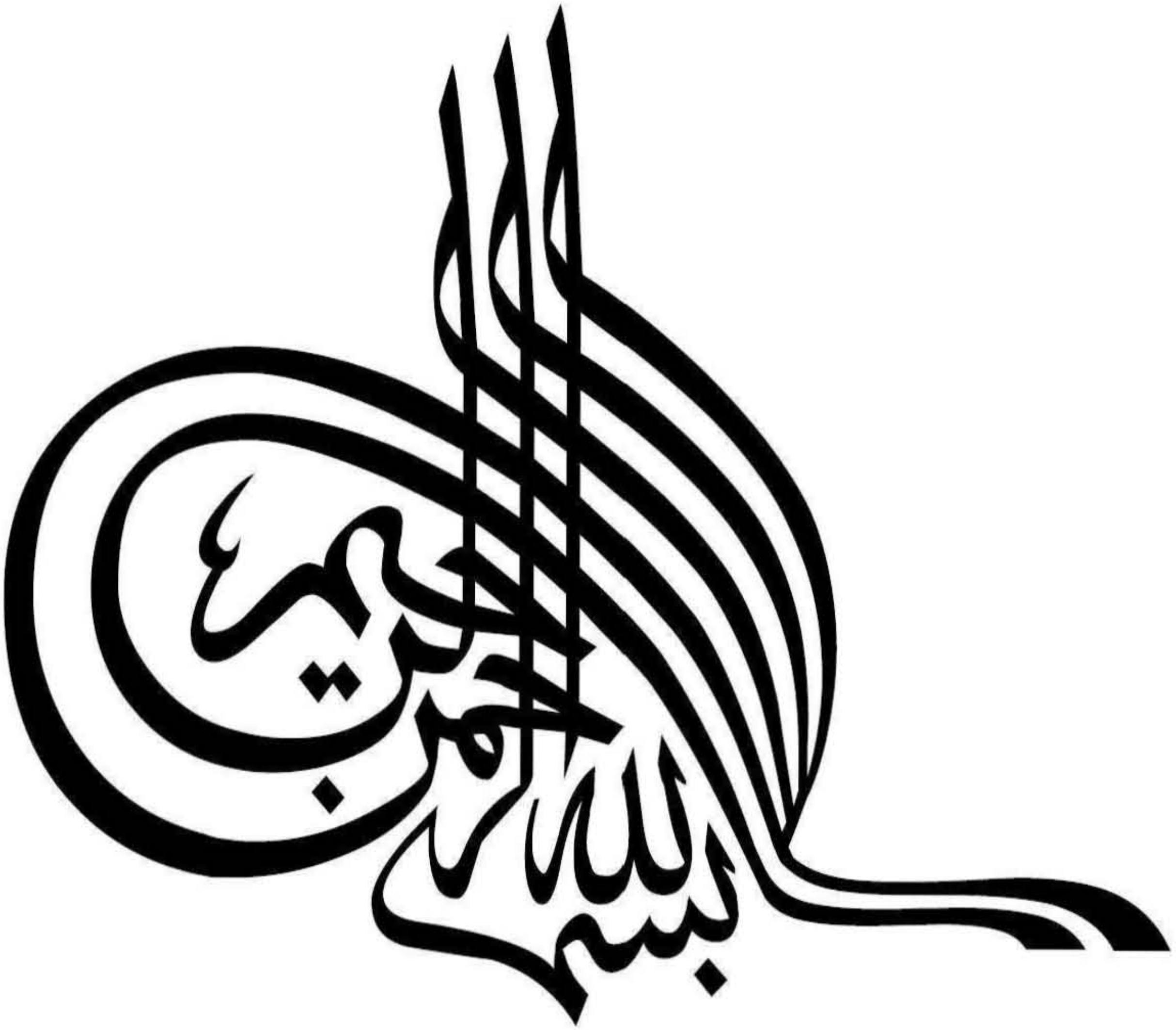


In the name of Allah,
the Most Beneficent,
the Most Merciful

Cryptosystems Designs over Random Number Generator and Chaos Theory: Image Encryption Applications

By

Dania Saleem Malik

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2021

Cryptosystems Designs over Random Number Generator and Chaos Theory: Image Encryption Applications

By

Dania Saleem Malik

Supervised

By

Prof. Dr. Tariq Shah

Department of Mathematics

Quaid-i-Azam University

Islamabad, Pakistan

2021

Cryptosystems Designs over Random Number Generator and Chaos Theory: Image Encryption Applications

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

Doctor of Philosophy
in
Mathematics
By

Dania Saleem Malik

Department of Mathematics
Quaid-i-Azam University
Islamabad, Pakistan
2021

Author's Declaration

I, **Dawood Shah,** hereby state that my PhD thesis titled **Finite Field Computation and Their Applications in Data 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: **Dawood Shah**

Date: **30-Aug-2021**

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled "**Finite Field Computation and Their Applications in Data 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: **Dawood Shah**

Finite Field Computation and Their Applications in Data Security

By

Dawood Shah

CERTIFICATE

A THESIS SUBMITTED IN THE PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF THE

DOCTOR OF PHILOSOPHY IN MATHEMATICS

We accept this thesis as conforming to the required standard

1. Snadeem

Prof. Dr. Sohail Nadeem
(Chairman)

2. Tariq Shah

Prof. Dr. Tariq Shah
(Supervisor)

3. Akbar Azam

Prof. Dr. Akbar Azam
(External Examiner)

Department of Mathematics, COMSATS University, Park Road Chak Shahzad, Islamabad.

4. Tahir Mahmood

Dr. Tahir Mehmood
(External Examiner)

Department of Mathematics & Statistics International Islamic University, Sector H-10 Islamabad.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2021

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **Finite Field Computation and Their Applications in Data Security** was conducted by **Mr. Dawood Shah** under the kind supervision of **Prof. Dr. Tariq Shah**. No part of this thesis has been submitted anywhere else for any other degree. This thesis is submitted to the Department of Mathematics, Quaid-i-Azam University, Islamabad in partial fulfillment of the requirements for the degree of Doctor of Philosophy in field of Mathematics from Department of Mathematics, Quaid-i-Azam University Islamabad, Pakistan.

Student Name: **Dawood Shah** Signature: Shah

External committee:

a) **External Examiner 1**: Signature: Akbar Azam
Name: **Prof. Dr. Akbar Azam**
Designation: Professor
Office Address: Department of Mathematics, COMSATS University, Park Road Chak Shahzad, Islamabad.

b) **External Examiner 2**: Signature:
Name: **Dr. Tahir Mehmood**
Designation: Assistant Professor
Office Address: Department of Mathematics & Statistics, Faculty of Basics Applied Sciences International Islamic University, Islamabad.

c) **Internal Examiner** Signature: Tariq Shah
Name: **Prof. Dr. Tariq Shah**
Designation: Professor
Office Address: Department of Mathematics, QAU Islamabad.

Supervisor Name: Signature: Tariq Shah
Prof. Dr. Tariq Shah

Name of Dean/ HOD Signature: Nadeem

Prof. Dr. Sohail Nadeem

This Thesis Is Dedicated To

My Affectionate Parents

For making me what i am today

Without whom none of my success would be possible

and

My Siblings

For their unconditional love, endless support and Encouragement
because their prayers, sympathies steer my way towards success

Acknowledgements

First and foremost, all praise and gratitude to **Allah Subhanautalaah**, the propitious, the benevolent, the most merciful, the greatest of all, for giving me determination and strength to do my research. His continuous grace and mercy were with me throughout my life and ever more during the tenure of my research. Countless salutation be upon His last prophet **Hazrat Muhammad (Swala Allahu Alaih Wassllam)**, who bestowed us the perfect code of life. Respect and Gratitude to my spiritual mentor **Khawaja Fazal Shah Kalyami**.

The work presented in this thesis was accomplished under the animate directions, observant pursuit, intellectual support and enlightened supervision of **Prof Dr. Tariq Shah**. I am grateful to his ever inspiring guidance, keen interest, scholarly comments and constructive suggestions throughout my research work. Indeed, I am indebted to his valuable advice which always served as a beacon of light to get me through all the difficulties of research work. I deem it my utmost pleasure in expressing my gratitude with the profound benedictions to Dean of department **Prof. Dr. Sohail Nadeem** for providing me research facilities.

I am also thankful to all respected teachers and friends especially **Sumaira, Saadia, Aini, Zikra,** and **Hina** for encouraging me all the time. I pay my profound gratitude and indebtedness to **Sir Ehtisham** for his valuable guidance whenever needed.

I have no words to acknowledge sacrifices, efforts, encouragement and firm dedication from my affectionate father throughout my academic career and life, who made me what i am today. I can’t express my love for my caring mother, who is the angel that constantly watches over my head and whose prayers always give me strength to hold-on. Many thanks to my siblings who helped me to achieve success in every sphere of life progressively through their endless patience, support and encouragement.

Dania Saleem Malik

Preface

Due to rapid developments in communicational networks, transmission of massive data by means of them has increased risk of security in multimedia information. For protecting information, data encryption plays a significant role. So, cryptography provides a platform to secure information. Cryptographic modern approaches are mainly focused on block-based encryption techniques which includes “Advance Encryption Standard” and “Data Encryption Standard”, abbreviated as “AES and DES”. But these modern approaches are valuable for textual information. However, owing to massive data transmission in the form of images, these techniques have failed in providing sufficient security due to lack of their efficiency for bulk data and randomness. Therefore, security of images is very challenging. Researchers have been concerned more than ever to secure multimedia information with modern and effective content preservation strategies to face this challenge.

From past few decades, many techniques to encrypt images were proposed, and it is found that the encryption techniques based on chaos are most effective. Since the chaotic non-linear systems have some important features like initial and parametric values, sensitivity, randomness, and unpredictability which renders them suitable for encryption of images. In this perspective, the need of hour is to design secure chaos-based cryptosystems which ensure authentication, confidentiality, and integrity of data before transmission. The chaos-based systems offer an appropriate source for abundant pseudorandom sequences generation and are useful to construct encryption nonlinear components.

The Substitution boxes commonly known as S-boxes are crucial non-linear components in block-ciphers, which plays a key role in multimedia cryptosystems security. The nonlinear S-boxes provide effective security to cryptosystems. For this reason, many encryption schemes for protecting image information use S-boxes in substitution phase where the values of plaintext are replaced with S-boxes to enhance the confusion and make it attack resistant.

Moreover, our focus is on confidentiality of content and controlling access that is addressed in encryption, which is only accessible to the parties who have keys for decryption to read the transmitted content (plain-image).

The proposed thesis objective is to design cryptosystems that use chaos and random numbers for strong encryption techniques to obtain ciphered images having excellent attack resistant properties.

In this perspective, the random numbers and chaos-based techniques have been addressed. Firstly, a hybrid-pseudorandom binary numbers generation (abbreviated as HPRNG's) is proposed. The HPRNG's is obtained by feedback shift registers in combination with modified quadratic chaotic map. Since the numbers generated by only feedback shift registers are easily hacked and are not having strong resistance so the modified quadratic chaotic map bits are added to feedback shift register in every cycle. Then the binary streams are used in construction of cryptographically strong block ciphers (S-boxes). The S-boxes are analyzed and tested using different testing techniques commonly used in literature like Nonlinearity, Avalanche criterion, Bit independency etc., which depicts their strong performance. After this, a permutation substitution-based encryption technique is presented. As in literature review, a lot of techniques based on permutation substitution phases have lack of key and image pixels association property, so they are easily hacked. This flaw is overcome in proposed encryption technique by creating a relation between the image pixels and keys.

Secondly, in design of strong cryptosystems, key is the main component. Because if the hacker gets any idea about the key, he can easily hack the algorithm. So, the focus of work is on the generation of strong keys. For this, some encryption techniques based on game rules (like chess-board game knight movement) and convolution codes along with chaos are presented. Apart from single encryption techniques, cryptosystem algorithms for multiple images encryption have also been designed. Thus, in last a multiple images encryption scheme is proposed. The most overwhelmed feature of these encryption algorithms is that they are not only easy to implement but also offers high level of security that make it resistant against brute force attacks.

A detail evaluation of these schemes is done via different analysis that includes Entropy, adjacent correlation between pixels, histograms, histogram variance, differential attacks, key space, and key sensitivity analysis to ensure their robustness. Also, cropping attacks, Noise and pepper attacks are done and there Mean square error (MSE), Peak signal to noise ratio and similarity structural indices are calculated that illustrates the high security level of proposed scheme. Moreover, the differential cryptanalysis is executed for proving the effectiveness of proposed schemes. The entropy values of proposed techniques are near the optimal value 8, which shows high randomness of proposed techniques. Correspondingly, to examine that the proposed encryption scheme has excellent statistical properties that help in the resistance of many attacks, we will analyze it by NIST SP 800-22.

The comparison of proposed schemes with some well-defined related schemes is also presented. Comparison results illustrates that the proposed encryption algorithms have better performance than other. Statistical and experimental simulation results depict that the proposed encryption techniques have all desirable characteristics like flexibility, efficiency, and high resistance against attacks like cryptanalysis.

Table of Contents

Chapter 1

Preliminaries

In this chapter, some basic concepts, definitions, and cryptographic background to understand concept of asymmetric cryptosystems is offered. In the start of this chapter, motivations, objectives, scope, contributions, and the layout of whole thesis is presented. Furthermore, terms and primitives of cryptography, are discussed. After that, a detailed review about hash function-based cryptography, block-ciphers, and generation of random numbers is done. Lastly, a detailed review and security principles of image encryption and chaos are explained.

1.1 Overview

With rapid innovations in development of data transmission, it has become a demanding challenge to secure confidential information from attackers or prohibitive actions. Exchange of data closely relate to the existence, like, commerce, military, financial affairs, money kept in phones, and telecasting of news [1]. Through modern multimedia progression technologies and telecommunications, a large amount of important information cruises in daily life by means of sharing and open networking. To transmit data across any ambiguous channel, few cryptographic techniques (encryption) are needed, which change consistent information to impenetrable form. Cryptography modern approaches are valuable for textual information. However, because of high-level redundancy and capacity of bulk information, they failed in providing computational based security [2].

