGL\big(2, GF(2^8)\big) \times GF(2^8) \rightarrow GF(2^8)$ defined as;

$$f(v) = \frac{az + b}{cz + d} \tag{7.1}$$

In Eq. (1), f is named as a linear fractional transformation (LFT) with $a;\ b;\ c$ and $d\ \in GF(2^8)$ satisfying the non-degeneracy condition $ad - bc \neq 0$. The algebraic complexity and nonlinearity of LFT give the incentive to employ this map for byte substitution. In our S-box we u a = 21; b = 8; c = 3 and d = 17. The images of this map provide our S-box as given in Table 1. The nonlinearity of the proposed S-box is equal to 112 which is the same to state-of-the-art AES S-box [94] but it employs a simple map rather than composition of maps as used by AES S-box [95].

7.3. One-dimensional Chaotic Maps

Literature regarding security protocols witnesses that one-dimensional chaotic maps have far-reaching applications due to the straightforward structure and computational simplicity. For the proposed study, we use three one-dimensional chaotic maps; the logistic map, the tent map and the sine map. In the following sub-sections, we discuss the fundamental properties of these three maps.

7.3.1. The Logistic Map

The most commonly used 1-D chaotic map is logistic map which have the simplest structure [92]. Its defining equation is simply a quadratic recurrence equation stated as,

$$\mathcal{L}(\mu, x_i) = x_{i+1} \ = \ \mu x_i(1 - x_i); \tag{7.2}$$

where $\mu \in (0, 4]$. Change in the value of the parameter, μ changes the behaviour of the map. We, therefore, may call μ the *catalyst* for chaos. In the study of dynamical systems, its quite interesting

to see the bifurcation pattern. It is clear from the bifurcation diagram (as shown in Fig. 1(a)) that $\mathbb{L}$ produces the chaotic effect for $\mu > 3.56995$. One can see that the Logistic map, though most markedly used map, unfortunately, has a limited chaotic range [3:56995; 4].

7.3.2. The Tent Map

The tent map is another example of most commonly used discrete dynamical systems. It is defined by a piecewise linear function given below and discussed in section 4.2.1 of this work. The bifurcation diagram of the tent map, Fig. 1(b), shows that for the parameter values $\lambda \in (2,4]$ the map has chaotic effect.

7.3.3. The Sine Map

The sine map is defined in section 4.2.2 of this thesis. The sine map has a chaotic behavior similar to the logistic map. The bifurcation diagram of Sine map is given in Fig. 1(c). Study regarding the combinations of one-dimensional chaotic maps shows that by introducing suitable combinations of such maps the chaotic range can be enhanced [92]. In the upcoming section, we explain this in detail.

7.4. Chaotic Combinations of Seed Maps

Here we detail the procedure to obtain new chaotic systems that possess chaotic nature throughout the domain. For this purpose, we model three nonlinear combinations of the involved seeds maps, as stated below;

1. Logistic Tent Chaotic System (*LT* chaotic system)
2. Logistic Sine Chaotic System (*LS* chaotic system)
3. Tent Sine Chaotic System (*TS* chaotic system)

Each of the above-stated systems can be defined by;

$$x_{i+1} = C_1(\tau_1, x_i) + C_2(\tau_2, x_2) mod 1; \quad (7.3)$$

where C_1 and C_2 are any two chaotic maps with their respective parameters τ_1 and τ_2. We explain the structure of each of the newly generated chaotic systems one by one as follows.

Table 1 LFT-based S-box

215	93	171	23	234	76	201	236	175	59	141	214	99	162	108	74
167	97	3	36	235	95	52	1	60	242	55	161	63	110	225	241
145	153	245	254	73	17	118	90	173	21	178	176	94	122	136	114
72	177	43	58	56	11	184	149	120	127	185	37	243	157	69	10
189	92	77	0	196	222	4	223	181	168	78	186	207	195	148	190
50	66	26	70	238	112	132	248	221	46	253	2	102	188	247	170
194	187	45	53	213	86	62	24	200	115	111	68	212	40	140	130
104	163	98	82	119	31	7	154	255	155	81	15	85	219	42	64
20	80	129	211	88	160	156	218	123	109	204	107	19	205	12	216
106	84	30	169	228	44	249	135	124	229	159	232	67	133	126	101
137	100	38	144	143	116	29	134	244	180	224	217	33	113	6	210
203	158	22	166	79	138	105	164	183	240	65	191	209	197	27	251
150	227	239	51	12	61	54	165	48	237	233	147	41	193	252	198
206	230	25	87	89	28	47	16	151	96	35	172	57	152	199	139
220	117	246	71	208	34	121	13	83	32	128	103	39	146	75	167
14	179	131	91	226	182	231	174	18	49	142	5	8	9	192	202

(a) Logistic (b) Tent (c) Sine

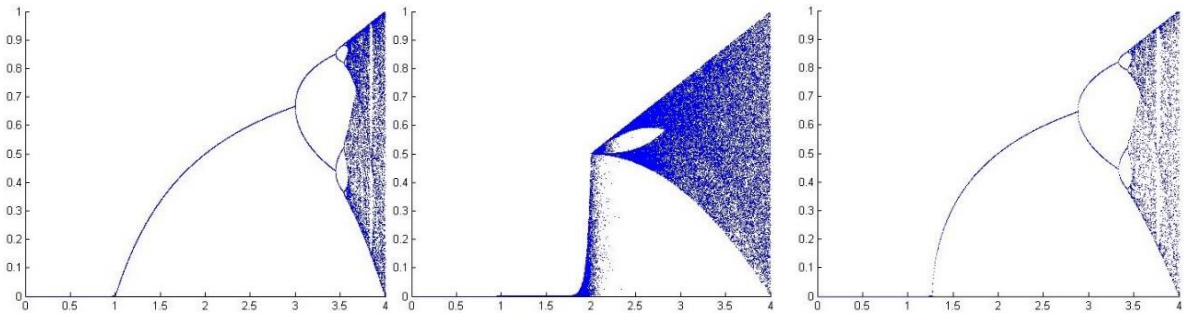


Fig. 1 Bifurcation diagrams of logistic, sine and tent map

(a) LT-System (b) LS-System (c) TS-System

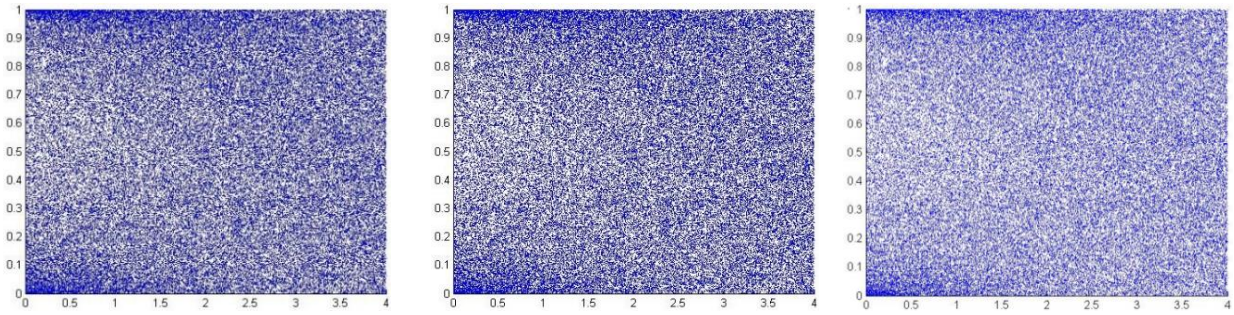


Fig. 2 Bifurcation diagrams of LTS, LSS and STS

Table 2 Comparison of performance indices of different S-boxes with LFT S-box

S-box	**Nonlinearity**	**SAC**	**BIC**	**DP**	**LP**
AES	112	0.5058	112.0	0.0156	0.062
APA	112	0.4987	112.0	0.0156	0.062
Gray	112	0.5058	112.0	0.0156	0.062
Skipjack	105.7	0.4980	104.1	0.0468	0.109
Xyi	105	0.5048	103.7	0.0468	0.156
RP	99.5	0.5012	101.7	0.2810	0.132
LFT	**112**	**0.510254**	**112**	**0.015625**	**0.0625**

7.4.1. *LT* chaotic System

From Eq (7.3), ***LT***- System is given as,

$$x_{i+1} = L(\vartheta, x_i) + T(4-\vartheta, x_i) mod 1,$$

$$= \begin{cases} \vartheta x_i(1-x_i) + \dfrac{(4-\vartheta)x_i}{2} mod 1 & ; \ x_i < \dfrac{1}{2} \\ \vartheta x_i(1-x_i) + \dfrac{(4-\vartheta)(1-x_i)}{2} mod 1 & ; \quad x_i \geq \dfrac{1}{2} \end{cases} \tag{7.4}$$

where the parameter $\vartheta \in (0, 4]$. The bifurcation diagram of the new chaotic system is given in Fig. 2(a). Comparing with the bifurcation diagrams of the logistic and the tent maps in Fig. 1, it's quite clear that the new chaotic system has much more chaotic range than that for the individual chaotic maps. (logistic and tent maps). One may observe that the performance of ***LT*** chaotic system in terms of the uniform distribution of the density function is also improved as compared to that of both the seed maps. This ensures the better chaotic behaviour of the newly generated chaotic system and makes them more efficiently applicable in information security problems. The similar properties are exhibited by the other two chaotic systems designed below.