1.2 Research Motivations

Since in many communicational networks, images are exchanged and huge digital information in them is either private or confidential. Researchers have been concerned more than ever to secure multimedia information with modern and effective content preservation strategies to face this challenge [3]. Many different features are involved in digital images security that includes protection from copyrighting, confidentiality, access control, and authentication. In general, our focus is on confidentiality of content and controlling access that is addressed in encryption, which is only accessible to the parties who have keys for decryption to read the transmitted content (plain-image).

In context of this, some encryption algorithms based on number theory techniques for encryption like DES (Data Encryption Standard) RSA (established by Rivest, Shamir and Adleman) and IDEA (International Data Encryption Algorithm) [4]. Nevertheless, such encrypting techniques are not suitable for applications of images, because of few important image features (like massive capacity of data, redundancy high values). Moreover, such schemes for encryption requires a lot of operations on compressed information therefore the demand for time is high. In communications of real time, owing to their low speeds for encipherment (encryption) and decipherment(decryption), they can introduce significant potential. The focus of this dissertation is on the application of encrypting images.

1.3 Objectives of Research

Since the chaos theory plays a vital role in most of encryption schemes because of their high sensitivity, randomness, complexity, and power of computations. Digital images have such characteristics that includes high redundancy, adjacent pixels strong correlations, and less sensitivity in comparison with text data. Shannon's presented the idea of using chaos in encryptions [5]. Chaos application in cryptography was biggest contribution for security improvement because of chaos excellent properties (like sensitive behavior, initial conditions dependence.

The cryptography based on chaos relies on nonlinear dynamical complex systems which are simple but deterministic. So, for this reason chaos provide secure and fast communication for protecting data, which are quite important for transmitting multimedia data through channels having fast communicating systems i.e., internet broadband communication.

The proposed thesis objective is to design cryptosystems that use chaos and random numbers to design strong encryption techniques to obtain ciphered images having excellent properties. In this perspective, the random numbers and chaos-based techniques have excellent performance. Proposed ciphered images statistical confusion diffusion properties are good. The correlation between pixels of encrypted images is near zero. In short, presented encryption schemes achieve good multimedia security performance.

1.4 Research Scope

Simple color images are used in proposed work. The main aim of proposed work is to provide techniques for encryption having large size of key, randomness, high complexity, and speed for the enhancement of performance.

1.5 Contributions of Dissertation

Prime goals of this dissertation are as follows:

1. In many cryptographic applications, random numbers are a need of hour for strong cryptosystem designs. In this context the proposed work is based on hybrid binary pseudorandom numbers generator (HPRNG) derived from feedback shift register known as Linear feedback shift register (abbreviated as LFSR) and modified quadratic chaotic map. Since the LFSR based PRNG's are not resistant against the attacks and reveals information about keys so to overcome this flaw the binary stream of random numbers obtained from LFSR are Xored with the random stream of modified quadratic chaotic map.
2. As the cryptographically strong substitution boxes (S-boxes) have an important feature like nonlinearity so the generation of S-boxes using nonlinear sequences is addressed in this work. To design S-box, binary stream of numbers generated by HPRNG's is used. After conversion of bits to bytes an S-box is achieved. Then strength of attained S-box is analyzed via Non-linearity (NL), Strict Avalanche effect (SAC), Bit independence criteria (BIC), Differential and Linear approximation Probability (DP, LP) which ensures that S-box is cryptographically strong and has high performance.
3. Technique for encrypting images based upon the chaos (i.e., chaotic map) and the S-box obtained in 1 is presented. Image encryption schemes based on S-box have some drawbacks such as lack of security against attacks and low complexity. To overcome this flaw a strategy to associate sequences of key with cipher-text of image is presented in proposed encryption algorithm for the substitution and permutation phase which renders it resistant against classical attacks.
4. To further enhance the security of encryption scheme, some new techniques based on the game rules (i.e., chess board game knight movement) and convolution codes are presented. A strong key generation is the main component of encryption schemes because the efficiency and security lie upon it. Focus of proposed work is to design algorithm for transmitting image data safely through any untrusted channel. In the proposed scheme initial conditions of chaotic keys are randomly generated by adapting image information to attain the image high sensitivity by increasing the amount of randomness in pixels.
5. The above-mentioned schemes are tested via different analysis such as histograms, histogram variances, Sensitivity of key, key space, adjacent pixels correlation measurements, Entropy, Differential attacks (Number of cipher image pixels rate change

(NPCR) and plain and ciphered images difference of average intensities (UACI)), quality of image measures, cropping attacks, Noise and pepper attacks that illustrates the high security level of proposed scheme. Also, the differential cryptanalysis is executed for proving the effectiveness of proposed schemes.

6. Correspondingly, to examine that the proposed encryption scheme has excellent statistical properties that help in the resistance of many attacks, we will analyze it by NIST SP 800-22.

1.6 Thesis Structure

The dissertation is divided into six chapters.

In Chapter 1, some basic background definitions, introduction, motivations of proposed work are provided. Also, detailed explanation of image encryptions and chaos theory is given in this chapter. Furthermore, the current research in encryption of images is also highlighted.

Chapter 2 presents a random number based strong S-box technique and its application in image encryption. In this chapter, we present a novel technique for generating sequences of random numbers then by using these sequences an S-box is obtained. Furthermore, this S-box in combination with binary sequence attained from chaotic map is used in security of image information.

In Chapter 3, cryptosystem design for the encryption of digital images is presented. Main contribution of this work is to design a model for scrambling image pixels. One-time pad keys are generated by the chaotic keys and plain image hash values. Simulation results and experimental analysis ensure the security of proposed scheme.

Chapter 4 introduces a block-wise RGB encryption scheme in which sequence of random numbers are generated via four-dimensional chaotic map. In this approach, to enhance proposed scheme security, the key is related with the pixels of plain-image using convolution codes. Also, the efficiency and strength of proposed scheme is analyzed by comparing it with some other encryption techniques.

After the single image encryption techniques, a multiple color image encryption scheme is offered in Chapter 5.

Finally, overall conclusion and future directions are given in Chapter 6.

1.7 Fundamentals of Cryptography

Currently, our society is strongly bounded by the domain of the information epoch, which classified by scholar and researcher assets and is functional inside data being deliberated priceless. Enlightening data exists which is used in various forms such as economic, military, and political. The protection and security of this data during transmission, saving and in routine practice is of prime importance because transfer of data may result in the revelation of various marketing, financial loss, or armed forces top secrets. Hence, the data should be secure while transmission, sensitive data like credit cards, banking transactions and social security numbers must be secure. For the protection and security of the data or information, cryptography plays a vivacious role [6]. Cryptography is study of protecting information or data. In other way, cryptography is study of converting data in secret codes or encrypting information or data which you want to hide from others. From aged time to current era, during time of war the facility to interconnect secretly has been significant. Cryptography is Greek word which means "Secret writing". The art to personate a message cryptography plays vital role so that only its legal successor has ability to recognize it. There are two thresholds to this course. In first way, the plaintext, or original data, is veiled. This is recognized as encryption. The reverse procedure in which the cipher text is decoded backward into original message must be known to authentic recipient. This process is known as decryption. The cryptographic keys or key mandatory for both encipherment and decipherment.

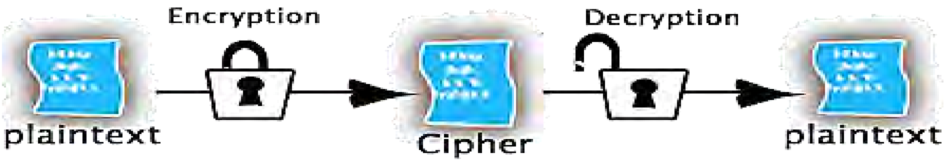


Figure 1.1: Pictorial representation of encryption and decryption

1.7.1 Components of Cryptography

The methodical learning of any regulation essentially constructed upon difficult classifications arise from basic perceptions. Some basic concepts used in cryptography are followed in this section [7].

- **Plaintext**

Any conversation within the language that we say the mortal language, which took the shape of plain text. It is implicit by the sender, receiver and those who have approach to that message.

- **Ciphertext**

Cipher signifies a secret or unreadable message. While any appropriate scheme is applied over the plain text to codified it, then the resulting codified message is known as cipher text.

- **Encryption**

The process of converting plain text messages into cipher text is known as encryption.

- **Decryption**

An inversion procedure for converting messages of cipher text behind the plain text is known as decryption.

- **Key**

A key is a vital characteristic of performing encipherment and decipherment. To make cryptographic procedure secure, key is utilized for both encryption and decryption.

1.7.2 Categories of Cryptography

Cryptography has been categorized into two forms:

1. **Symmetric (Private) key Cryptography**
2. **Asymmetric (Public) key Cryptography**

1.7.2.1 Symmetric key Cryptography

This category involves a person whom the secret key should be known. Both the receiver and sender of message may also be kept it. In private key cryptography both receiver and sender each have copy of secret key. In this instance, during this passage approach to the key is vouchsafe. There are two set-ups to ponder, in first both the interactive parties are acquainted with each other. In this situation, without any encrypting scheme the key is shared. In second case, familiarity is limited. For example, when seeing secure website, keys should be swapped in a secure way [8]. Symmetric key cryptography is further classified in to two categories, Block cipher and Stream cipher.

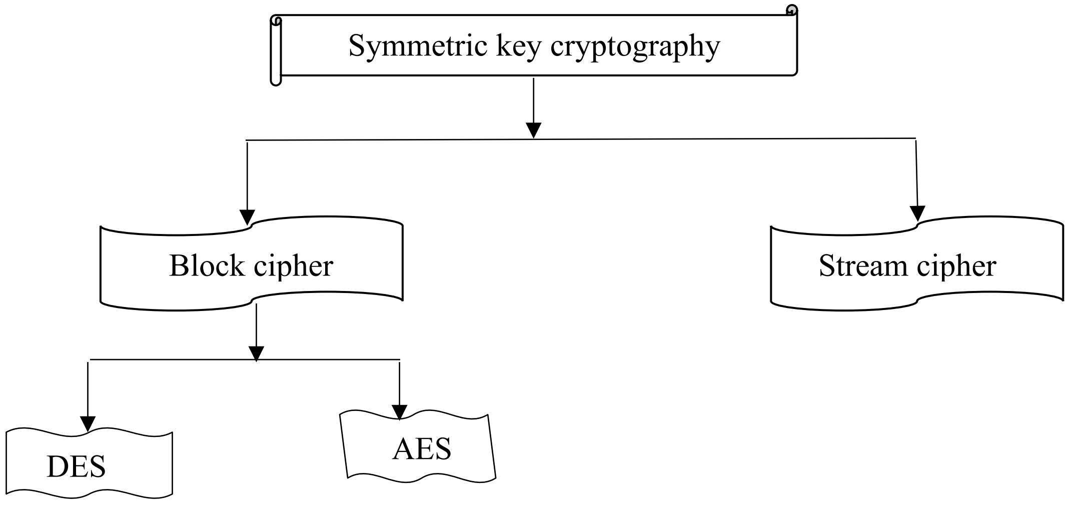


Figure 1.2: Symmetric key cryptography

1. Stream Cipher

In stream cipher one-bit stream digital data should be encrypted at a time. In standard cryptography stream ciphers example is Vigenere cipher auto keyed and example of stream cipher in modern cryptography is RC4. If keystream cryptographic is haphazard, then it is difficult to break this cipher by some means besides to find the keystream. Though, in advance the keystream should be known to both sender and receiver via some independent and confident channel. In programing techniques stream cipher is modest and relatively quicker. It presents incredible logistical problems if the proposed data traffic is large. For concrete reasons, the generator of bit-stream necessarily executed as an algorithmic procedure, hence the bit-stream cryptography bit stream could be designed by both sender and receiver. In this tactic, the generator bit-stream is a key-controlled process which produce a cryptographically robust bit stream. Present, both the users' only need to share the generating key, and everyone could produce the keystream.

2. Block Ciphers

Block ciphers are very important in private key-based r symmetric cryptosystems, where the key is only known to sender and receiver. Block cipher refers to group of bit sequences having fixed lengths named as blocks, where defined length input bit sequences (labeled as plain text) are converted by using complex operations into output of accurately same length bit sequences (designated as cipher text) [9].

The common examples of block cipher are Advanced Encryption Standard (AES) and Data Encryption Standard (DES).

a) **DES:** Data encryption standard is one of the ancient techniques in symmetric block cipher. In 1976, to encounter National Bureau Standards (NBS) criteria for encryption system, DES was authoritatively standardized. In methodology of DES symmetric block cipher encrypted data in length of 64 bits block. It occupies length key of 56 bit which is articulated as number of 64 bits. In each byte, the last bit behaves as parity check for preceding 7 bits [10].

b) **AES:** Like DES, AES is symmetric block cipher. In AES, for encryption and decryption same key would be used. Moreover, AES differs from DES in numerous ways. The Rijndael technique allows many block and key sizes, not just for the blocks of DES of 64 and 56 bits and size key. The key and block could be elected independently from 128, 160, 192, 224, 256 bits which are not necessarily same. But the AES standard stated that the algorithm could only admit a block of 28 bits size and a selection of three keys 128, 192 and 256 bits [11].

1.7.2.2 Asymmetric key Cryptography

Cryptography of asymmetric key is usually termed as 'cryptographic Public key'. In asymmetric key cryptography, two keys are used. One is known as 'Public key' that could be spontaneously shared over insecure channel also the other key that could be kept secret and not easily shared is termed as 'Private key' [12].