7.4.2. LS Chaotic System

Logistic Sine System is given by,

$$x_{i+1} = L(\vartheta, x_i) + S(4-\vartheta, x_i) mod 1,$$

$$= \vartheta x_i(1-x_i) + \frac{(4-\vartheta) sin(\pi x_i)}{4} mod 1 \tag{7.5}$$

where $\vartheta \in (0, 4]$.

7.4.3. TS-chaotic System

Again from Eq. (7.3), we may deduce an expression for the ***TS*** chaotic system which is discussed in section 4.2.3. Fig. 2(b) and (c) show the bifurcation diagrams of ***LS*** and ***TS*** chaotic systems respectively.

7.5. Steganographic Scheme

The steganographic algorithm is pretty alike to [93], except for the two major differences which critically affect the results of the used scheme. Our scheme primarily includes a byte substitution step to boost the security level. Amir et.al. [93] used plain one-dimensional chaotic maps however, we hire chaotic systems, with enhanced chaotic range, for embedding information. The scheme utilizes a spatial domain and the information is embedded through the following steps.

1- The host image is fragmented into two parts; the upper and the lower.

2- Three improved chaotic range systems, *LT*, *LS* and *TS* are constructed in the foregoing section. These systems are applied to define the embedding position of pixels in both the upper and the lower parts of the host image such as *LT* -System defines the row number, *LS* -System defines the column number and *TS* -System corresponds to the frame number respectively.

3- Every specific pixel of the host image in both the parts is changed into binary 8 bits. These 8 bits are further split into the most significant bits (MSBs) and the least significant bits (LSBs) for both the upper and the lower parts.

4- An S-box is structured by using LFT and the nonlinearity of this S-box (Table 1) is 112, which is equal to that of the state of art, AES S-box.

5- The input text (that is to be hidden in the host image) is substituted through the proposed S-box and is then converted from decimal values to binary 8 bits. These 8 bits are further split into 4 MSBs and 4-LSBs.
6- For the upper part, the 4 LSBs are then replaced with the 4 LSBs of the substituted text, however, for the lower part, 4 LSBs are replaced with the 4 MSBs of the substituted text.
7- For each of the upper and the lower parts, the unchanged MSBs and the changed LSBs are joined together and converted into the decimal form. At this stage, joining the frames together produces the steganographic image. Fig. 4 represents the Host and steganographic images of Pepper, Baboon and Lena.

7.5.1. Inverse Steganographic Scheme

In order to obtain the host image, one may use the reverse of the above-stated methodology, we further explain it through the following steps.

1- Split the stego image into two parts. Again, we may call them the upper and the lower part.
2- Use the chaotic systems *LT*, *LS* and *TS* to identify the pixels' position in both the upper and the lower parts in a similar fashion as described in the steganographic scheme
3- Convert every specific pixel in both parts into binary 8 bits and further split each of 8 bits into MSBs and LSBs
4- 4 LSBs of the upper part are considered as the 4 LSBs of the text character and the 4 LSBs of the lower part are considered as the 4 MSBs of the text character.
5- Join these binary bits together and convert from 8 binary bits into the decimal form. This produces the substituted text.
6- Apply the inverse S-box to recover the original text.

Fig. 3 Flowchart of proposed steganographic scheme

It is evident that reverting the process requires the inverse S-box, this step seriously increases the security of the proposed technique when compared with [93]. Though not possible, but if an unintended recipient is able to recover the intermediate text, he would not be able to recover the original information unless the substitution algorithm is known.

(a) Host image (b) Steganographic Image

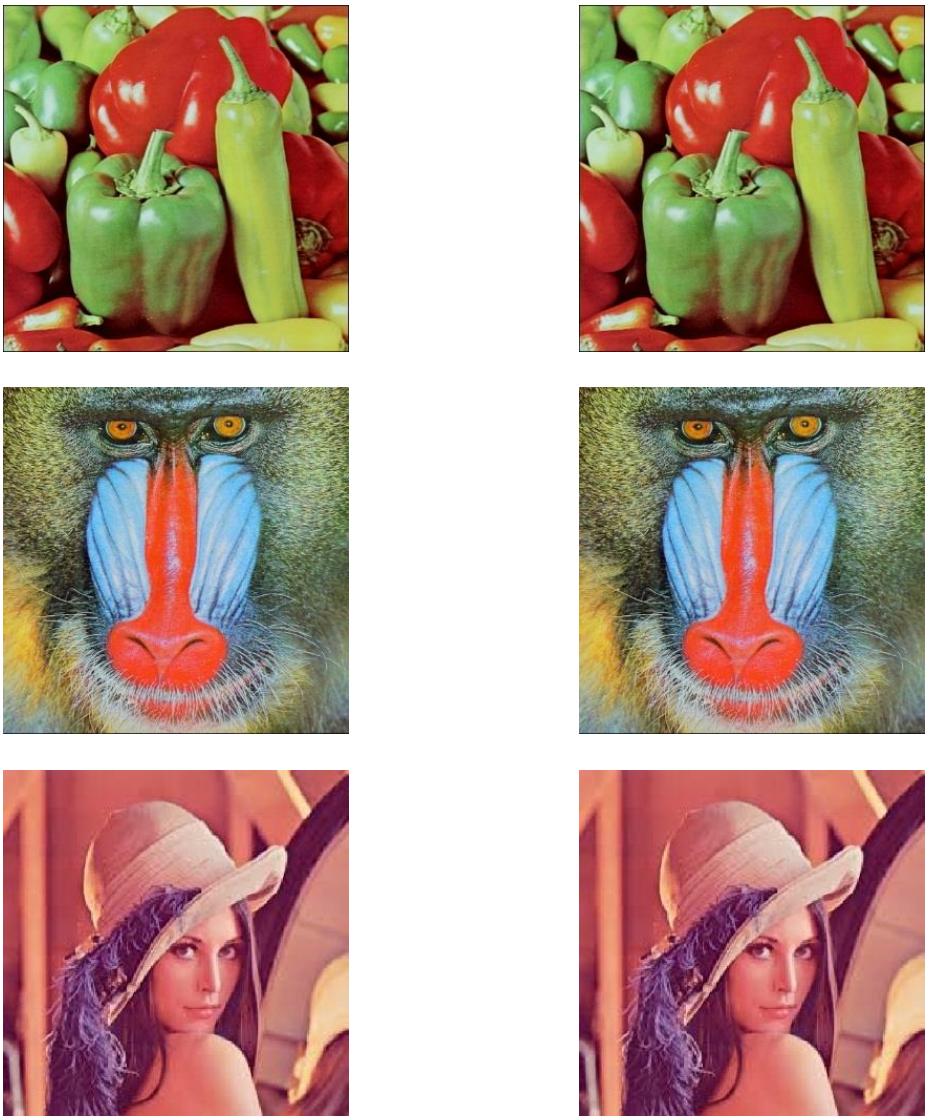


Fig. 4 Host and steganographic images of Pepper, Baboon and Lena

7.6. Statistical Security Analysis

We measure the cryptographic strength of the new method with the help of analysis such as ,homogeneity, correlation entropy, contrast, , peak signal to noise ratio (PSNR). We selected three benchmark images, Pepper, Baboon and Lena for analysis. One may observe that the specialty of the used scheme is the high similarity between original and

Table 3: Majority logic criterion analyses for original images

Original images	**Entropy**	**Contrast**	**Correlation**	**Homogeneity**
Peppers	5.5002	0.2190	0.9660	0.9637
Baboon	5.6840	0.3422	0.9571	0.8840
Lena	5.4183	0.1432	0.9665	0.9533

Table 4: Majority logic criterion analyses for steganographic images

Original images	**Entropy**	**Contrast**	**Correlation**	**Homogeneity**
Peppers	5.5003	0.2190	0.9660	0.9637
Baboon	5.6790	0.3409	0.9573	0.8845
Lena	4.9612	0.1217	0.9703	0.9603

Table 5 MSE and PSNR

Image	MSE	PSNR
Peppers	0.0013	28.8962
Baboon	0.0024	26.2405
Lena	0.0017	27.6436

steganographic images. Here, all the security parameters will be discussed and we present the numerical results in Tables 3-5. The numerical results are arranged in Table 3 and 4 for both the original and the steganographic images.

7.7. Robustness Analysis

To assess the robustness of our steganographic algorithm, we apply JPEG compression, the inclusion of noise and cropping effect on the steganographic images define the common similarity between the original image and the steganographic image.

(a) Compression (b) Noise (c) Cropping

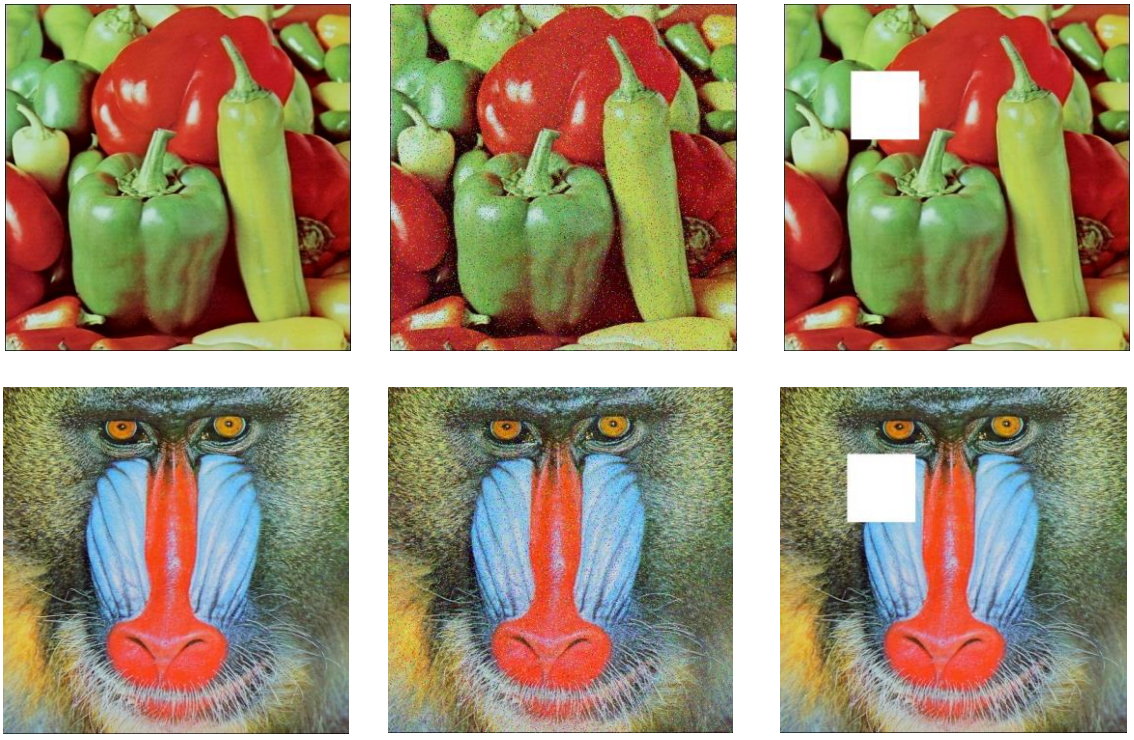


Fig. 5 Image processing effects on Pepper, Baboon and Lena's images

We study the effect on the steganographic image when information is embedded during JPEG compression. We compress the steganographic images of peppers, baboon and Lena as shown in Fig.5 and Table 6 which prove the robustness of our proposed scheme.

Table 6 Measure of similarity in steganographic images for image processing attacks

Attacks	**Peppers**	**Baboon**	**Lena**
Compression	1.1123×10^{-4}	1.1124×10^{-4}	1.1125×10^{-4}
Noise	1.0868×10^{-4}	1.0906×10^{-4}	1.0957×10^{-4}
Cropping	1.1087×10^{-4}	1.1087×10^{-4}	1.1087×10^{-4}

We further evaluate our algorithm under the effect of salt and pepper noise. The outcomes are given in Fig.5 and Table 6. In the light of these results, one can infer that this novel method is quite robust beside the noise attacks. Fig.5 shows the cropped steganographic images of peppers, baboon and Lena in which cropping effect is visible near the top left corner.In Table 6, the numerical results prove the strength of the steganographic technique against the geometric attack of cropping. The technique presented in this chapter is an improvement of the scheme introduced in [93].The involvement of a high-nonlinearity S-box and chaotic systems with improved chaotic range produces the enhanced security for the proposed steganographic method. Both the original and steganographic images exhibit almost same results under the application of statistical analysis

techniques. The strength of the steganographic algorithm is evaluated with the help of security analyses. In addition to this, our technique shows the property of robustness counter to different malicious attacks. Table. 6 witnesses that our scheme is semi-fragile to robust. In chapter 8, the chaotic steganographic technique in combined spatial and transform domain will be discussed in detail.

Chapter 8

Steganographic Technique Using Chaotic S-box in Combined Domain

This chapter presents a robust steganographic algorithm using substitution box, with high embedding capacity. The scheme is predominantly based on a potent application of chaos. The proposed method effectively addresses two major objectives of steganography: high embedding capacity and robustness. In this regard, on one hand, our method deploys the amalgamation of the spatial and the transform domain to enhance the capacity of embedding secret information. On the other hand, the involvement of stronger chaotic systems with enhanced chaotic range increases the robustness. The statistical strength of our algorithm is examined through various reliable analysis techniques. We further examine the robustness of our novel technique against several images processing attacks The outcomes of these analyses show that our algorithm is robust and highly secure and can be reliably used in multimedia applications.

8.1. Introduction

The study and improvement of ingenious ideas, to keep secret information protected from intruders, is the foremost objective of the modern research. [73], [74], [83], [96]–[98]. Steganography deals with concealing confidential information into other information. The methodology of watermarking and steganography revolves around embedding secret information

but their motives are different. The proposed framework deals with the technique of steganography.

With the advent of modern computer technology, remarkable skills for surreptitious communication have been developed [73], [76], [98], [99]. The wide-ranging applications of steganographic methods in computer forensics, copyright protection, broadcast monitoring, circumvention of web-censorship etc. made it an absolutely ascendant strategy in communication security.

A steganographic technique involves two steps: firstly, hiding secret information in the carrier image, secondly, retrieving hidden information from the stego image. Generally, in steganography, secret information is embedded in either spatial or the transform (frequency) domain. In spatial domain embedding, LSB- substitution technique is most common. However, in the transform domain, invertible transforms such as discrete cosine transform, discrete Fourier transform or discrete wavelet transforms are applied to transform the image into its frequency representation. Both the domains have some advantages and disadvantages also. Frequency domain embedding is robust but spatial domain offers increased capacity for hiding data. This motivates researchers to deploy the combinations of both the domains [100]–[102].

The features of chaotic systems, such as unpredictability, irregularity and sensitivity to the initial conditions, speed and computational power etc., distinguish them in multimedia security applications [84]–[86]. Keeping this in view, the study and analysis of chaos-based steganographic techniques have been quite popular in last few decades. It is, however, observed that some chaos-based methods are vulnerable to the statistical analysis because of the limited chaotic range of the used maps.

In [92] Zhou et. al. anticipated a nonlinear combination of chaotic maps that enhance the chaotic range of the resulting system. Such systems are applied in image encryption applications [92], but, these systems have not been applied in steganographic methods as yet. We, in this chapter, establish a successful image-steganographic application of improved chaotic systems in information embedding process. To structure these systems, we engage two most frequently used one-dimensional chaotic maps, the logistic map and the sine map. By constructing S-box with the amalgamation of these two maps, we construct a chaotic S-box. We further exploit the combination of the spatial and transform domains to reach the significantly high capacity level for embedding secret information. The evaluation of our novel method is done with the help of some most frequently used analysis techniques and we prove that our technique produces coherent results.

8.2. One-dimensional Chaotic Maps

In the understudy problem, we use two of the most popular one-dimensional chaotic maps; the logistic map and the sine map. These maps are further used to develop stronger chaotic systems. In the consequent subclasses, the fundamental properties of these maps are thoroughly discussed. The logistic map is the most frequently used map having a straightforward structure. The chaotic logistic map is defined in section 7.3.1. Similarly, the sine map is thoroughly explained in section 7.3.3.[92].

8.2.1. Combinations of Chaotic Maps

The two models of the nonlinear combinations of the involved seeds maps, as stated below;

1. **Logistic-Logistic System (LLS)**

2. **Sine-Sine System (SSS)**

Each of the above-mentioned systems can be defined by

$$x_{i+1} = \mathcal{F}_1(\lambda_1, x_i) \times G(k) - floor(\mathcal{F}_2(\lambda_2, x_i) \times G(k); \quad (8.1)$$

where $G(k) = 2^m, 8 \leq m \leq 20$ and $\mathcal{F}_1$ and $\mathcal{F}_2$ are any two chaotic maps with their respective parameters λ_1 and λ_2. We explain the structure of each of the new chaotic systems one by one as follows.