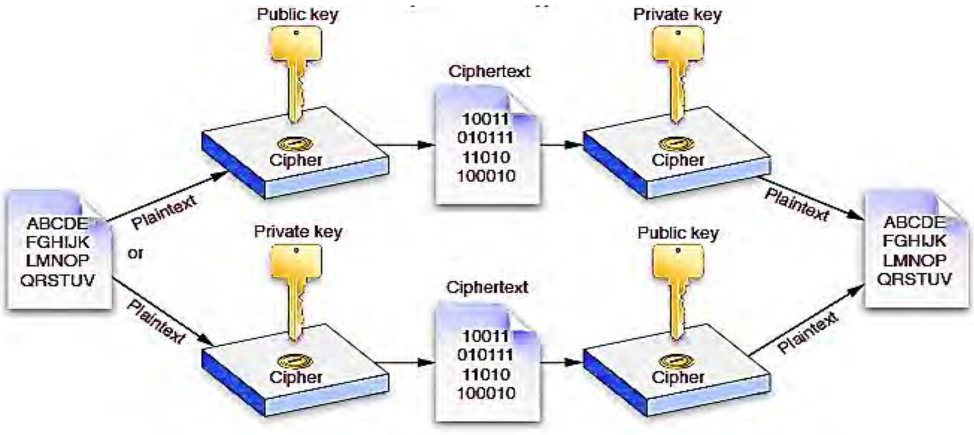


Figure 1.3: Asymmetric Encryption

1.7.3 Purposes of Cryptography

Cryptography not only plays a role in encrypting and decrypting messages, but it also used to hoist real-world complications that need safety for information or data [13]. In current cryptography, that four main purposes that arise are as follows.

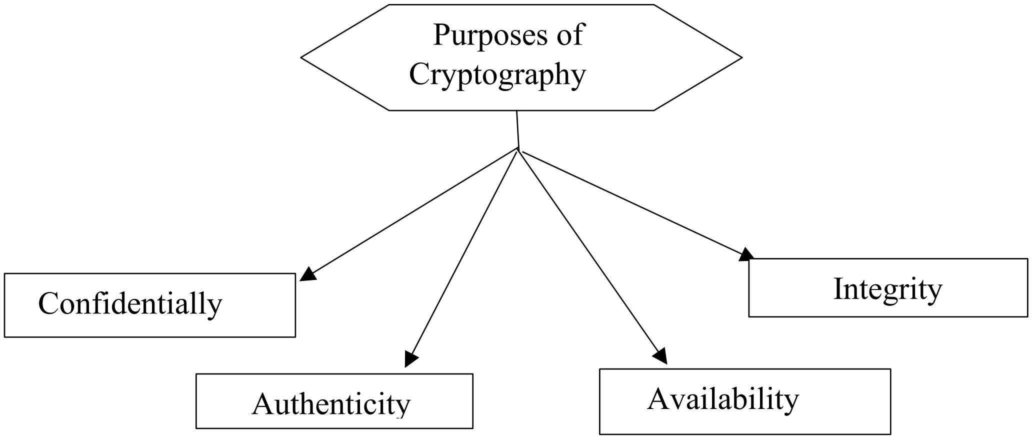


Figure 1.4: Cryptographic purposes

- **Confidentially**

Two connected concepts covered in this term,

a. **Data confidentiality:** Non-availability or revelation of private or confidential data to unlawful folks is guaranteed.

b. **Privacy:** Assured the individual's authority that, what kind of information associates with them might be collected and accrued, by whom and to whom that type of information might be shared.

- **Integrity**

Integrity involves the following:

a. **Data integrity:** Assured that data or information is rehabilitated merely in a specific and lawful way.

b. **System integrity:** A guaranteed system that accomplish proposed function in an unaffected manner, which is free from unintentional illegal exploitation of system.

- **Authenticity**

The competence of communicating revels to recognize, each other and the source of the message.

- **Availability**

The accessibility of computer scheme to certified parties on requirement.

1.8 Modern Cryptographic Tools

Before 1950, like an art cryptography was known, but current cryptography depends on discipline which requires provision from various fields which includes electronics, mathematics and computer science. After World War *II,* cryptographic research area had found the great importance by military intelligence forces. After 2 years, in 1970's the first symmetric cryptosystems i.e., public key ciphers and DES were invented. At that time, the algorithms were established with the help of computers. Then researchers recognized that worthy ciphers were established by joining small tools. These tools are as follows:

1.8.1 Substitution

In cryptography, the process of replacing one symbol with another symbol is known as substitution. In standard cryptography, the substitution cipher example is Caesar Shift Chip in which every plaintext letter should be substituted by the letter three places further down in the alphabet.

1.8.2 Permutation

From a set an exact arbitrary reallocation of its two members is termed as permutation.

1.8.3 Diffusion and Confusion

To create disorder in data to make it more secure, Shannon presented two concepts confusion and diffusion for a good cryptosystem [14]:

- Diffusion is a technique in which if we alter a single plaintext bit it creates alternation in several cipher text bits. Similarly, alter of single bit of cipher text creates alternation in many plaintext bits. In case of block ciphers, bit alternation is communicated with the assistance of diffusion, from unique part of the block to other parts.
- Confusion produces a relationship between secret key and plain text. In confusion key is not directly related to cipher text. In general, every cipher text character should depend on many chunks of keys.

1.9 Substitution Boxes

In the sphere of information and computer technology, the unified algebraic perceptions have notable impacts. In cryptography, the safety of information or data highly depends on substitution progression. Substitution is basically non-linear renovation which executes 'bits' disorder. The substitution boxes (S-boxes) play a very vital role in cryptosystem. Strong cryptosystem should be given by substitution due to its confusion property given by Shannon. He proposed that by substitution combining with transposition constantly strong ciphers can be formed. The block ciphers of early time were the simplest networks which merge the circuits of substitution, permutation and termed as SPN (substitution permutation networks). For the model of block ciphers to give a non-linear connection between input binary bits and output binary bits, S-boxes are mainly included in it to create misperception and confusion [15].

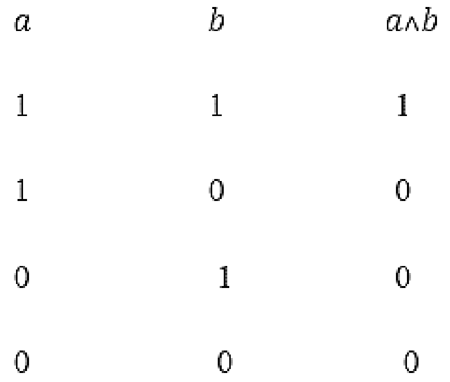
An S-box is an $r \times s$ mapping $t: \mathbb{Z}_2^r \rightarrow \mathbb{Z}_2^s$ from r input binary bits to s output binary bits, having number of 2^r and 2^{s} inputs and outputs, respectively. Generally, S-boxes are lookup tables that map n binary bits to m binary bits. S-box dimension has a consequence on the individuality of the input and output, which may distress the S-box properties. For an S-box having dimension $r \times s,$ where if $r < s$ then the amount of binary input bits is superior from binary output bits, so there should be a repetition in the entries of S-Box. Nevertheless, if $r = s,$ then there is a bijection in S-box, i.e., the input values mapped on unique output values and the entries of S-box are distinct [16]. S-boxes having both injection and surjection properties are usually referred as bijective S-boxes that are reversible, which shows the existence of the inverse S-box for these S-boxes. The momentous lot of time spent on designing and analyzation of the S- boxes because of its nonlinear component which is the most important part of the algorithm to provide strength. Hence, every weakness in S-boxes can consequently lead to easily intercept able cryptosystems [17] - [18].

The robustness of cryptographic algorithms is based on nonlinear integrant of the process. Therefore, erection of cryptographically robust S-box plays a vibrant role in the proposal of protected cryptosystems. For safety and secure communication, diverse type of S-box has built, which built on applied and algebraic erections. S-boxes built on algebraic erection have more fascination owing to their robust cryptographic features. In cryptographic literature, a lot of S-boxes constructed over Galois field having strong resistance against algebraic attacks. Also, the erection of S-boxes over Galois ring and maximal cyclic subgroup of unit elements is firstly presented by Shah et al [19]. When designed S-box is presented, it is crucial to analyze the assets revealed by them. For newly constructed S-boxes, their encryption strength could be checked by the assistance of the consequences from algebraic and statistical analysis.

1.10 Logic Operations

- **AND Operation**

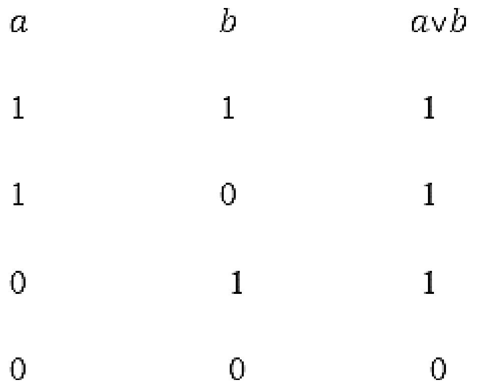
In this operation consider $T = \{0,1\}$, by applying AND operation on T the input a, b should be taken from T and the output column is represented as $a{\wedge}b$ and its resulting value will be 1 if it has both inputs values 1, else it will be 0. Truth table for AND operation should be given as:



a	b	$a{\wedge}b$
1	1	1
1	0	0
0	1	0
0	0	0

- **OR Operation**

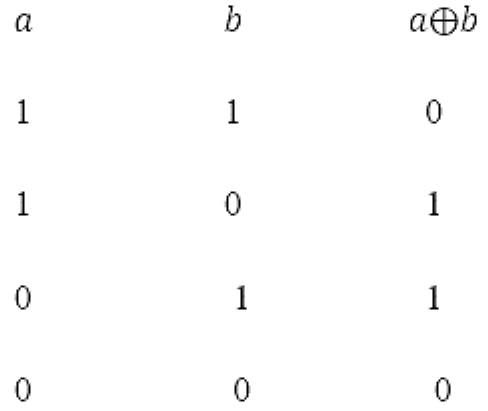
In this operation for both input $a, b \in T$, the output represented as $a{\vee}b$ has values equal to 0 for both input arguments having 0 value, otherwise it would be 1. The OR table is given below:



a	b	$a{\vee}b$
1	1	1
1	0	1
0	1	1
0	0	0

- **XOR Operation**

For both inputs a, b taken from T in XOR operation, the output values represented as $a{\oplus}b$ have zero value if both input values are identical, in other case they will be 1. XOR table should be given below:



a	b	$a\oplus b$
1	1	0
1	0	1
0	1	1
0	0	0

1.11 Criteria for Cryptographically Strong S-boxes

The S-boxes are declared to have strong resistance if they satisfy following criteria's:

1.11.1 Non-Linearity

To define the non-linearity, it is substantial to checked whether the Boolean functions are balanced or not. If the output of Boolean functions has equal number of zero's and one's corresponding to given input, then they are called balanced functions. Alternative technique to understand the definition of non-linearity is the minimum distance between Boolean functions and affine mappings. To define non-linearity in terms of Walsh Spectrum first calculate the Walsh spectrum as follows:

1.11.1.1 Walsh Spectrum

A $n \times n$ matrix which have entries (1, -1) is called Hadmard matrix. The sequence defines for Hadamard matrix is given as,

$$H_1 = [1], H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, H_n = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes H_{n-1}, n = 1,2,3, \dots$$

This transform will calculate the distance between Boolean functions and affine functions. In this transform the f_n's values of truth table will be taken and then multiply them with Hadmard matrix the result will be equal to Walsh-Spectrum (Here it will represent the distance between Boolean and affine functions) i.e.

$$f_n's \times Hadmard\ matrix = Walsh\ spectrum$$

After calculating the Walsh-Spectrum the formula for calculating nonlinearity of Boolean functions is given as [20]:

$$NL(f_n) = 2^{n-1} - \frac{1}{2} \max_{a \epsilon F_2^n} |W_f(a)|$$

The upper bound of nonlinearity of balanced Boolean functions is measured by the following (see [21]):

$$NL(f_n) \leq 2^{n-1} - 2^{\frac{n}{2}-1} - 2, \qquad for\ n\ (even)$$

The non-linearity in terms of Hamming distance is referred as the minimum distance between Boolean functions and all possible affine functions. To attain the nearest affine function of a Boolean function, the bits require modifications in configuration. The non-linearity technique enumerates the number of alternate bits to make the function closer to an affine function. In cryptographic literature, S-boxes represented in the case of the Galois field $GF(2^n)$, the upper bound of non-linearity is given as $2^{n-1} - 2^{n/2-1}$. For instance, if $n = 8$, then calculated optimal value of non-linearity for the Galois field $GF(2^8)$ dependent is 120.

1.11.2 Strict Avalanche Criterion

In 1986, Webster and Tavares originated strict avalanche criteria for strength analyzation of proposed S-boxes. A function satisfies the Sac property if by implementing single input bit, its every output bit alternates with probability of 0.5 [22].

1.11.3 Bit Independence Criterion

This criterion was firstly presented by Webster and Tavares [23]. In this criterion, the variables are pairwise related to collect the information about independence of such variables. In this technique for the analysis for independence variables the output vectors are used, and input bits are tackled separately. The bit independence criterion is highly recommended property in cryptographic structures because the increase independence among the bits creates more confusion to recognize the design of the structure.

1.11.4 Differential Approximation Probability

In encryption process, S-box is the non-linear component which context uniform differentiability in unique situations. The differential approximation probability is mathematically defined as:

$$\text{DP}\ (\Delta s \rightarrow \Delta t) = \frac{\{s \in S/\ \Omega(s) \oplus \Omega(s \oplus \Delta s) = \Delta t\}}{2^m}$$

Which means, an input differential must be uniquely mapped on output differential, which ensure uniform mapping probability for each i [24].