8.2.2. Logistic-Logistic System LLS

From Eq. (8.1), LLS is given as

$$= \nu x_i(1 - x_i) \times 2^{14} - floor(\nu \times x_i \times (1 - x_i) \times 2^{14} \quad (8.2)$$

where the parameter $\nu \in (0,4]$. The bifurcation diagram of the new chaotic system. It is quite clear from bifurcation diagrams of the logistic and the tent maps that the new chaotic system has enhance chaotic range than that for the individual seed maps (logistic and logistic maps)., One may observe that the performance of LLS in terms of the uniform distribution of the density function is also improved as compared to that of both the seed maps. This ensures the better chaotic behaviour of the newly generated chaotic system and makes them more efficiently applicable in information security problems. The similar properties are exhibited by the other chaotic system designed below.

8.2.3. Sine-Sine System SSS

By using eq (8.1), Sine-Sine System is given by,

$$= \nu \times sin(\pi x_i) \times 2^{14} - floor(\nu \times sin(\pi \times x_i) \times 2^{14} \quad (8.2)$$

where $\nu \in (0,4]$.

8.3. Construction of chaotic S-box using group action

Block ciphers are one of the vital components to build cryptosystem and they have a phenomenal dependence on the quality of S-box. In this substitution process, m binary input bits transform into n binary output bits. The resistance against any differential and linear cryptanalysis in encryption scheme depends on the suitable selection of S-box. In this chapter, Sine-Logistic map (SLM) is applied for the synthesis for new S-boxes due to its wider chaotic range and cryptographic properties. The Fig. 1 of flow chart shows that the initial values as input for the design of proposed S-box are taken from chaotic SLM. These values are then assigned to the linear fractional transformation for the action of the projective general linear group on the finite field 2^8 having 256 elements. The proposed chaotic S-box has 256 unique values and given in Table 1.

8.3.1. Proposed S-box

In this chapter, S-box are constructed by taking exponents value 1 of chaotic SLM. The mathematical description of the map corresponds to S-box is given in equation (8.4)

$$Y_{n+1} = \Pi_{SL}\left(\mu, {Y_n}^{\beta}\right) = \left(S\left((4-\mu), {Y_n}^{\beta}\right) + L\left(\mu, {Y_n}^{\beta}\right)\right) mod 1$$

$$= \left((4-\mu) Sin(\pi {Y_n}^{\beta})/4 + \mu {Y_n}^{\beta}\left(1 - {Y_n}^{\beta}\right)\right) mod 1 \qquad (8.4)$$

where $0 < \mu \leq 4$.

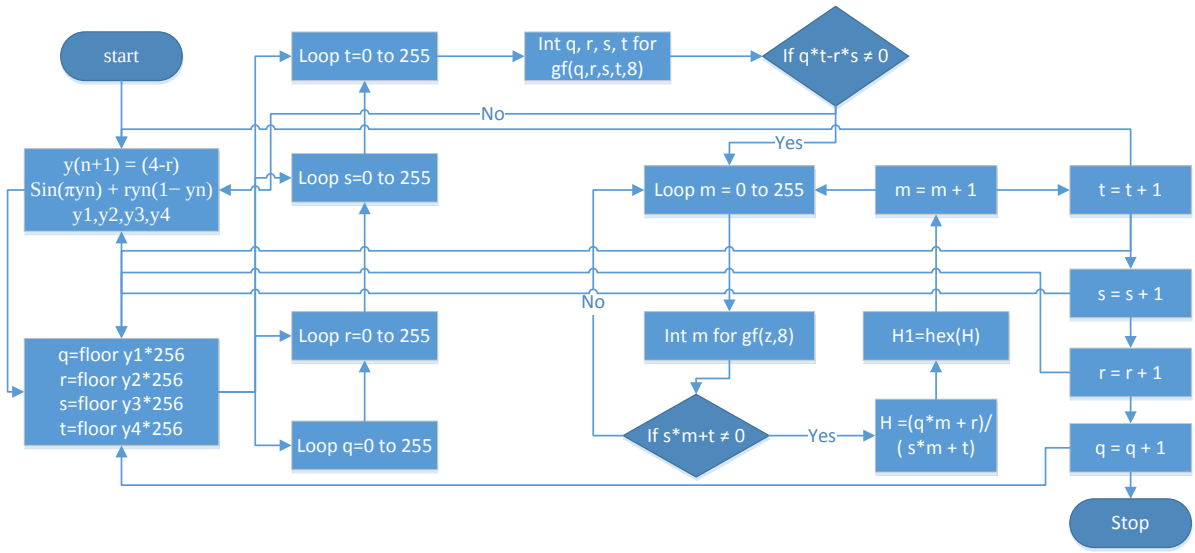


Fig. 1. Algorithm for the synthesis of proposed S-box

Table 1. S-box corresponds to the SLM, $\beta = 1$

1	**88**	**219**	**77**	**115**	**240**	**245**	**33**	**165**	**85**	**198**	**35**	**117**	**201**	**192**	**10**
62	251	205	143	47	69	3	0	188	149	94	190	58	246	27	177
158	202	146	118	138	148	137	239	108	66	43	49	218	20	172	52
124	25	19	67	73	206	168	22	233	81	193	181	105	113	211	122
222	31	109	164	212	210	101	56	104	39	225	249	141	159	106	140
247	242	145	176	185	57	237	64	100	238	228	128	111	199	34	215
18	136	220	110	252	183	5	91	216	15	42	241	38	253	72	155
87	221	203	63	142	163	103	28	96	194	175	46	80	129	24	41
162	160	61	16	86	150	208	8	213	231	232	11	78	13	123	147
60	187	53	135	130	125	196	227	173	6	157	83	134	17	244	144
189	120	26	112	236	99	7	152	119	79	217	45	102	156	131	75
209	230	89	14	151	30	54	169	243	37	76	93	178	21	71	197
132	2	84	127	29	116	40	153	171	255	107	180	32	207	82	174
48	70	186	114	121	55	229	167	126	59	195	90	223	184	182	23
224	234	133	235	170	214	254	226	97	154	65	200	51	9	68	74
166	44	95	204	92	248	50	98	4	12	250	161	36	139	191	179

8.4. Background of DWT and DCT

In Discrete wavelet transform (DWT), the time domain signal is gone through sequential high-pass filtering and low-pass filtering for decomposition of a signal into various frequency bands. There are two functions in 1D-DWT namely as scaling and wavelet functions. Scaling is related with low-pass filters whereas wavelet functions are related with high pass filters. Signal decomposition into a coarse approximation and detail information for analyzing at a different frequency with different resolutions is an important feature of DWT. Moreover, the characteristics of multi-resolution, excellent spatial localization and its analysis performance similar to Human visual system (HVS) make DWT a necessary and important tool for digital watermarking.

In 1D-DWT, the Nyquist's criteria suggest the elimination of half of the samples of original signal $z[m]$ after filtering through half band high pass filter $x[m]$ and low pass filter $t[m]$ as highest frequency of signal remained $\pi/2$. It gives the opportunity to sub-sample the signal by 2, by discarding every other sample. Mathematically,

$$g_{high}[c] = \sum_m z[m] \otimes x[2c - m] \tag{8.5}$$

$$g_{low}[c] = \sum_m z[m] \otimes t[2c - m] \tag{8.6}$$

where, $g_{high}[c]$ is the result of high pass filtering and $g_{low}[c]$ is the outcome of low pass filtering. In DWT, the time resolution remains half and frequency resolution gets double after the filtering and sub-sampling of signal at every decomposition.

By applying row-wise and column-wise 1D-DWT transform, our transformation can easily get in 2-dimensional discrete wavelet transform. These 2D-DWT filters divide the host image into four disjoint multi-resolution sub-bands LL, HL, LH, and HH. The approximation band LL1 represents low-frequency coefficients whereas vertical, horizontal and diagonal edges of the digital image are

in HL1, LH1, and HH1 as shown in Fig. 2. The next coarser scale of wavelet coefficients is obtained by repeating the same process on LL1; we will have 3m+1 sub-bands, where m is a count of decomposition levels.

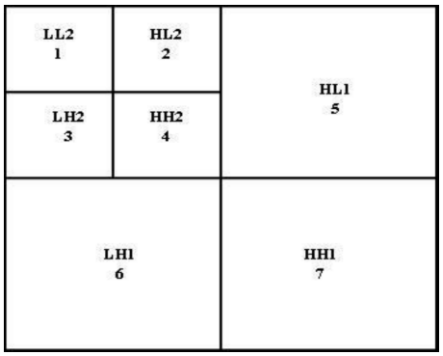


Fig. 2: 2 level sub-band DWT transformation

It is observed that Fourier series provide the foundation of different transforms which includes discrete cosine transform (DCT). The compression through data quantization is obtained through (DCT) which transform an image into frequency domain. The DCT uses only the real part of the Fourier complex kernel. Mathematically, the pair of equation (8.7) and (8.8) represents DCT and inverse DCT respectively.

$$F(u,v) = \mathrm{C(u)C(v)} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) cos \frac{(2x+1)u\pi}{2N} cos \frac{(2y+1)v\pi}{2N} \tag{8.7}$$

$$f(x,y) = \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} \mathrm{C(u)C(v)} F(u,v) cos \frac{(2x+1)u\pi}{2N} cos \frac{(2y+1)v\pi}{2N} \tag{8.8.}$$

8.5. Steganographic Scheme

The proposed scheme highlights two most important steps for information embedding process. First, rather depending on either spatial or transform domain only, it employs the combination of both the domains to reach the acceptable level of embedding capacity.

(a) Original (b) Steganographic

Fig. 3: Lena: Original and steganographic images

as well as robustness. Secondly, the scheme is based on stronger chaotic combinations which depict extra ordinary features when compared with the individual seed maps.

The detailed steganographic strategy is explained through the flowchart. In this process, we take the host image I_H (sized 512×512), and shape this into a vector of length m. The secret information is a text I of about 20% of the size of the host image. This text message is first substituted with SLM S-box to increase the security level. Break I into two parts I_1 and I_2 such that I_1 and I_2 are 70% and 30% of I respectively. We aim to embed I_1 in the spatial domain and I_2 in the frequency domain. First I_1 is inserted at random positions of I_H using the chaotic system LLS. This gives the partial stego image in the spatial domain. We reshape this partial stego image into a matrix form and convert into frequency domain by using both discrete wavelet transform DWT and discrete cosine transform DCT. Again, revamp the obtained image into a vector of length m and pick the largest frequency components (30% of the whole) and use the sine-sine chaotic system to embed

I_2 at the random positions of the selected largest values. This produces the frequency domain version of the stego image. At this stage, we apply the inverse transform to reach the final version of the stego image.

The reverse process of the above mentioned method is required for the extraction of original image I from the stego image. The flow chart of the whole method is thoroughly explained in. Fig. 4. We apply the steganographic algorithm on 512×512 benchmark images of Lena in Fig. 3.

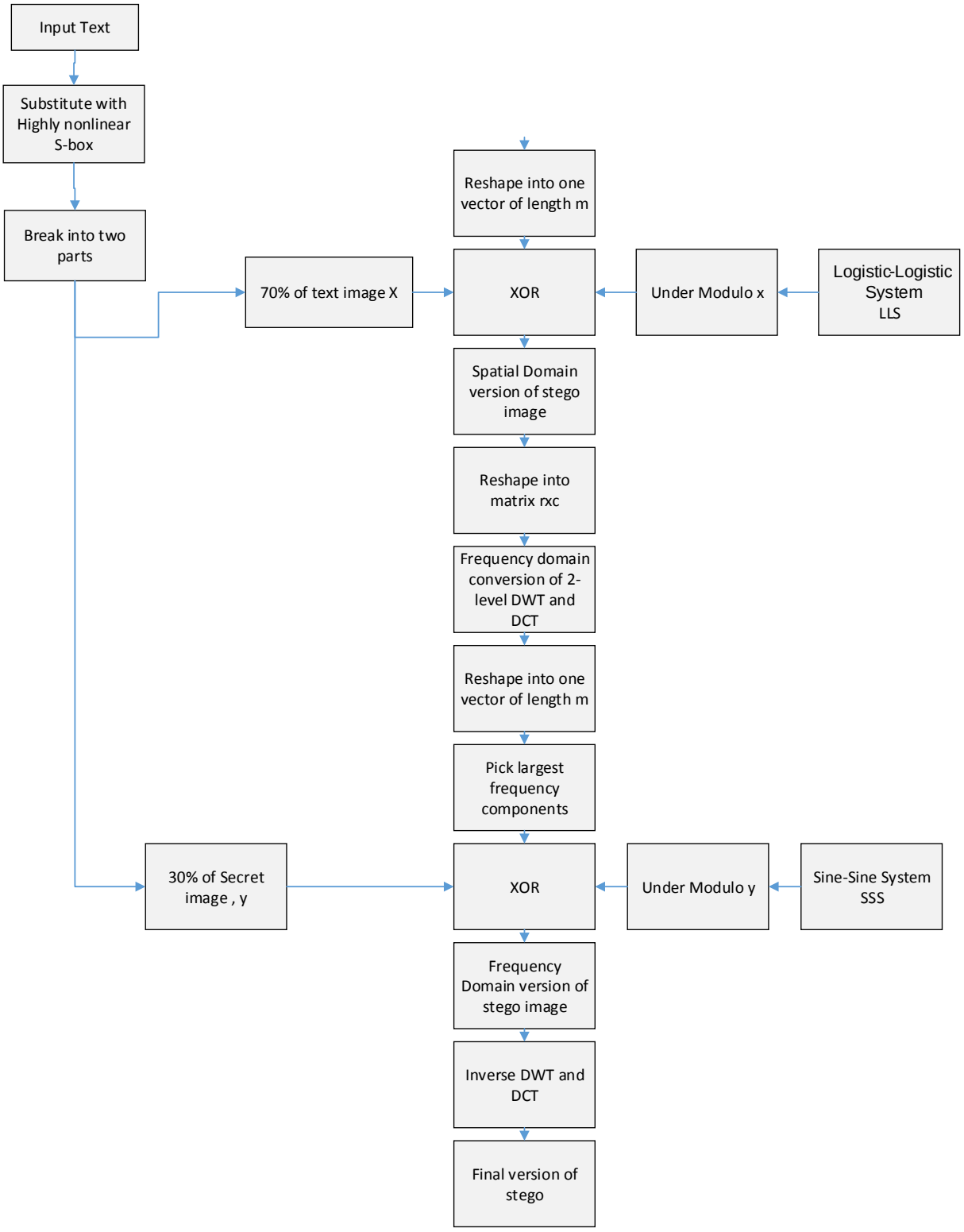


Fig. 4. Algorithm for the proposed watermarking technique

8.6. Statistical Security Analysis

Here, we measure the cryptographic strength of our new technique with the help of analysis such as correlation, entropy, homogeneity, contrast, peak signal to noise ratio (PSNR) and Mean squared error (MSE). We selected two benchmark images of Lena and baboon for analysis. One may observe that the specialty of the used scheme is high similarity between original and steganographic images. Table 2-4 provide the results of all security parameters.

Table 2: Original Image: results of majority logic criterion

Images	Entropy	Contrast	Correl.	Homog.
Lena	5.4183	0.1432	0.9665	0.9533
Babbon	5.6840	0.3422	0.9571	0.8840

Table 3: Stego Image: results of majority logic criterion

Images	**Entropy**	**Contrast**	**Correl.**	**Homog.**
Lena	4.9612	0.1217	0.9703	0.9603
Babbon	5.6790	0.3409	0.9573	0.8845

Table 4: MSE and PSNR

Image	**MSE**	**PSNR**
Lena	0.0017	27.6436
Baboon	0.0024	26.2405

8.7. Robustness Analysis

The robustness of our novel steganographic algorithm is measured by applying JPEG compression, the addition of noise and cropping effect on the steganographic images. This helps to conclude the similarity between the host steganographic image and the steganographic image extracted by applying the above-mentioned effects. The High correlation between these two images demonstrates the robustness of our method. Fig. 5 represents the image processing attacks on our scheme and Table 5 is the tabular form of these analyses.

Table 5: Measure of similarity in steganographic images for image processing attacks

Attacks	Peppers	Baboon	Lena
Compression	1.1124×10^{-4}	1.1125×10^{-4}	1.1125×10^{-4}
Noise	1.0906×10^{-4}	1.0957×10^{-4}	1.0957×10^{-4}
Cropping	1.1087×10^{-4}	1.1087×10^{-4}	1.1087×10^{-4}

(a) Compression (b) Noise (c) Cropping

Fig. 5: Image processing effects on Lena and Baboon's image

The involvement of a S-box and chaotic systems with improved chaotic range produces the enhanced security for the proposed steganographic method. For any invader, it is very hard to obtain the information from the steganographic image as this image is apparently similar to the host image. The original text is first substituted with S-box which increased the security of the proposed scheme and by amalgamation of spatial and frequency domain, we address the issue of capacity and robustness. The strength of the steganographic algorithm is evaluated with the help

of security analyses. In addition to this, our technique shows the property of robustness against different malicious attacks. In the last chapter, we give the conclusion of the whole thesis with some future directions.

Chapter 9

Conclusion

This chapter deals with brief and precise description of the results obtained in this thesis. Some future guidelines are also part of this chapter.

The central objective of the presented work can be categorized in the following categories.