1.11.5 Linear Approximation Probability

The analyzation of maximum imbalance event value is termed as linear approximation probability (LP). In this technique, the two masks i.e.,A_q and A_r over parity of input and output bit are applied. In [25], the LP of S-box should be given as:

$$LP = \max_{A_q, A_r \neq 0} \frac{\{q \in Q \,/\, q.A_q = S(q).A_r\}}{2^n} - \frac{1}{2}$$

where A_q and A_r represents the input and output masks, respectively, the "Q" set contains all possible inputs and 2^n represents number of elements of Q.

1.12 Image Encryption

In many daily life applications such as video call conferencing, military branches, medical, communication of wireless networks images have significant role. When an image is transmitted two major issues need to be resolved, firstly check the transmitted image has assigned bandwidth and then must ensure that the images are transmitted through secure channel. So, for this purpose algorithms for encrypting images play a key role. Encryption algorithms encode the data which make it unreadable to viewer and it can be achieved by relocating or scrambling the pixels/pixel positions of image. To secure the digital images, now a day's researchers paid attention on creating such encrypted techniques that satisfies the following properties [26].

- The pixels of original and ciphered images need to be less correlated. The best encryption schemes have correlation values are near zero.
- The value of key space must be large because if the key space value is higher, so it is difficult for attacker to find the exact key.
- Sensitivity of key is also obligatory. In other terms, slight change of key will not decrypt the ciphered image.
- Entropy value of algorithm should be near optimal value i.e., 8. Since it refers to highest degree of randomness.
- The encrypted image should have high resistance against the attacks like chosen plain-text, chosen cipher-text.

1.13 A Review of Recent Research in Image Encryption

This section presents the literature survey of encryption schemes/algorithms for images.

1.13.1 Random numbers-based image encryption

Liu et al. [27] introduced an encryption scheme using random numbers. Novelty of his work lies on one-time pad key generation utilizing the hash value of random noise like digital voice recording device. Also, the already attained chaotic system enhanced by using this system. Because of varying input in every iteration this technique is resistant against the attacks.

1.13.2 Image encryption using Logistic double chaotic map

For key enhancement, this methodology is used, and this scheme is presented by W. Haifaa et al. [28] The keys of proposed scheme are generated by logistic chaotic map. Xor operation is used between them and in last again XOR operation is applied between resultant and plain-image values.

1.13.3 DNA conjunction with chaos-based image encryption

With the use of density information concepts, computing technique of DNA has high complexity. Image pixels are scrambled by permutations while the redundancy information of image is obtained by diffusion. In [29] K. Radihka et al. combine sequences of DNA with chaotic-maps. Image is divided in blocks then convert the decimal pixel values to binary matrices then encode them with DNA rules. After block scrambling, sub-blocks division is done. Addition DNA is added to blocks compile the blocks again.

1.13.4 A Color-image Encryption technique via randomly selective signal (Noise)

Eltous et al. [30] offered a color image encryption technique in which random noise is selected and then add noise signal to image after this step the image pixels are rearranged. The main purpose of this method is to increase the efficiency and achieves high level protection.

1.13.5 A color encryption-decryption technique based on blocks and reordering

Block-wise encryption and reordering based encryption technique was suggested by Khrisat et al. [31] two secret keys are used. Firstly, the image pixels are reshaped to single row matrix. Then number of blocks are selected the size of blocks is obtained by division with whole size of matrix then lastly the reordering of matrix is done to achieve encrypted image. For testation of scheme different experimental analysis are done.

1.13.6 Encryption Scheme using quantum chaos and DNA coding

Jian et al. [32] proposed an encryption scheme based on DNA coding, quantum chaos and Lorenz map. To enhance the security new encryption scheme dynamically use DNA four base pairs which select eight DNA encoding rules and eight different types of addition and XOR rules. The proposed scheme is tested via different statistical and experimental analysis.

1.13.7 Color Encryption Scheme based on sequences of quantum chaos

An innovative encryption scheme using quantum chaos is presented by Liu et al. [33]. In this scheme, pixels are permuted by Arnold scrambling technique. For diffusion, a folding technique is utilized which modify the diffused pixels. For high complexity and randomness, logistic and quantum chaotic maps are paired with closest neighbor paired lattices.

1.14 Random Number Generation (RNG)

An unpredictable sequence is known as sequence of random number. If the numbers have no correlation between them then that sequence is considered as truly random. In this way the prediction of succeeding number by using preceding is totally impossible. Distribution is the main part of any number sequence i.e., check how much the number sequences are uniformly distributed by generator. Also, the important feature of any sequence is its range [34].

1.14.1 Random Numbers Role in Cryptography

The random number sequences are used for different objectives, for example in generating keys for encryption, simulations and for modeling complexity. Random numbers generation is characterized in to two major approaches one is true random number generator (abbreviated as TRNG's) and other is pseudo-random number generator (PRNG's). RNG is a technique/algorithm in which bits of binary sequences are generated which are independent statistically. PRNG is a deterministic technique which produce nearly random sequences of binary bits. The PRNG have input value known as seed and the output of it is known as binary sequences. RNG are commonly used in applications and cryptographic techniques. In cryptographic schemes like secret key of DES, RSA technique prime number these are used for providing security. The output having length l of PRNG is not so random but it takes a small bit which is truly random and then expanded it to greater sequence. Like this, PRNG sequences could not be differentiated from truly random sequences. For the confirmation of output PRNG randomness some tests (statistical) and other analysis must be implemented. So, for the testation of random and pseudo random number generators many statistical analyses are implemented.

A comparison between among PRNG and TRNG is shown in table 1.1, which depicts TRNG is the most suitable choice for cryptographic designs.

Table 1.1: PRNG and TRNG comparison

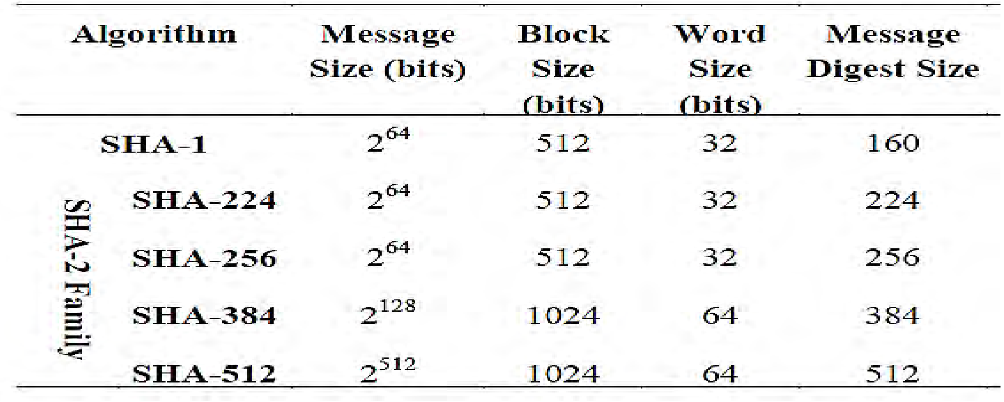
Traits	PRNG	TRNG
Effectiveness	Outstanding	Weak
Deterministic	Yes	NO
Periodicity	Yes	NO

1.14.2 Hash Functions Cryptography

In cryptography, Hash functions plays a very important role. Hash function cryptography is technique in which the hash value of message/image is generated for applications of cryptography that includes authentication, confidentiality, integrity, and many other protection services. In this mechanism, the input variable message/image lengths are accepted by hash functions then as an output a hash value of fixed length is produced which is referred as message digest or hash code. The dependency of hash values lies on input message/image bits, so any alteration in input data will alter and affect the value of hash code. The hash functions in cryptography are mainly divided in two major parts: one functions (hash) are secret-key dependent known as key hash functions and those which are not key dependent are known as non-keyed functions (hash) (see figure 1.5). Generally, the hash function idea is used as procedure of iteration which process complete message for hash-value production. Hash functions are also used for pseud-random number generations which are utilized in generating secret keys of algorithm. Hence, security to web, login password, online payments through internet depends mainly on hash values of functions. Internet do not work in the absence of hash values/functions. In 1993, Secure hash functions (SHA) was designed by National institute of standard and technology (NIST) having high hash values that are used as a standard hash function [35].

The first member of SHA family i.e., SHA-0 was created by NIST and in 1993, it became the original technique published by Federal Information Processing Standard abbreviated as FIPS [36]. After its publication, National Security Agency (abbreviate as NSA) withdrawn with it. So FIPS designed another algorithm like SHA-1 to overcome the flaw lies in original technique in 1995 [37]. In comparison with other techniques (Message-digest 4, Message-digest 5 etc.) SHA-1 algorithm has strong resistance against attacks, so it is most preferable algorithm by cryptographers. SHA-1 process on the input (message) having bit length lower than $2^{64}$for the generation of hash value of length 160 bit so it is considered as hash function of one-way. It is useful in providing integrity to message because of its sensitivity for altering input message/image. Due to this feature, it is very fruitful for authentication in message codes, digital techniques like signature, and random generation of bits [38]. Based on hash values of long length few other SHA families were published having a slight change in their designs and are known as: SHA-224, SHA-256, SHA-384 SHA-512 and collectively they are known as SHA-2 family. See table 1.2,

Table 1.2: SHA Families



	Algorithm	Message Size (bits)	Block Size (bits)	Word Size (bits)	Message Digest Size
	SHA-1	2^{64}	512	32	160
SHA-2 Family	SHA-224	2^{64}	512	32	224
	SHA-256	2^{64}	512	32	256
	SHA-384	2^{128}	1024	64	384
	SHA-512	2^{512}	1024	64	512

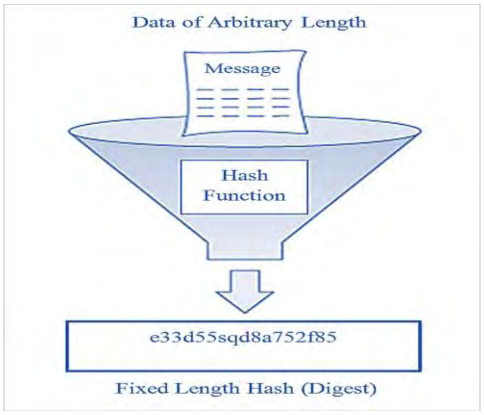


Figure 1.5: Model for iterated general Hash function

1.15 Chaos Theory

The chaos is taken from Greek letter ‘Xaos’ that means unpredictable or disorderly state. The systems based on chaos are simple, dynamical, deterministic, and non-linear which demonstrates their unpredictability having random appearance. Also, chaotic systems have a high initial value sensitivity which means that if a parametric input value is changed the output results are totally different.

In 1996, Alligood et al. [39], introduced a dynamical system that includes all states which are possible and rules that regulate the succeeding state from preceding ones uniquely, although to determine evolution of system a mathematical equation are always used. In differential dynamic equations bifurcation change solution if parametric values are changed.

Poincare [40] has published article in 1890, in this article he presented the dynamic equations and problems of three body, this simplifies viewing complex continuous trajectory of differential equations.

After this, [41] Hadamard (1898) monitored initial conditions sensitivity and unpredictable behavior of special systems, call this geodesic tide/flow. Later, Poincare (1908) pointed out that the sensitivity of chaos depends on initial values which gives unpredictable consequences [40]. In 1963, Edward Lorenz analyzed theory of chaos and depicted simple prediction of weather based mathematical structure. For detection of non-linear chaotic dynamical system Lorenz numerical paradigm was first model. Lorenz's conclusions were so amazing in which equations have so complexity and random behavior that depends on initial values [42].

So, Yorke and Li (1975) were first ones who presents 'Chaos' in literature of math's, where the results of system are randomly appeared [43].

Recently, Chaos theory is an active subject in area of research due to its traits that includes initial values sensitivity, complexity, and complete deterministic behavior. The behavior of chaos may be observed in various systems for example in lasers, fluid dynamics, electronic structures, climate, economics, and weather. Generally, chaotic systems characterize large infinitely fields based on real values.

1.15.1 Cryptography and Chaos

From last few decades, focus of researchers is the theory of chaos in many fields like lasers, fluid dynamics, electronic structures, climate, economics, and cryptography. Because of chaotic theory traits (like unpredictable behavior, randomness, initial conditions sensitivity). Cryptographers used dynamical chaotic-systems for the development of cryptographic novel primitives using maps based on chaos for instant Henon, logistic, and tent maps. Some traits of chaos and cryptography are similar, and few are different. Chaotic map parameters are significant, usually when they depend on real numbers which could be used in many techniques of cryptography as keys for encryption and decryption process. Chaos is very sensitive to initial values and shows unpredictable behavior so in cryptographic techniques of encryption it creates diffusion. Chaotic maps/systems iteration will result in initial state spreading throughout the complete stage, and in cryptographic techniques it is achieved by round based designed algorithms. The major difference in chaos and cryptography is that the transformation of encryption is defined over finite-sets, while mostly chaotic systems are defined on real value/numbers. Very few chaotic systems are defined over complex number that is squaring complex maps, which are not used in chaos-based cryptography yet. Later 1990, many digital chaos-based algorithms are presented to provide security by utilizing chaotic maps [44].

1.16 Image Texture Evaluation

The most substantial attributes of a material which defines its surface appearance is known as texture, together with color. To do this analysis various techniques are presented e.g., Wavelet and Fourier approach. But recent analysis is appealing as it is related to optical system of human that identifies the texture, that is the first approach by Haralik [45] to design texture analysis, which is extensively used in segmentation of images. Following features are used to describe the image texture analysis: energy, contrast, homogeneity, correlation, and Entropy.

1.16.1 Contrast

The difference amount in an image allow observer to detect image entities. During the process of encryptions, if the contrast value increases the unpredictability in encrypted images is also increased. The robust scheme has highest contrast value of ciphered images. Illustration of this analysis is as follows:

$$C = \sum_{u}\sum_{v}(u-v)^2 p(u,v),$$

Here u and v represents the pixels in an image, and number of gray-level co-occurrences matrices (GLCM) is represented by $p(u,v)$. For constant image the contrast value is 0.