1. By employing algebraic structures which include finite local ring, linear fractional transformation to construct S-boxes to enhance the security level.
2. With the help of combined one-dimensional chaotic systems, multiple S-boxes are constructed. The combination of chaotic systems enhanced the chaotic range which is helpful to create confusion in cryptosystems.
3. To introduce new techniques for digital watermarking and steganography to enhance the security of digital contents. The involvement of S-box in the schemes, not only develops confusion but also provides more security and robustness.

9.1. Conclusion

In chapter two, a novel S-box technique is presented which is based on projective general linear group over the unit element of Z_{512}. Randomness and improved security is perceived with the support of security analysis results. The ability of new S-box to create perplexity in data is quite exceptional. In certain analyses, vulnerability to malicious attacks and ability to create confusion is being checked. The analysis started from calculating nonlinearity of S-box followed by input/output bit designs analyses which consist of strict avalanche criterion and bit independence

criterion analysis. These analyses give features and assembly of bits at input and output. In the end, approximation probability which consists of linear and differential probabilities gives the probability of events and differential uniformity to progress in the form of iterative process. The proposed S-box is equated with AES, Xyi , Skipjack, S8, Gray, APA, and Prime S-boxes, frequently involved in variant encryption systems. The proposed S-box is extremely valuable for information security methods and different encryption process.

In chapter three, the kernel of the presented work lies in the fact that the choice of the background Galois field and its generating primitive polynomial matters to the function and performance of the substitution boxes. This fact leads to the fascinating idea that rather the development of new algorithms, the improvement of the existing algorithms is worth-studying as its least laborious but most effective. We propose, on the basis of the example discussed, that the effect of the choice of generating polynomial may lead to an intensive research in future to modify the design models of S-boxes. It will definitely affect the applications of S-boxes in other branches of the digital communication, such as steganography, watermarking and image encryption etc

By applying chaotic tent-sine system, the construction of different S-boxes is presented in chapter four. The linear fractional transformation is used on random values obtained through the chaotic map and provides 256 different values of S-box. The randomness produced through inclusion of chaos not only increases the unpredictability of the cipher but also supports to confront any attempt of cryptanalysis. These two prominent properties help to confirm secure communication of data. The outcomes of the various statistical analysis confirm the performance of our new S-boxes. The generated S-boxes show better results when matched with some privileged S-boxes, as apparent from the different statistical analysis.

Chapter 5 represents a new idea of utilization of a chaotic system of differential equation for construction of S-box. This S-box is further utilized for frequency domain watermarking. It is almost impossible to recognize watermark once the watermarking is done with frequency domain include the chaos from numerical solution of the differential equation. The embedding of the watermark (secret signature) has been done in the frequency domain of the host image whose copyrights is to be protected. The random results of chaotic map are applied to identify the embedding positions. The embedding through chaos is our idea which differentiates our work from others. In addition to this, the outcomes of security statistical analysis along with robustness test with the help of confidence measure really support the new idea of watermarking. The similarity after image processing tests which is between 42 and 77 % proposed scheme is an example of semi fragile watermarking technique

In the next chapter, a new idea is presented for watermarking that mainly relies on a newly designed 8×8 S-box from a local ring instead of a Galois field. The involvement of S-box in the scheme, where we substitute the values of the watermark image, not only develops confusion in understanding the used scheme but also provides more security and support to our argument for copy right protection of digital data. This technique of watermarking is based on frequency domain Discrete Cosine Transform. The complexity of the algebraic structure of the S-box and then frequency domain technique makes almost impossible to identify watermark. Moreover, the outcomes of statistical analyses and robustness tests really support the new idea of watermarking. The numeric results of similarity, after the application of the image processing tests, lie in the range 40- 79%, (78.92 % in our case) which makes us conclude that our technique is a semi-fragile watermarking technique.

The technique presented in chapter 7 is an improvement of the scheme introduced in [103]. The involvement of a high-nonlinearity S-box and chaotic systems with improved chaotic range produces the enhanced security for the proposed steganographic method. It is very challenging for any invader to get the information from the steganographic image as this image is apparently identical to the host image. Both the original and steganographic images exhibit almost same results under the application of statistical analysis techniques. The strength of the steganographic algorithm is calculated with these security analyses. In addition to this, our technique shows the property of robustness against various malicious attacks. Table. 6 witness that our scheme is semi-fragile to robust.

In the last chapter, a watermarking technique in combined spatial and frequency domain is presented. This technique involves high-nonlinearity S-box and improved chaotic range. This technique addresses the problem of watermark embedding capacity, robustness and security of the technique. It is very tough to get any information from the steganographic image as this image is a decoy of the host image. The simulation and statistical analyses indicate the strength of the steganographic algorithm. Moreover, our technique shows the property of robustness against different malicious attacks.

9.2. Future work

While going through this research work, multiple queries came across in my mind but remained unanswered. These may be helpful for future directions or can be considered as the continuation of the proposed research. Some of these are listed below.

- To construct cryptographically strong component for block ciphers (S-box) having a better number of input bits to withstand against numerous linear and differential attacks.

- Construction of S-boxes with simple algebraic structures having high nonlinearity.
- Project different software to study cryptographic properties of S-box
- The invention of novel techniques based on the combination of algebraic and chaotic structures for the improvement of cryptographic properties of the nonlinear component of block cipher.
- Construction of S-boxes with the utilization of various algebraic structures like the symmetric group, Galois ring, cyclic groups and loop theory etc. Design of novel techniques of multimedia security based upon these S-boxes.

REFERENCES

[1] P. W. Wong, "A Public Key Watermark for Image Verification and Authentication," in *Proceedings of IEEE International Conference on Image Processing*, 1998, pp. 425–429.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, 1949.

[3] J. Daemen and V. Rijmen, "The design of Rijndael-AES: the advanced encryption standard.," *Springer, Berlin*, 2002.

[4] A. U. Rehman, J. S. Khan, and J. Ahmad, "A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps," *3D Res. Springer*, vol. 7, p. 7, 2016.

[5] S. S. Jamal, T. Shah, S. Farwa, and M. U. Khan, "A robust chaotic steganographic technique with enhanced security based on a high-nonlinearity S-box. Submitted.," 2017.

[6] S. Farwa, T. Shah, and L. Idrees, "A highly nonlinear S-box based on a fractional linear transformation," *Springerplus*, vol. 5, no. 1, p. 1658, 2016.

[7] S. S. Jamal, M. U. Khan, and T. Shah, "A Watermarking Technique with Chaotic Fractional S-Box Transformation," *Wirel. Pers. Commun.*, vol. 90, no. 4, 2016.

[8] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*. CRC Press, Inc. Boca Raton, FL, USA ©2007, 2007.

[9] T. W. Cusick and P. Stanica, *Cryptographic Boolean functions and applications*. Elsevier/Academic Press, Amsterdam, 2009.

[10] I. Hussain and T. Shah, "Literture survey on nonlinear components and chaotic nonlinear components of block ciphers," *Nonlinear Dyn.*, vol. 74, pp. 869–904, 2013.

[11] C. Carlet, *A larger class of cryptographic Boolean functions via a study of the Maiorana-McFarland construction*, vol. 2442. 2002.

[12] L. Burnett, “Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography,” Queensland University of Technology, 1997.

[13] M. Matsui, “Linear cryptoanalysis method for DES cipher,” *Lect. Notes. Comput. Sc.*, vol. 765, pp. 386–397, 1994.

[14] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic applications,” *IEEE Trans. Inform. Theory*, vol. 30, no. 5, pp. 776–780, 1984.

[15] O. S. Rothaus, “On bent functions,” *J. Comb. Theory Ser. A.*, vol. 20, pp. 300–305, 1976.

[16] W. Meier and O. Stafielbach, “Nonlinearity criteria for cryptographic functions,” *Adv. Cryptol. - EUROCRYPT ’89, Lect. Notes Comput. Sci.*, vol. 434, pp. 549–562, 1990.

[17] E. Biham and A. Shamir, “Differential Cryptanalysis of DES-like Cryptosystems,” *J. Cryptol.*, vol. 4, no. 1, pp. 3–72, 1991.

[18] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Labs. Tech. J.*, vol. 28, no. 1949, pp. 656–715, 1949.

[19] W. Meier and O. Staelbach, *Nonlinearity criteria for cryptographic functions*. Lect. Notes. Comput. Sc., 1990.

[20] .R Forre, *The strict avalanche criterion: Spectral properties of boolean functions and an extended definition*. Lect. Notes. Comput. Sc., 1990.

[21] T. Siegenthaler, “Correlation-immunity of nonlinear combining functions for cryptographic appli- cations,” *IEEE Trans. Inform. Theory*, vol. 30, no. 5, pp. 776–780, 1984.

[22] A. F. Webster and S. E. Tavares, “On the design of S-boxes, Lect. Notes. Comput. Sc,” vol. 218, pp. 523–534, 1986.