1.16.2 Entropy

To check the randomness entropy is an important feature. To calculate the entropy of an image following formula is used:

$$\mathcal{H}(m) = -\sum_{u=0}^{2^n-1} \mathrm{P}(m_u)\log_2[\mathrm{P}(m_u)],$$

where grey-level u occurrence probability is denoted by $\mathrm{P}(m_u), u = \{0,1,2, \ldots\ldots 2^n\}$ and 2^n is greyscale image level number. If the occurrence probability of every m_u is same in image, then probability $\mathrm{P}(m_u) = \frac{1}{2^n}$. So, image shows complete random behavior by $\mathcal{H}(m) = n$.

1.16.3 Energy

In this analysis execution, the GLCM is used. Energy is basically the sum of squared numbers in GLCM. Proposed analysis mathematical demonstration is:

$$\mathrm{E} = \sum_{u} \sum_{v} p^2(u, v)$$

Constant images have energy value equal to 1.

1.16.4 Homogeneity

The image pixels are scattered positively. For measurement of scattered pixels closeness in GLCM-to-GLCM diagonal homogeneity analysis is implemented. Gray pixel levels ordering statistics is indicated by GLCM in tabular form. The homogeneity is calculated by:

$$\mathrm{H} = \sum_{u} \sum_{v} \frac{p(u, v)}{1 + |u - v|}$$

1.16.5 Correlation

Image adjacent pixels relationship is provided by correlation. It is partitioned in three distinct categories that include horizontal, diagonal, and vertical formats. The whole image texture kept under consideration while performing this analysis. The mathematical formulation of this analysis is the equation:

$$K^* = \sum_{u,v} \frac{(u - \mu u)(v - \mu v)p(u, v)}{\sigma_u \sigma_v}$$

1.17 Image Metric Evaluation

For the evaluation of encrypted/ciphered images performance, to evaluate the performance of the encrypted images, there are several quality measuring techniques like Mean square error (MSE), and Peak signal to noise ratio (PSNR) [46].

1.17.1 MSE

MSE is a squared average difference among distorted and original image. The mathematical formulation of MSE is:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} (P(i, j) - C(i, j))^2,$$

where $m \times n$ is image size. $P(i,j)$ and $C(i,j)$ parameters refer the location of pixel at ith and jth row and column of original and ciphered images. For encryption scheme having good security, MSE value must be higher. [46]

1.17.2 PSNR

The representation of signal is affected by any noise. PSNR is equal to ratio among noise and signal power.

$$PSNR = 10log_2\left(\frac{\mathrm{I}_{\max}^2}{\sqrt{MSE}}\right),$$

$\mathrm{I}_{\max}$ represents image pixel maximum value [46].

1.18 Differential Attack Analysis

To extract image significant information mostly attackers used a tactic in which they change the original plain image slightly and then proposed scheme is applied to encrypt the plain and already encrypted image (which they want to crack). So, two encrypted images are obtained. In this manner, the attackers crack cryptosystem by the difference rates of both ciphered images this overall process is known as Differential analysis. For encryption algorithm robustness, the proposed method should be highly sensitive to plain text and secret key, so any slight alteration in secret key or plain text would lead to complete alteration in ciphered text. The strength against the differential attacks of an encrypted/ ciphered image is estimated by two way; one is the number of pixels change rate (NPCR) and other one is unified average changing (UACI). The NPCR [47] considered two ciphered images by changing only one pixel, if first image is represented by $\mathcal{C}_1(u,v)$, and second by $\mathcal{C}_2(u,v)$, then NPCR is evaluated as.

$$NPCR(\mathcal{C}_1,\mathcal{C}_2) = \frac{\sum_{u,v}\mathcal{D}(u,v)}{\mathcal{T}} \times 100\%,$$

where $\mathcal{T}$ is the total number of pixels and $\mathcal{D}(u,v)$ is defined as

$$\mathcal{D}(u,v) = \begin{cases} 0, & if\ \mathcal{C}_1(u,v) = \mathcal{C}_2(u,v) \\ 1, & if\ \mathcal{C}_1(u,v) \neq \mathcal{C}_2(u,v) \end{cases}.$$

The UACI (Unified average changed intensity) [47] is for testing the pixels change number and it measures intensity average change among cipher images. Mathematically this analysis is represented by the formula,

$$UACI(\mathcal{C}_1, \mathcal{C}_2) = \frac{1}{MXN} \sum_{u=0}^{M-1} \sum_{v=0}^{N} \frac{|\mathcal{D}(u,v) - P(u,v)|}{F \times T} \times 100\%,$$

where F represents largest validated pixel value having compatibility to cipher image format and $\mathcal{D}(u,v)$ is defined as:

$$\mathcal{D}(u,v) = \begin{cases} 0, & if\ \mathcal{C}_1(u,v) = \mathcal{C}_2(u,v) \\ 1, & if\ \mathcal{C}_1(u,v) \neq \mathcal{C}_2(u,v) \end{cases}.$$

1.19 Classical Types of Attacks

To cryptanalyze a cryptosystem, generally it is assumed that a cryptanalyst exactly knows the working and design of understudy cryptosystem, except secret key everything is known to him. To break any cryptosystem four well-known attacks are applied by attackers termed as: the known-plain text attack, chosen plain-text attack, ciphertext only attack, chosen cipher-text attack [48].

(1) Cipher-text only attack: Opponent has accessed to the ciphertext string.

(2) The Known-plaintext attack: Opponent has accessed to both plain and cipher text strings.

(3) Chosen plaintext: In this attack opponent can select a random string of plaintext and gets the corresponding string of ciphertext.

(4) Chosen ciphertext: In this attack opponent can select a random string of ciphertext and gets the corresponding string of plaintext.

Chapter 2

Design of S-boxes via Hybrid PRNG's: An RGB Image Encryption Application

In this chapter, to analyze the security of an encryption using PRNG'S S-boxes, an efficient color image encryption technique based upon hybrid pseudo-random binary numbers and S-boxes is proposed. The aim of the presented work is to design S-boxes over binary pseudo random numbers generated by linear feedback shift registers (LFSR) in combination with modified quadratic chaotic map. Firstly, cryptographically robust S-boxes are constructed by using binary pseudo random number sequences, and then the cryptographic properties of presented S-boxes are tested. Results proved that suggested S-boxes shows good results. Secondly, an RGB image encryption algorithm utilizing sequence generated by modified quadratic chaotic map and S-boxes is offered. The new color image encryption techniques comprised on two steps (one is permutation and other is substitution), also the key association with content of image is addressed. This strategy can bring "one-time pad" effect and make algorithm resistant to chosen-plain-text attack (CPA). The proposed scheme has been institute to be more valuable than most of the existing schemes. S-boxes are analyzed by nonlinearity test, bit independent criterion (BIC), strict avalanche criterion (SAC), differential and linear approximation probability tests. A comparison with different S-boxes presented in literature is also done. The comparison shows encouraging results about the quality of the proposed box. From security and experimental outcomes effectiveness of presented color image encryption technique is verified. Proposed scheme has evident efficiency benefits, which implies that proposed colored encryption of images scheme has a better potential application in encryption schemes of real-time.

2.1 Background

In modern times, the public wishes to possess information secrets and hide from another populace. In the past, people used various techniques to keep information secrets from adversaries. The rulers, armed forces, and bureaucrats for their sensitive material, which helped them in transmission of their information to their militaries in a safe and secure way, used vital coding methods. With rapid development of civilization, it is very important to develop strategies for preservation of information. Currently, data security has a prime significance. Therefore, to resolve security issues, cryptography plays a substantial role for hiding data into an unreadable format [49].

Cryptosystems are generally classified into two main classes: Block and Stream cipher. In block ciphers, the data is transformed in form of blocks (i.e., the input bits of m length are transformed to output bits of length n by use of block cipher). While in Stream cipher, it operates on single bit at a time mean a single input bit is transformed to single output bit [50].

Numerous encryption techniques evolved with the passage of time for securing information of high intelligence value. Wireless communication, being prone to more theft, requires data security using advanced encryption techniques [51]. Block cipher-based cryptosystems are heavily dependent on S-boxes, designers of cryptosystems have their focus on design of cryptographically strong S-boxes.

For the bulk of data Advance Encryption Standard (AES) and Data Encryption techniques were used for encryption and decryption. Over the passage of time, AES superseded the Data Encryption Standards. In AES, the nonlinear transformation of S-box (Substitution box) is an essential constituent. The strength of an S-box plays a vital role for the algorithm's security. Thus, researchers spend a much time on improving the strength of an S-box [52].

The significant portion of the time spent on design and analysis is devoted to the S-box construction, as it is the only nonlinear part of the algorithm. Hence, every weakness in the S-box can be intercepted easily in a cryptosystem [53]. For this purpose, many techniques for construction of S-boxes are proposed by many researchers. Since, non-linear systems have fact of randomness, so in cryptography chaos plays a great role. Because chaos helps in generation many pseudo random sequences which are used in nonlinear components of encryption construction. Many chaos-based cryptosystems have reported in recent years because of existence of chaotic and cryptosystems properties relationship [see 54-63].

Since some traditional techniques for encryption (like AES, DES, single one-dimensional chaos etc.) are not suitable for encryption of images as explained. So, the need of hour is to formulate strategies that secure the information of images. In view of this, many block-ciphers based encryption techniques utilizing random numbers generated by chaos are presented which provides a large security [64-67].

For contribution in study of cryptosystem design this chapter of dissertation presented a technique for designing S-boxes based on pseudo binary bits stream of numbers and its application in encryption schemes. The binary bit streams of random numbers are generated via hybrid modified chaos and feedback shift registers. The S-boxes constructed by using this scheme shows excellent properties, which indicates it can be valuable in cryptosystems. Developing a novel image encryption algorithm, first we use random numbers to scramble the pixels of image then the S-boxes are substituted to create confusion. To check the robustness of presented color image encryption, scheme the comparison of various image quality measures with RGB image encryption based on chaos schemes has been given.

2.1.1 Linear Feedback Shift Registers (LFSR)

In digital circuits, shift registers are a kind of logic circuits, compiled in a linear mode whose inputs are connected to output in such a manner that by trigging a circuit the data is moved along the line. LFSR is a shift register whose input bits are the linear function of its more than two preceding states. An n-stage LFSR has n-length numbered as $\{0,1,2, \dots\dots, n-1\}$, each have ability to store single bit and clock is used to control the shuffling of data. Shift register is initialized by vectors having entries $w_0, w_1, w_2, \dots\dots, w_{n-1}$. The operations used in LFSR are as follows:

1. w_j (The zero-stage entry) constitutes the output part.
2. The entry of j-stage is shifted to $j-1$ stage, for $1 \leq j \leq n-1$.
3. The new entry of $n-1$ stage is obtained by subset of n-stage entry using Xor.

The starting input bit value of LFSR is known as seed. Well-defined seed and feedback function of LFSR generates a random bit sequence having a large period value. If the input bit value in LFSR consists of only 0's then the registers would stop working and output is only zero. Each initial state (other than zero) generates a periodic sequence of states of period $(2^n - 1)$ [68-69].

2.2 Improved Quadratic Chaotic Map

Improved Quadratic chaotic map is defined as:

$$X_{i+1=}(R + (1 - 2X_i)^2) \; mod \; 1.$$

This map has state variable X and parameter R. The parametric value R shows chaotic behavior in these intervals $[0, 0.14], [1.56, 2.14], [2.56, 3.14], \dots infinity$ (see 70). Simple modification of this chaotic map is used in proposed work for generating chaotic binary numbers as follows:

$$\left.\begin{array}{l} X_{i+1=}(R+(1-2X_i)^2)\ mod\ 1. \\ \\ Y_{i+1=}(P+(1-2Y_i)^2)\ mod\ 1. \end{array}\right] \quad \ldots\ldots (1)$$

where X, Y are state variables $X(0) \neq Y(0)$ and R, P are parameters and used as secret keys. Bifurcation diagram of improved quadratic chaotic map is shown in Fig 2.1.

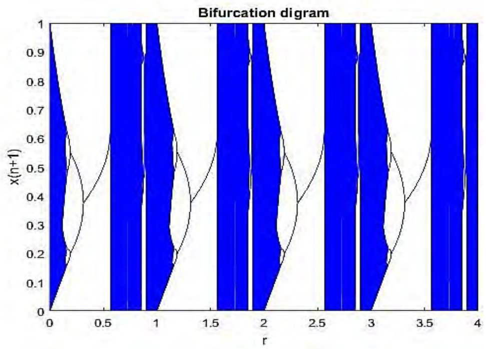


Figure 2.1: Bifurcation diagram

2.2.1 Binary Sequence Generation using Modified Quadratic Map

This section presents a technique of generating pseudorandom binary sequences using threshold simple function which is combined with real numbers of modified quadratic chaotic maps. The following steps are used for this purpose:

- First determine the initial values and parameters $\{X(0), Y(0), R(0), P(0)\}$ from equation 1, given in section 2.2.
- The modified quadratic equations are iterated K and L times respectively, where K and L are different constant values.
- By iterating equation 1, two sequences (decimal) $X(i), Y(i)$ are generated using following formulas:

  $$X(i) = abs(mod(floor(X \times 100000000000000)), 2));$$
  $$Y(i) = abs(mod(floor(Y \times 100000000000000)), 2));$$

  where the $floor$converts the value of X to closest integer equal of less than X, $mod\ (X, Y)$ is used to return reminder value after the division, and $abs(X)$ is used to give absolute X value.
- Now apply threshold function (W) as:

  $$W(i) = \begin{cases} 1, & if\ X(i) > Y(i) \\ 0, & if\ X(i) \leq Y(i) \end{cases}$$

  After that, a bit stream of pseudorandom numbers is obtained.