[23] H. M. Heys, “A tutorial on linear and differential cryptanalysis, Technical Report CORR 2001- 17,” *Cent. Appl. Cryptogr. Res. Dep. Comb. Optim. Univ. Waterloo*.

[24] E. Biham and A. Shamir, “Differential cryptanalysis of DES like cryptosystems,” *Lect. Notes. Comput. Sc.*, vol. 537, p. 2–21, 1991.

[25] L. L. Bartosov, “Linear and differential cryptanalysis of reduced round AES,” *Tatra Mt. Math. Publ.*, vol. 50, no. 1, pp. 51–61, 2011.

[26] M. T. Tran, D. K. Bui, and A. D. Doung, “Gray S-box for advanced encryption standard,” *Int Conf Comp Intel Secur*, pp. 253–256, 2008.

[27] L. Cui and Y. Cao, “A new S-box structure named Affne-Power-Affine,” *Int. J. Innov. Comput. I*, vol. 3, no. 3, pp. 45–53, 2007.

[28] I. Hussain, T. Shah, and H. Mahmood, “A New Algorithm to Construct Secure Keys for AES,” *Int. J. Contemp. Math. Sci.*, vol. 5, no. 26, pp. 1263–1270, 2010.

[29] I. Hussain, T. Shah, H. Mahmood, M. A. Gondal, and U. Y. Bhatti, “Some analysis of S-box based on residue of prime number,” *Proc Pak Acad Sci.*, vol. 48, no. 2, pp. 111–115, 2011.

[30] X. Y. Shi, H. Xiao, X. You, and K. Y. Lam, “A method for obtaining cryptographically strong 8x8 S-boxes,” *Int. Conf. Inf. Netw. Appl.*, vol. 2, no. 3, pp. 14–20, 2002.

[31] J. Kim and R. C.-W. Phan, “Advanced differential style cryptanalysis of the NASA’s skipjack block cipher,” *Cryptologia*, vol. 33, no. 3, pp. 246–270, 2009.

[32] H. Feistel, “Cryptography and computer privacy,” *Sci. Am.*, vol. 228, no. 5, pp. 15–23, 1973.

[33] X. Yi, X. S. Cheng, H. Y. Xiao, and K. Y. Lam, “Method for obtaining cryptographically strong 8 × 8 S-boxes,” in *In IEEE Global Telecommunications Conference, GLOBECOM*

97, 1997, vol. 2, no. 3, pp. 689–693.

[34] D. Feng and W. Wu, *Design and analysis of block ciphers*. Beijing: Tsinghua University Press, 2000.

[35] I. Hussain, T. Shah, H. Gondal, and M. A. Mahmood, "A projective general linear group based algorithm for the construction of substitution box for block ciphers.," *Neural Comput. Appl.*, vol. 22, pp. 1085–1093, 2013.

[36] Z. Hua, Y. Zhou, C. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci. (Ny).*, vol. 297, pp. 80–94, 2015.

[37] M. Matsui, "Linear cryptanalysis method of DES cipher," Advances in cryptology, proceeding of the Eurocrypt'93, Lecture Notes in Computer Science, 1994, pp. 386–397.

[38] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Statistical analysis of S-box in image encryption applications based on majority logic criterion," *Int J Phys Sci*, vol. 6, no. 16, pp. 4110–4127, 2011.

[39] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, "Construction of new S-box using a linear fractional transformation," *World Appl. Sci. J.*, vol. 14, no. 12, pp. 1779–1785, 2011.

[40] K. Nyberg, "Perfect nonlinear S-boxes, Advances in Cryptology," *Springer Heidelberg,EURO- CRYPT'91. Lect. notes Comput. Sci. 457.*, pp. 378–386, 1992.

[41] G. Chen and T. Ueta, "Yet another chaotic attractor," *Int. J. Bifurc. Chaos*, vol. 9, no. 7, pp. 1465–1466, 1999.

[42] A. F. Webster and S. Tavares, *Advances in Cryptology*, 85th ed. Proceedings of CRYPTO. Lecture Notes in Computer Science, 1986.

[43] G. Tang, X. Liao, and Y. Chen, "A novel method for designing S-boxes based on chaotic

maps," vol. 23, pp. 413–419, 2005.

[44] G. Chen, Y. Chen, and X. Liao, "An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps," vol. 31, pp. 571–579, 2007.

[45] Y. Wang, K. W. Wong, X. Liao, and T. Xiang, "A block cipher with dynamic S-boxes based on tent map.," *Commun. Nonlinear Sci. Numer. Simul.* , vol. 14, p. 3089, 2009.

[46] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "An efficient approach for the construction of LFT S-boxes using chaotic logistic map," *Nonlinear Dyn.*, vol. 71, pp. 133–140, 2013.

[47] I. S. Sam, P. Devaraj, and R. S. Bhuvaneswaran, "An intertwining chaotic map based image encryption scheme," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 1995–2007, 2012.

[48] G. Tang and X. Liao, "A method for designing dynamical S-boxes based on discretized chaotic map," vol. 23, pp. 1901–1909, 2005.

[49] G. Chen, "A novel heuristic method for obtaining S -boxes," *Chaos, Solitons and Fractals*, vol. 36, no. 4, pp. 1028–1036, 2008.

[50] F. Özkaynak and A. B. Özer, "A method for designing strong S-boxes based on chaotic Lorenz system," *Phys. Lett. A374(36), 3733-3738 (2010).*, vol. 374, no. 36, pp. 3733–3738, 2010.

[51] Mukherjee, S. Maitra, and S. T. Acton, "Spatial Domain Digital Watermarking of multimedia objects for Buyer Authentication.," *IEEE Trans. Multimed.*, vol. 6, no. 1, p. 2004.

[52] G. Caronni, "Assuring ownership rights for digital images," in *Proceedings of Reliable IT Systems, viewveg Publishing Company, Germany,* 1995, pp. 251–263.

[53] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "Construction of S 8 Liu J S-boxes

and their applications.," *Comput. Math. with Appl.*, vol. 64, no. 8, pp. 2450–2458, 2012.

[54] O. E. Ro¨ssler, "An equation for continuous chaos. Physics Letters A," vol. 57, no. 5, pp. 397–398, 1976.

[55] Y. Wang, Q. Xie, Y. Wu, and B. Du, "A software for S-box performance analysis and test," *Int. Conf. Electron. Commer. Bus. Intell. ECBI 2009*, pp. 125–128, 2009.

[56] C. Adams and S. Tavares, "Advances in Cryptology," in *Proceedings of CRYPTO. Lect. Notes Comput.*, 1989, vol. 89, pp. 612–615.

[57] M. Khan, T. Shah, H. Mahmood, M. A. Gondal, and I. Hussain, "A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems," pp. 2303–2311, 2012.

[58] U. Cox, L. Kilian, F. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, pp. l673–1687, 1997.

[59] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Processing*, vol. 92, no. 4, pp. 1101–1108, 2012.

[60] Kitamytra, S. Kanai, T. Kanai, and T. Kishinami, "Copyright Protection of Vector Map using Digital Watermarking Method based on Discrete FourierTransform.," in *Proceedings of IEEE International Symposium on Geosciences and Remote Sensing*, 2001, pp. 1191–1193.

[61] W. D. Hong, L. D. Ming, Y. Jun, and C. F. Xiong, "An Improved Chirp Typed Blind Watermarking Algorithm Based on Wavelet and Fractional Fourier Transform. ICIG 291-296, Aug. .," in *Proceedings of IEEE International Conference on Images and Graphics*, 2007, pp. 291–296.

[62] S. Kaur and R. K. Sidhu, "Robust digital image watermarking for copyright protection

with SVD-DWT-DCT and Kalman filtering," *Int. J. Emerg. Technol. Eng. Res.*, vol. 4, no. 1, pp. 59–63, 2016.

[63] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, 2003.

[64] F. Liu and F. Yang, "An improved blind watermarking algorithm based on DCT," *Comput. Eng. Appl.*, vol. 45, no. 13, pp. 124–126, 2009.

[65] G. M. Wang and Z. F. Hou, "Watermarking scheme based on DCT," *Comput. Eng. Des.*, vol. 29, no. 21, pp. 5635–5637, 2008.

[66] Q. Zhang, Y. Li, and X. Wei, "An Improved Robust and Adaptive Watermarking Algorithm Based on DCT," *J. Appl. Res. Technol.*, vol. 10, no. 3, pp. 405–415, 2012.

[67] Z. H. Xu, G. Shen, and S. Lin, "Image encryption algorithm based on chaos and S-boxes scrambling," *Adv. Mater. Res.171172*, pp. 299–304, 2011.

[68] C. J. Benvenuto, "Galois Field in Cryptography.," *Univ. Washingt.*, 2012.

[69] F. Sattar and M. Mufti, "Spectral characterization and Analysis of Avalanche in Cryptographic Substitution Boxes using Walsh-Hadamard Transformations," *Int. J. Comput. Appl.*, vol. 28, no. 6, 2011.

[70] A. F. Webster and S. Tavares, "On the design of S-boxes. In: Advances in Cryptology, Lecture Notes in Computer Science," in *Proceedings of CRYPTO'85*, 1986, pp. 523–534.

[71] S. Saraireh, "A secure data communication system using cryptography and steganography," *Int. J. Comp. Networks Comm.*, vol. 5, no. 3, pp. 125–137, 2013.

[72] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," *Nonlinear Dyn.*, vol. 73, no. 3, 2013.

[73] B. J. Mohd, S. Abed, B. Naami, and T. Hayajneh, “Hierarchical steganography using novel optimum quantization technique,” vol. 7, no. 6, pp. 1029–1040, 2013.

[74] R. Crandall, “Some Notes on Steganography,” *link: http://dde.binghamton.edu/download/Crandall matrix.pdf*, 1998. .

[75] N. Provos and P. Honeyman, “Hide and seek: An introduction to steganography,” *IEEE Secur. Privacy*, vol. 1, no. 3, pp. 32–44, 2003.

[76] A. Kanso and H. S. Own, “Steganographic algorithm based on a chaotic map,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 8, pp. 3287–3302, 2012.

[77] K. Bailey and K. Curran, “An evaluation of image based steganography methods,” *Multimed. Tools Appl.*, vol. 30, pp. 55–88, 2006.

[78] P. . H. and S. rovos, N., Honeyman, “An introduction to steganograaphy,” *, IEEE Secur. Priv.*, vol. 1, no. 3, pp. 32–44, 2003.

[79] L. Yu, Y. Zhao, R. Ni, and T. Li, “Improved adaptive LSB steganography based on chaos and genetic algorithm,” *EURASIP J. Adv. Signal Process.*, 2010.

[80] D. Bandyopadhyay, K. Dasgupta, J. K. Mandal, and P. Dutta, “A novel secure image steganography method based on chaos theory in spatial domain,” *Int. J. Sec. Pri. T. Man.*, vol. 3, no. 1, pp. 11–22, 2014.

[81] A. Cheddad, J. Condell, K. Curran, and P. . Kevitt, “Digital image steganography: Survey and analysis of current methods,” *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.

[82] M. Ghebleh and A. Kanso, “: A robust chaotic algorithm for digital image steganography,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 6, pp. 1898–1907, 2014.

[83] M. Aziz, M. H. Tayarani-N, and M. Afsar, “A cycling chaos-based cryptic-free algorithm

for image steganography," *Nonlinear Dyn.*, vol. 80, no. 3, pp. 1271–1290, 2015.

[84] M. Baptista, "Cryptography with chaos.," *Phys. Lett. A*, vol. 240, no. 12, pp. 50–54, 1998.

[85] Z. Dawei, C. Guanrong, and L. Wenbo, "A chaos-based robust wavelet-domain watermarking algorithm," *Chaos, Solitons and Fractals*, vol. 22, no. 1, pp. 47–54, 2004.

[86] X. Y. Wang, X. J. Wang, J. F. Zhao, and Z. Zhang, "Chaotic encryption algorithm based on alternant of stream cipher and block cipher," *Nonlinear Dyn.*, vol. 63, no. 4, pp. 587–597, 2011.

[87] C. Lia, S. Lib, M. Asimc, J. Nunezd, G. Alvarezd, and G. Chena, "On the security of an image encryption scheme," *Image Vis.Comput.*, vol. 11, no. 2, p. 2007/090, 2007.

[88] M. I. Sobhy and A.-E. R. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *IEEE International Conference on Acoustics, Speech, and Signal Processing*, 2001, vol. 2, pp. 1001–1004.

[89] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems.," in *Proceedings of the 3rd International Workshop on Information Hiding*, 2000.

[90] N. Provos, "Defending against statistical steganalysis," in *Proceedings of the 10th USENIX Security Symposium , Washington, DC, USA*, 2001, pp. 323–335.

[91] S. Dumitrescu and X. Wu, "A new framework of LSB steganalysis of digital media," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3936–3947, 2005.

[92] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–184, 2014.

[93] A. Anees, A. M. Siddiqui, J. Ahmed, and I. Hussain, "A technique for digital steganography using chaotic maps," *Nonlinear Dyn.*, vol. 75, no. 4, pp. 807–816, 2013.

[94] J. Fridrich and J. Kodovsky, "Rich models for steganalysis of digital images," *IEEE*

Trans. Inf. Foren. Sec., vol. 7, no. 3, pp. 868–882, 2012.

[95] S. Farwa, T. Shah, and L. Idrees, "A highly nonlinear S‑box based on a fractional linear transformation," *Springerplus*, vol. 5, no. 1, p. 1658, 2016.

[96] J. Y. Chen, K. W. Wong, L. M. Cheng, and J. W. Shuai, "A secure communication scheme based on the phase synchronization of chaotic systems," vol. 508, no. 2003, 2013.

[97] S. S. Jamal, T. Shah, and I. Hussain, "An efficient scheme for digital watermarking using chaotic map," *Nonlinear Dyn.*, vol. 73, no. 3, 2013

[98] P. M. Cheddad, A. Condell, J., Curran, K., Kevitt, "Digital image steganogra- phy: Survey and analysis of current methods, Signal Process.," vol. 90, no. 3, pp. 727–752, 2010.

[99] M. Ghebleh and A. Kanso, "A robust chaotic algorithm for digital image steganography.," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 6, pp. 1898–1907, 2014.

[100] D. Asatryan and N. Asatryan, "A Combined Spatial and frequency Domain watermarking," in *Proceedings of 7th International Conference on Computer Science and Information Technologies*, 2009, pp. 323–326.

[101] S. V. Joshi, A. A. Bokil, N. K. Jain, and D. Koshti, "Image steganoraphy Combination of Spatial and Frequency Domain," *Int. J. Comput. Appl.*, vol. 53, no. 5, pp. 25–29, 2012.

[102] A. Anees and A. M. Siddiqui, "A technique for digital watermarking in combined spatial and transform domains using chaotic maps," in *IEEE 2nd National Conference on Information Assurance (NCIA)*, 2013, pp. 119–124.

[103] A. Anees, A. M. Siddiqui, and I. Hussain, "A technique for digital steganography using chaotic maps.," *Nonlinear Dy- namics*, vol. 75, pp. 807–816, 2013.

Turnitin Originality Report

Algebraic and Chaotic schemes to synthesis S-boxes and their applications in multimedia security. by Sajjad Shaukat Jamal

From Theses (QAU theses)

- Processed on 06-Aug-2018 09:23 PKT
- ID: 987859667
- Word Count: 34283

Similarity Index
14%
Similarity by Source

Internet Sources:
6%
Publications:
11%
Student Papers:
4%

16/8/2018
Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

sources:

1 1% match (publications)
Hussain, Iqtadar, and Tariq Shah. "Literature survey on nonlinear components and chaotic nonlinear components of block ciphers", Nonlinear Dynamics, 2013.

2 1% match (publications)
Iqtadar Hussain, Naveed Ahmed Azam, Tariq Shah. "Stego optical encryption based on chaotic S-box transformation", Optics & Laser Technology, 2014

3 1% match (publications)
Nargis Bibi, Shabieh Farwa, Nazeer Muhammad, Adnan Jahngir, Muhammad Usman. "A novel encryption scheme for high-contrast image data in the Fresnelet domain", PLOS ONE, 2018

4 1% match (Internet from 08-Mar-2018)
https://springerplus.springeropen.com/articles/10.1186/s40064-016-3298-7

5 1% match (Internet from 02-Mar-2017)
http://crypto.math.uni-bremen.de/Arbeiten/dipljanson.pdf

6 < 1% match (publications)
Tariq Shah, Dawood Shah. "Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over Z2", Multimedia Tools and Applications, 2018

7 < 1% match (publications)
Iqtadar Hussain. "A group theoretic approach to construct cryptographically strong substitution boxes", Neural Computing and Applications, 04/06/2012

8 < 1% match (student papers from 19-Jan-2017)
Submitted to Higher Education Commission Pakistan on 2017-01-19

9 < 1% match (publications)
Amir Anees, Adil Masood Siddiqui. "A technique for digital watermarking in combined spatial and transform domains using chaotic maps", 2013 2nd National Conference on Information Assurance (NCIA), 2013

10 < 1% match (student papers from 25-Apr-2017)
Submitted to Higher Education Commission Pakistan on 2017-04-25

11 < 1% match (student papers from 11-Nov-2016)
Submitted to Higher Education Commission Pakistan on 2016-11-11

< 1% match (Internet from 16-Oct-2016)

13/8/18
KHALID BASHIR MIRZA
Assistant Librarian
DRSM LIBRARY
Quaid-i-Azam University
ISLAMABAD