- Repeat the process until the desired bit stream of pseudorandom numbers W' is obtained. The whole process is explained in figure 2.2,

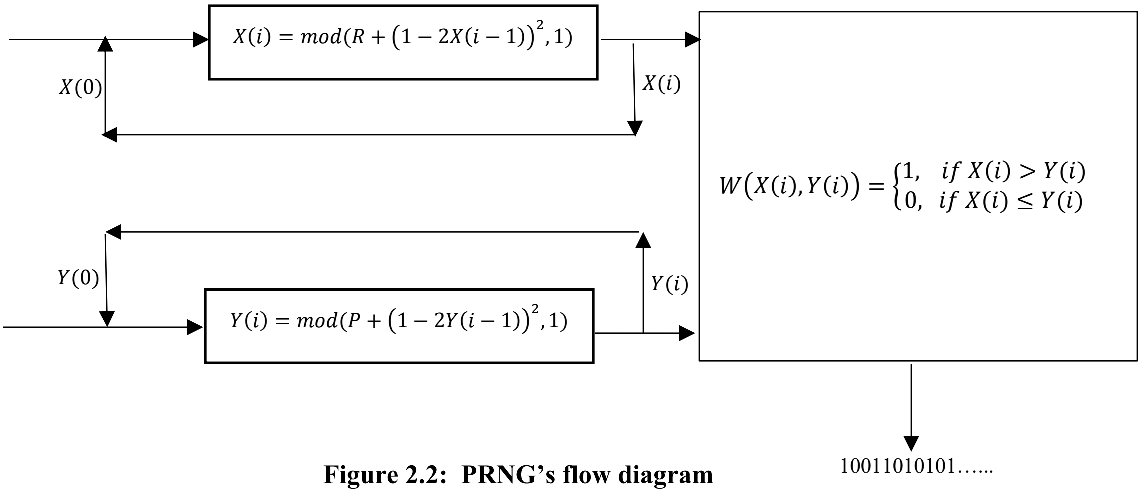

$X(i) = mod(R + (1 - 2X(i-1))^2, 1)$
$X(0)$
$X(i)$
$W(X(i), Y(i)) = \begin{cases} 1, & if\ X(i) > Y(i) \\ 0, & if\ X(i) \le Y(i) \end{cases}$
$Y(0)$
$Y(i)$
$Y(i) = mod(P + (1 - 2Y(i-1))^2, 1)$
10011010101……

Figure 2.2: PRNG's flow diagram

2.2.2 Hybrid Pseudorandom Binary Sequences Generation

The design of HPRNG's is based on LFSR of length 32 bits and modified quadratic chaotic maps, since many PRNG based LFSR are not resistant against attacks and provides the information about the secret key. This flaw is overcomed by using XOR operation in which random bits obtained by modified quadratic map PRNG's binary stream (Section 2.2.1) are Xored with LFSR feedback in every clock cycle to generate the binary stream of random numbers S. The LFSR tap positions are decided by the primitive polynomial $q^{32} + q^{22} + q^2 + q^1 + 1$. The total keys required for hybrid PRNG's are $\{X(0), Y(0), R(0), P(0), f\}$, where f denote the input vector in LFSR. Key space for LFSR of 32 bit is $2^{32} - 1 = 429{,}4967{,}295$. Flow diagram of figure 2.3, demonstartes the whole process of HPRNG's.

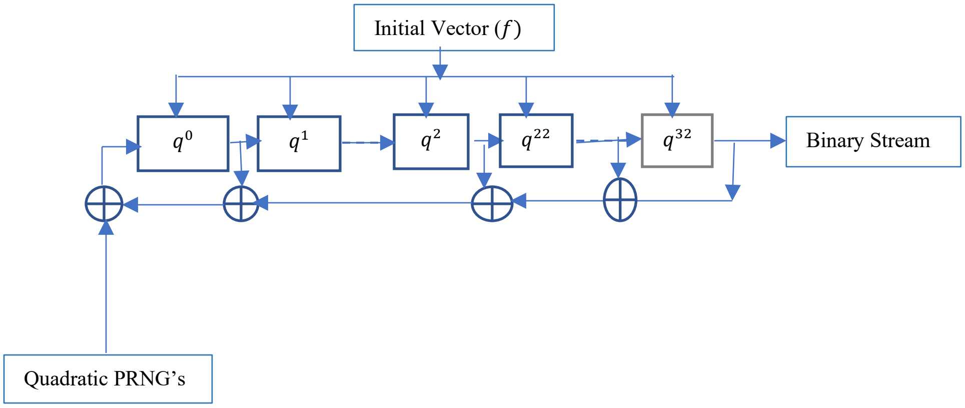


Figure 2.3: HPRNG's flow diagram

2.3 S-boxes Construction using HPRNG's

Simple steps are used for the construction of cryptographically secure S-boxes as follows:

The bit stream $S = \{S_0, S_1, S_2, S_3, \dots \dots\}$ generated in section 2.2.2 is then used in the construction of S-boxes as follows:

Step1: Each block sequence consisting of N-bits are generated as:

$$B_0 = \{S_0, S_1, S_2, \dots \dots S_{N-1}\},$$
$$B_1 = \{S_N, S_{N+1}, S_{N+2}, \dots \dots S_{2N-1}\},$$
$$B_2 = \{S_{2N}, S_{2N+1}, S_{2N+2}, \dots \dots S_{3N-1}\}, \dots$$
$$B_k = \{S_{kN}, S_{KN+1}, S_{KN+2}, \dots \dots S_{(K+1)N-1}\}.$$

Step 2: Now each N-bit block i.e., $B_0, B_1, B_2, \dots .., B_k$ is converted to integer numbers as $C_0, C_1, C_2, \dots .., C_k$.

Step 3: To get distinct 2^n values the repeated numbers are removed.

Step 4: Create S-boxes.

Step 5: After one S-box, consider other blocks of N-bits then repeat the whole process to generate other two S-boxes. In proposed work, N= 8 to generate 8x8 bits-based S-Boxes.

The S-boxes are given in Table 2.1-2.3.

Table 2.1: S-box 1

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

Table 2.2: S-box 2

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

Table 2.3: S-box 3

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

2.4 S-boxes Algebraic Analysis

In this section, proposed S-box evaluation is presented**.** The assessment of S-boxes ensures the efficiency and ability to create misperception in any cipher. For S-boxes algebraic properties testation the analysis used are NL(Non-Linearity), BIC (Bit-independence criterion), SAC (Strict-avalanche criterion), LP (Linear-approximation probability), DP (Differential-approximation probability). From the analysis, it is observed that proposed S-boxes achieved almost all conditions close to the ideal result. Also, the comparison of proposed S-boxes with S-boxes generated by different schemes is presented**.**

2.4.1 Nonlinearity

Boolean and all set of affine functions distance is measured by non-linearity. Proposed S-boxes NL calculations are given is Table 2.4. Presented analysis reveals that produced S-boxes could replace the algebraic constructed S-boxes because their construction is appealing and based on random numbers generated by hybrid chaos and feedback registers which creates massive randomness.

2.4.2 Strict Avalanche Criteria (SAC)

SAC examines the S-boxes randomness when any alteration in inputs is done. The results are shown in Table 2.4. From results, it is clearly seen that average SAC value of S-boxes are near ideal 0.5 values, which verifies S-boxes SAC property fulfilment.

2.4.3 Bit Independent Criterion (BIC)

BIC checks the dependency and statistical patterns among vectors and guarantees that no dependency and statistical patterns among vectors outputs is detected. Results are displayed in Table 2.4, which suggested that S-boxes satisfies BIC.

2.4.4 Linear Approximation Probability (LP)

An event unbalanced value is known as LP. From the analysis of LP for synthesized S-boxes it is observed that the S-boxes have average LP value 0.0343 which ensures its resistance against attacks.

2.4.5 Differential Approximation Probability (DP)

S-box differential homogeneity is quantified by DP. Less DP value provides more resistant to attacks (differential attacks). Average DP value of all three S-boxes is 0.0364.

All three suggested S-boxes catalogs are given in Table 2.4, and their comparison with other S-boxes is shown in Table 2.5.

Table 2.4: **Performance Indexes of S-box 1, S-box 2, S-box 3**

Analyses	Maximum	Minimum	Average	Square − Deviation	Approximated differential probability (DP)	Approximated Linear Probability(LP)
NL						
Sbox 1	106	100	103			
Sbox 2	108	103	105.5			
Sbox 3	110	98	104			
SAC						
Sbox 1	0.565	0.422	0.494	0.013		
Sbox 2	0.625	0.421	0.502	0.015		
Sbox 3	0.421	0.422	0.502	0.021		
BIC						
Sbox 1		95	105.2	0.903		
Sbox 2		110	103.2	3.216		
Sbox 3		94	104.2	2.252		
BIC − SAC						
Sbox 1		0.474	0.502	0.0132		
Sbox 2		0.480	0.503	0.0142		
Sbox 3		0.472	0.500	0.0139		
DP						
Sbox 1					0.0324	
Sbox 2					0.0312	
Sbox 3					0.0457	
LP						
Sbox 1	146					0.070
Sbox 2	150					0.013
Sbox 3	158					0.012

2.4.6 S-boxes Comparison

For the testation of cryptographic proposed S-boxes performance, extensively used performance criterion for S-boxes are employed. Additionally, a comparison between cryptographic proposed S-boxes performance with recently suggested S-boxes is done and results are shown in Table 2.4, in criteria of evaluated performance, BIC -SAC and SAC ideal value is 0.5. Greater value of Non-linearity indicates S-boxes better performance and its resistance against attacks (cryptanalysis). For better resistance against differential and linear cryptanalysis LP, DP values for S-boxes must be smaller. From results of Table 2.5, suggested S-boxes have less DP, LP values than the majority proposed schemes, which means that S-boxes of presented scheme has strong robustness against cryptanalysis attacks (Linear and Differential). S-boxes nonlinearity is also higher than many others. Table 2.5 also suggests that the SAC and BIC-SAC values of proposed S-boxes are close to ideal SAC value.

Table 2.5: Proposed S-boxes Comparison

$S-$ boxes	Nonlinearity	SAC	BIC	DP	LP
AES	112	0.5058	112	0.0156	0.062
APA	112	0.4987	112	0.0156	0.062
Gray	112	0.5058	112	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
Residue Prime	99.5	0.5012	101.7	0.2810	0.132
[71]	103.3	0.500	104.0	0.047	0.133
[72]	105.5	0.499	106.0	0.125	0.133
[73]	106.5	0.495	103.8	0.039	0.141
[74]	104.5	0.498	104.6	0.047	0.125
[75]	105.5	0.5000	103.8	0.047	0.1250
proposed:					
$S-$ box 1	103	0.494	105.2	0.0324	0.016
$S-$ box 2	105.5	0.502	103.2	0.0312	0.013
$S-$ box 3	104	0.502	104.2	0.0320	0.012

2.5 Image Encryption Scheme

For the elimination of insecurities in S-boxes based image encryption schemes, a novel encryption technique based on S-box and binary stream of pseudo random numbers is proposed. The innovations of proposed encryption algorithms are as follows:

Firstly, a new technique is used to generate S-box and binary pseudo random number sequences, which are then used in substitution and permutation process of presented scheme. The flow diagram of proposed scheme is shown in figure 2.4:

2.5.1 Permutation Process

The process of permutation involves following steps:

1. First, take an original color image Q of length $m \times n \times 3$ and associate this image with some random security keys taken as $K = (K_1, K_2, K_3, \dots\dots, K_9)$ whose values lies between 0 and 1, which are then used as initial values and parameters of modified quadratic chaotic map (equation 1) given in section 2.2.
2. Apply sum between the pixel values of matrices Q_R, Q_G, Q_B as:

$$sum_R = \sum_{j=0}^{n+1} \sum_{i=0}^{m+1} Q_R(i,j)\,;$$

$$sum_G = \sum_{j=0}^{n+1} \sum_{i=0}^{m+1} Q_G(i,j)\,;$$

$$sum_B = \sum_{j=0}^{n+1} \sum_{i=0}^{m+1} Q_B(i,j);$$

where Q_R, Q_G, Q_B are the matrices of red, green, blue channels of original color image Q.

3. Now, the initial and parametric values of modified quadratic chaotic map are generated by using the following formula:

$$X(0) = mod((K_1 \times \log(sum_R) + K_2 \times \log(sum_G) + K_3 \times \log(sum_B)),256);$$
$$R(0) = mod((X(0) + 1) \times (K_4 \times K_5 \times K_6)),1);$$
$$Y(0) = mod((K_7 \times \log(sum_R) + K_8 \times \log(sum_G) + K_9 \times \log(sum_B)),256);$$
$$P(0) = mod((Y(0) + 1) \times (K_4 \times K_5 \times K_6)),1);$$

$mod(u, 1)$ or $mod(u, 256)$ denotes the decimal fraction value of u.

4. Iterate the modified quadratic map given in equation 1, by using initial values obtained in Step 3. Hence, new-sequences $X'(i), Y'(i)$ are generated.
5. Now the pixels of image are permuted row and column wise through sequences $X'(i), Y'(i)$. Then permuted image $I' = \{I'(1), I'(2), I'(3), \ldots\ldots I'(H)\}$, $H = M \times N$ is obtained.

2.5.2 Substitution Process

To get final encrypted image E, substitution is achieved as:

First, the binary pseudorandom number sequence W' obtained in section 2.2.1 is converted to key sequence having integer 8-bit values by following formula:

$$W'(i) = mod(floor(W'(i) \times 10000000000000), 2^8);$$

For substitution process, key $W', \boldsymbol{S_{box1}}$ and permuted image I' are used. First convert the permuted image into three layers I'_R, I'_G, I'_B. Then apply the procedure as:

Substitute every pixel of permuted image I'_R with $\boldsymbol{S_{box1}}$ and the sequence W'. The substitution is done using following formula:

For first pixel,

$$\begin{cases} j = mod[(1 + I'_R(2)), H] + 1, \\ E(1) = sub\_byte[\boldsymbol{S_{box1}}, v_0 \oplus I'_R(1)] \oplus w^{'}(j), \end{cases}$$

where v_0 is any number in $\{1,2 \ldots 255\}$.

For i^{th} pixel,

$$\begin{cases} j = mod\left[\left(i + I'_R(i+1)\right), H\right] + 1, \\ E(i) = sub\_byte[\boldsymbol{S_{box1}}, E(i-1) \oplus I'_R(i)] \oplus w^{'}(j), \\ i = (1,2,3, \dots \dots . . H-1) \end{cases}$$

Last H^{th} pixel,

$$\begin{cases} j = mod[(H + v_0 + vl), H] + 1, \\ E(H) = sub\_byte[\boldsymbol{S_{box1}}, E(H-1) \oplus I'_R(H)] \oplus w^{'}(j), \end{cases}$$

where, vl belongs to $\{1,2,3, \dots 255\}, sub_{byte}[\boldsymbol{S_{box1}}, X]$ used for byte substitution for X using S-box1. Hence, we get final encrypted image for red layer $E_R(i,j)$. Repeat the process by using $\boldsymbol{S_{box2}}, \boldsymbol{S_{box3}}$ for I'_G, I'_B. Decryption is the reverse of encryption scheme. The proposed scheme original and encrypted images are shown in figure 2.5. From figure 2.5, it can be clearly seen that the encrypted image is totally different from original image.

Original and encrypted combine and each R, G, B layer representation of Lena image is shown in Figure 2.5.

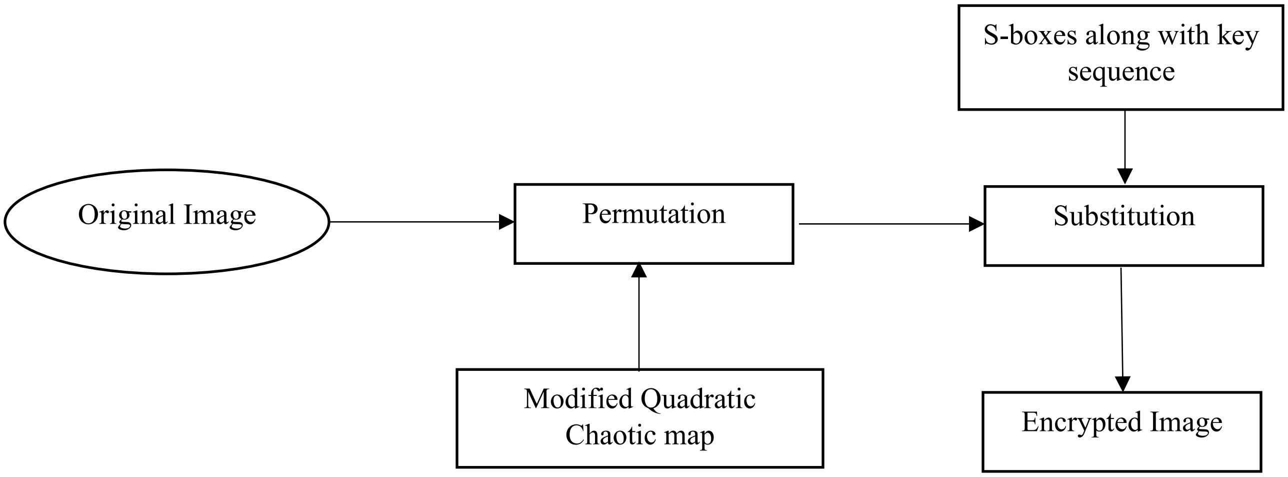

S-boxes along with key sequence
Original Image
Permutation
Substitution
Modified Quadratic Chaotic map
Encrypted Image

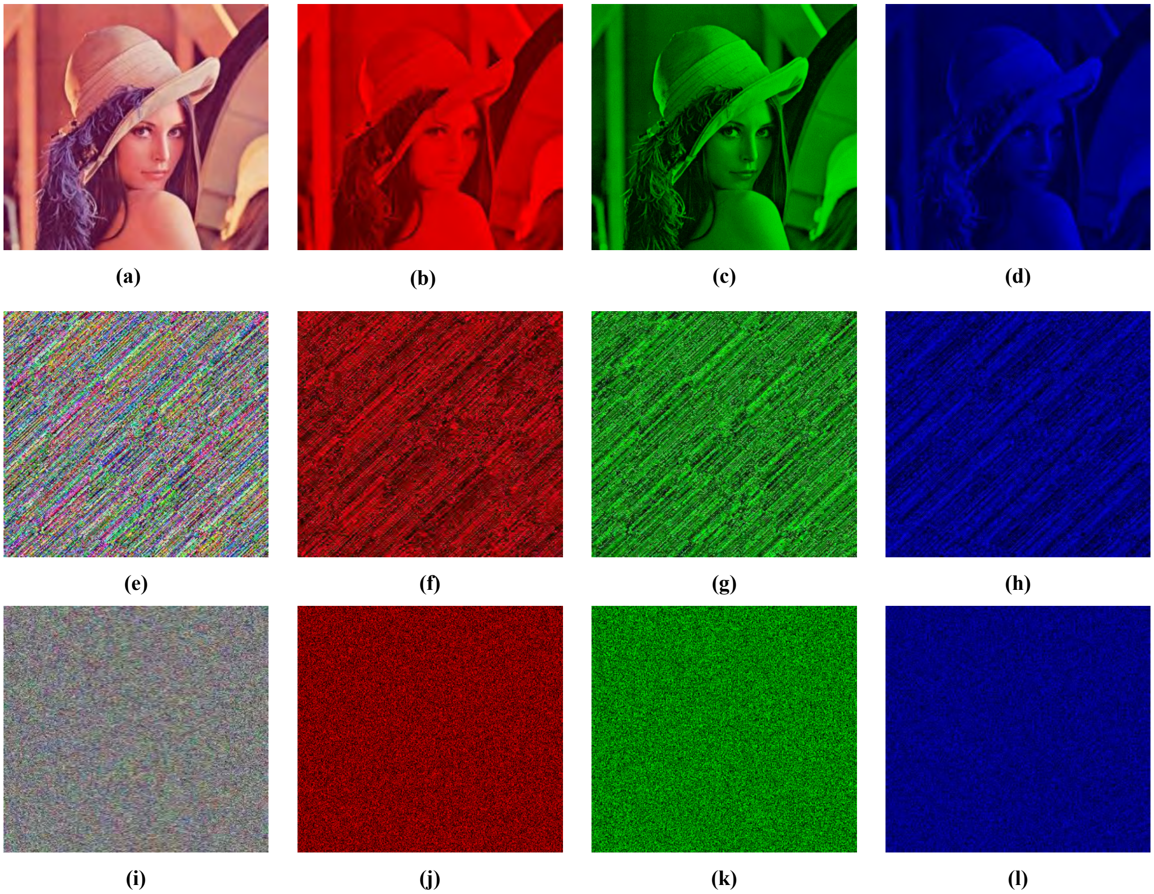
Figure 2.4: Flow chart of Encryption Scheme

.

2.5.3 Pseudocode of Encryption Scheme

```
Input: Original plain Image (Q) of size $m \times n \times 3$, security keys $K = (K_1, K_2, K_3, \ldots\ldots, K_9)$,
    with $K_1 = 0.253496532144, K_2 = 0.467321337632, K_3 = 0.100643892652,$
    $K_4 = 0.564329647734, K_5 = 0.472931065490, K_6 = 0.689546143287,$
    $K_7 = 0.6257742381092, K_8 = 0.734518093476, K_9 = 0.779834561276.$
Output: Encrypted Image (E) of size $m \times n \times 3$.
  1. $Q = [Q_R, Q_G, Q_B]$,  $\%Q_R, Q_G, Q_B = Red, Green, Blue\ channels\ matrices\ of\ image\ Q.$
  2. $sum_L = \sum_{j=0}^{n+1} \sum_{i=0}^{m+1} Q_L(i,j)$ ; %Apply sum between pixel value of matrix $Q_L, L = R, G, B.$
  3. Take modified quadratic chaotic map given in section 2.2.
  4. %Initial values and parametric values generation in step [5,6,7,8];
  5. $X(0) = mod((K_1 \times \log(sum_R) + K_2 \times \log(sum_G) + K_3 \times \log(sum_B)),256)$;
     % Initial variable $X$ calculation.
  6. $R(0) = mod((X(0) + 1) \times (K_4 \times K_5 \times K_6)),1)$; % Initial parameter value $R$.
  7. $Y(0) = mod((K_7 \times \log(sum_R) + K_8 \times \log(sum_G) + K_9 \times \log(sum_B)),256)$;
     % Initial variable $Y$ calculation.
  8. $P(0) = mod((Y(0) + 1) \times (K_4 \times K_5 \times K_6)),1)$; % Initial parameter $P$ calculation.
  9. Iterate equation (1) given in section 2.2 using initial variables and parameters calculated in 5,6,7,8 steps to obtain sequence $X'(i), Y'(i)$.
 10. $x = X'(i), y = Y'(j), i = 1,2,3, \ldots, m; j = 1,2,3, \ldots. n;$
 11. $I'(i,j) = swap\big(Q(i,j), Q(x,y)\big)$; %permuted image
 12. %conversion of binary sequence $w'$(obtained in 2.2.1) to 8-bit integer value as;
 13. $w'(i) = mod(floor(w'(i) \times 10000000000000), 2^8);$
 14. $I' \to {I_R}', {I_G}', {I_B}'$ (% split permuted image in three channels $R, G, B$)
 15. % Red channel first pixel substitution in step 16, with $v_0 = 234$,
 16. $\begin{cases} j = mod[(1 + I'_R(2)), H] + 1, \\ E(1) = sub\_byte[\boldsymbol{S_{box1}}, v_0 \oplus I'_R(1)] \oplus w'(j), \end{cases}$
 17. % $i^{th}$ pixel substitution in step 18,
 18. $\begin{cases} j = mod\big[\big(i + I'_R(i+1)\big), H\big] + 1, \\ E(i) = sub\_byte[\boldsymbol{S_{box1}}, E(i-1) \oplus I'_R(i)] \oplus w'(j), \\ i = (1,2,3, \ldots\ldots.. H - 1) \end{cases}$
 19.        % Last $H^{th}$ pixel substitution in step 20, with $vl = 56$;
```

```
20. $\begin{cases} j = mod[(H + v_0 + vl), H] + 1, \\ E(H) = sub\_byte[\boldsymbol{S_{box1}}, E(H-1) \oplus I'_R(H)] \oplus w'(j), \end{cases}$
21. $E_R(i,j)$ %Red channel encrypted image
22. Repeat the steps [15-20] for green and blue channel substitution.
23. $E(i,j) = cat(3, E_R(i,j), E_G(i,j), E_B(i,j))$ %Encrypted image
24. End.
```


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

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

(i) (j) (k) (l)

Figure 2.5: (a) Original Lena image (b) Lena-image Red layer (c) Lena-image Green layer (d) Lena-image Blue Layer(e) Permuted image (f) Red-layer permuted image (g) Green-layer Permuted image (h) Blue-layer permuted image(i) Encrypted Image (j) Red-layer of encrypted image (k) Green-layer of encrypted image (l) Blue-layer of original image

2.6 Security Analysis

To analyze the suggested encryption outline strength, experiments to check security are performed on "Lena" image. The standard analysis used to examine encrypted image are histogram, entropy, adjacent pixel correlation, UACI, and NPCR analysis. The proposed scheme simulations are done via MATLAB 9.1.0.441655 (R2016b). The initial and parametric values of modified quadratic map were chosen as $X(0) = 0.02001, Y(0) = 0.03, P(0) = 3.15, R(0) = 1.60,\ vl = 56, v_0 =$

234 and the inputted random keys are taken as $K_1 = 0.253496532144, K_2 = 0.467321337632, K_3 = 0.100643892652, K_4 = 0.564329647734,$ $K_5 = 0.472931065490,$ $K_6 = 0.689546143287, K_7 = 0.6257742381092, K_8 = 0.734518093476, K_9 = 0.779834561276.$

2.6.1 Entropy

An encryption scheme having the entropy values close to 8 are highly resistant against the attacks. The entropy results of proposed encrypted image and its comparison with other schemes are shown in Table 2.6. Entropy values for each layer of proposed image are close to optimal value. Also, the comparison depicts that the proposed scheme achieved better results as compared to others.

Table 2.6: Comparison of Entropy Analysis

Images	R	G	B	Average
Proposed	7.99842	7.99867	7.99789	7.99832
[76]	7.99614	7.99408	7.99686	7.99569
[77]	7.9973	7.9969	7.9971	7.9971
[78]	7.9901	7.9912	7.9921	7.9911
[33]	--	--	--	7.9973

2.6.2 Analysis for Key

Total number of keys used in the encryption techniques are considered as key space. The proposed scheme has nine random keys given in section 2.6, and $\{X, Y, P, R\}$ are used. The computational accuracy is 10^{14}, so total number of keys are $(10^{14})^{13} = 10^{182}$ which is quiet enough to resist against attacks.

2.6.3 Correlation Analysis

Algorithms for encryption must have the ability to provide relations among the connecting image pixels in vertical, horizontal, and diagonal directions. The highly correlated pixels have estimated coefficient values near 1 or -1 while the non-correlated pixels coefficient values are close to zero. The correlation analysis of proposed original and ciphered RGB image in horizontal, vertical, and diagonal directions is given in Table [2.7, 2.8,2.9]. Figure 2.6 represents horizontal, vertical, and diagonal correlation analysis for RGB image. Clearly seen from tables that the correlation of original image for each channel is near 1 but for ciphered images values are near zero which depicts that there is no correlation between adjacent pixels of ciphered images which makes difficult for attacker to attack.

Table 2.7: Horizontal Correlation

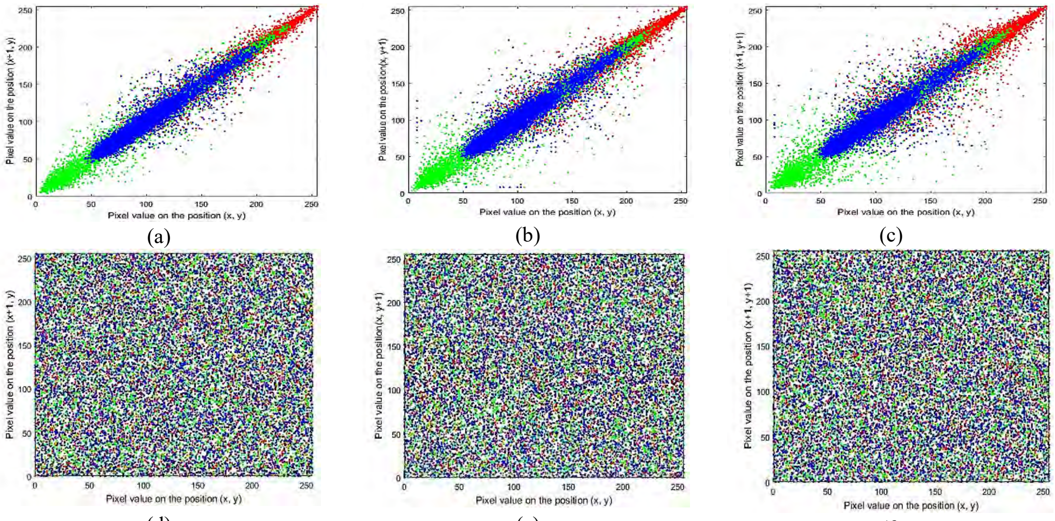
Images	R	G	B
Original	0.9595	0.9460	0.8956
Encrypted	-0.0110	-0.0017	0.0033

Table 2.8: Vertical Correlation

Images	R	G	B
Original	0.94499	0.9674	0.9306
Encrypted	-0.0021	0.00205	0.0019

Table 2.9: Diagonal Correlation

Images	R	G	B
Original	0.9272	0.94136	0.9164
Encrypted	0.00297	0.0021	-0.0285



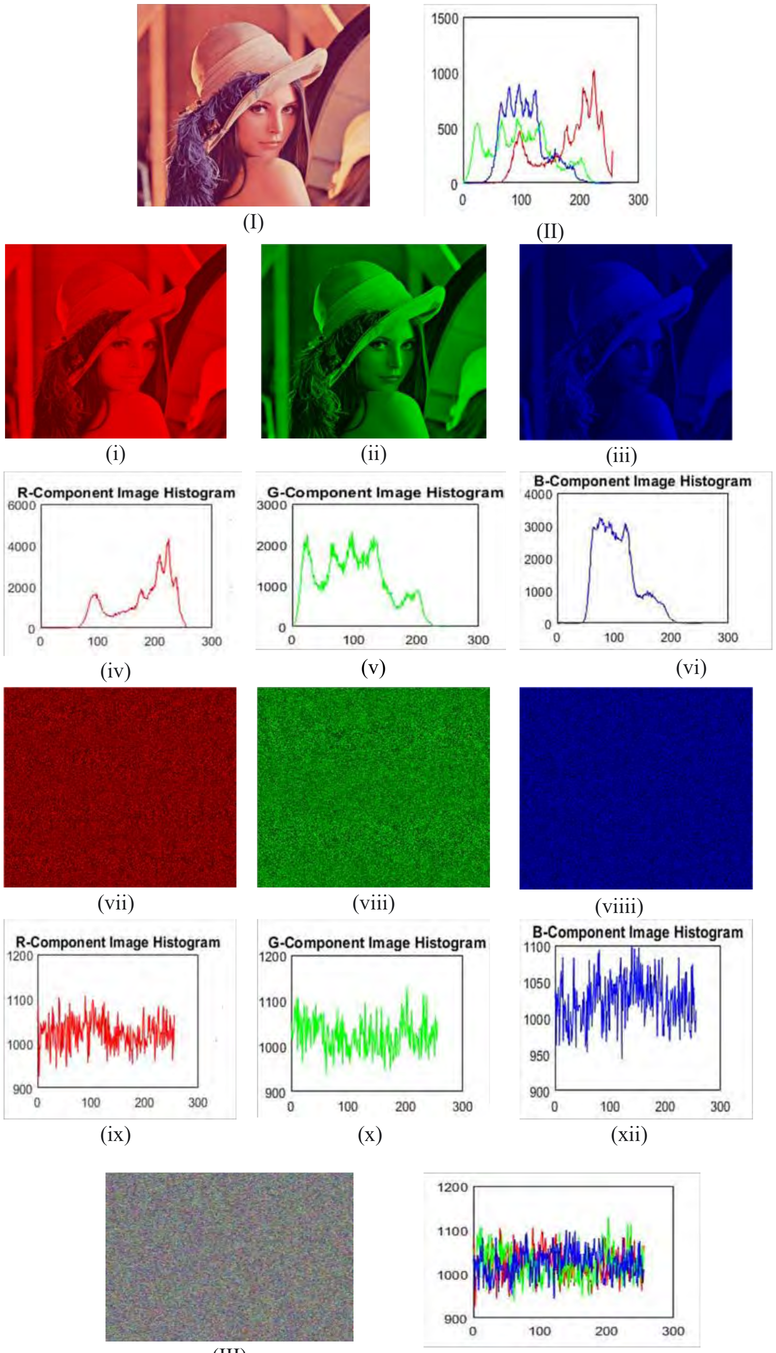
(a) (b) (c)

(d) (e) (f)

Figure 2.6: Plain image correlation analysis (a) Horizontally, (b) Vertically (c) Diagonally ; Ciphered images (d) Horizontal correlation (e) vertical correlation (f) Diagonal correlation.

2.6.4 Histogram Analysis

To assess the security of encryption schemes, uniformity of encrypted image histogram is very important. To check the pixel values dispersion in certain image this analysis is used. An encryption scheme has strong algebraic properties if its histogram is uniform. The proposed encrypted image histograms are identical and altered from original image, which ensures its resistance against the attacks. In Figure 2.7, histogram of original and encrypted Lena image is presented. Also, in figure 2.7 each layered histogram of Lena original and encrypted image is given. So, by figures it is clearly seen that the histogram of encrypted image is totally different from original image and shows excellent results.



(I) (II)

(i) (ii) (iii)

(iv) (v) (vi)

(vii) (viii) (viiii)

(ix) (x) (xii)

(III) (IV)

Figure 2.7: (I) Original image (II) Original image histogram (i) Red layer image (ii) Green layer image (iii) Blue Layer image histogram original (iv) red layer (v) green layer (vi) blue layer; Encrypted histogram (vii) Red layer (viii) Green layer (ix) Blue-layer (III) Encrypted combine Image (IV) Encrypted image combine histogram

2.6.5 Chosen Plain-text Attack Analysis

The classical types of attack are defined in Section 1.19 of chapter 1. From those four types of attacks the most important one is chosen plain-text. In permutation phase of proposed scheme, firstly the initial key values are defined which depends on the colored plain image channels information so if the images are different the key streams are also changed. And then in substitution phase, the pixels of permuted image R, G, B layers are substituted with S-boxes and the chaotic sequence. And for every layer different S-boxes are used which enhance the security of proposed schemes. So, the proposed encryption process strongly interlinks the image content with keys in such a way that a slight change in key would change the sequences thus making it resistant against attacks.

2.6.6 Differential Analysis

Generally, crackers make little change in original image pixels and apply the same encryption steps on that image to encrypt. After the encryption they notice the association of ciphered images. So, against differential assaults proposed technique robustness is analyzed via number of changing pixels rate and average unified intensity change typically known as: NPCR and UACI.

The proposed image (Lena) UACI and NPCR values are provided in Table 2.10. From results, we have seen that the percentage of NPCR and UACI is greater than 99% and 33.4%. Also, its comparison depicts that proposed technique NPCR results for each layer are better than other compared schemes and UACI results are better than [76] and comparable with others.

Table 2.10: Proposed scheme NPCR, UACI analysis and comparison

	NPCR			UACI		
Images	**R**	**G**	**B**	**R**	**G**	**B**
Proposed	0.99756	0.99687	0.99598	0.33123	0.33242	0.33067
[**76**]	0.996429	0.995956	0.995285	0.327633	0.300491	0.275669
[**77**]	0.9960	0.9961	0.9961	0.3356	0.3345	0.3349
[**78**]	0.9966	0.9954	0.9967	0.3312	0.3400	0.3390

2.7 NIST Analysis

The security level of any system could be noted by identifying its complexity, distribution, output data and period. Secured systems have large period, high complexity and uniformity. NIST SP 800-22 analysis is used for testing the digital images randomness [79]. Few test parts have subclasses which are copious. For image randomness testing, great beginning key deals are utilized. Ciphered image is obtained by completely blended encryption technique of color (RGB) Lena image. Outcomes of tests are exhibited in Table 2.11. By smashing these outcomes, it can be derived that expected digital image encryption tool efficiently pass NIST tests. Accordingly, considering the accomplished outcomes, the produced random ciphers in proposed encryption algorithm might be declared that are very asymmetrical in its output.

Table 2.11: NIST test results for strongly blended encrypted image

Test	**P – values for color encryptions of ciphered image**				**Results**
		Red	**Green**	**Blue**	
Frequency		0.48662	0.50664	0.18413	Pass
Block frequency		0.88925	0.79697	0.36562	Pass
Rank		0.29191	0.29191	0.29191	Pass
Runs ($\mathbf{M = 10,000}$)		0.35506	0.74652	0.34447	Pass
Long runs of ones		0.7127	0.7127	0.7127	Pass
Overlapping templates		0.85988	0.85988	0.81567	Pass
No overlapping templates		0.99286	1	0.98974	Pass
Spectral DFT		0.88464	0.46816	0.38399	Pass
Approximate entropy		0.00079253	0.49641	0.82903	Pass
Universal		0.99416	0.99018	0.98656	Pass
Serial	**p values 1**	0.0027882	0.89447	0.14816	Pass
Serial	**p values 2**	0.00050648	0.90991	0.46122	Pass
Cumulative sums forward		0.23706	0.24343	0.17915	Pass
Cumulative sums reverse		1.5885	0.61835	0.092695	Pass
Random excursions	$\mathbf{X = -4}$	0.54297	0.026078	0.21236	Pass
	$\mathbf{X = -3}$	0.45415	0.42343	0.50684	Pass
	$\mathbf{X = -2}$	0.54882	0.26033	0.64829	Pass
	$\mathbf{X = -1}$	0.95535	0.44549	0.17235	Pass
	$\mathbf{X = 1}$	0.6787	0.92004	0.12441	Pass
	$\mathbf{X = 2}$	0.091737	0.034076	0.38548	Pass
	$\mathbf{X = 3}$	3.1745e-08	0.03146	0.29277	Pass
	$\mathbf{X = 4}$	0.11988	0.40938	0.54159	Pass
Random excursions variants	$\mathbf{X = -5}$	0.61368	0.76344	0.54694	Pass
	$\mathbf{X = -4}$	0.38132	0.85558	0.31266	Pass
	$\mathbf{X = -3}$	0.046366	0.91425	0.21878	Pass
	$\mathbf{X = -2}$	0.030754	0.94459	0.2763	Pass
	$\mathbf{X = -1}$	0.33466	0.952	0.20873	Pass
	$\mathbf{X = 1}$	0.59873	0.63013	0.81366	Pass
	$\mathbf{X = 2}$	0.59873	0.65143	0.75084	Pass
	$\mathbf{X = 3}$	1	0.46734	0.94398	Pass
	$\mathbf{X = 4}$	0.83989	0.37493	0.92901	Pass
	$\mathbf{X = 5}$	0.69946	0.38827	0.79341	Pass

Chapter 3

An RGB Chaos-based Image Encryption Scheme using SHA-256 and Scan Patterns

Recently, the implementation of set rules of many famous games in encryption field specifically in image encryption, has prompted the crystallization of innovative cryptographic models. Inspired by games, a permutation technique utilizing scan patterns in combination with chaos and secure hash functions is presented in this chapter. In proposed algorithm, permutation stage is achieved by using the scan patterns attained by movement of knight from chess game ideology. The main aim of proposed work is to find the starting position of Knight to obtain patterns for scanning. For this purpose, firstly the chaotic sequences are sorted, then their index values are saved in the form of matrices. Highest index values are then used as starting position of knight. Then after the complete movement of knight, scan pattern is gained. Now these patterns are used for scrambling the bits of pixel values. Then the scrambled image is Xored with chaotic sequences to get final ciphered image. Simulation and experimental analysis illustrate that the scheme shows randomness, attain good experimental results and resistance against brute force attacks.

3.1 Introduction

Due to rapid advancements in the field of information technology, a significant amount of digital data can be produced and distributed across all kinds of networks. The visual texture of digital images is very clear therefore it is broadly used in digital formats of data. Moreover, digital images possess substantial potential and other information. For instance, a particular photograph of person cannot express the appearance only but also give other particulars like their age and health. In addition, protecting the security of image data is particularly important, specifically in fields of medical, military, and commercial. The data of images carries a large amount of information, high-level redundancy, and strong associations. So, the security of such data is very challenging for researchers. Many scrambling techniques for digital images are

designed for hiding the actual information. But the goal of researchers is to find a suitable technique that provide a large amount of security to digital images. For the protection of useful information of images encryption of images plays a vital role [32].

In nonlinear sciences field, chaos theory is active subject for study. Cryptography and chaotic systems have so many similarities like randomness, sensitivity, and periodic behavior. That is the reason mostly scheme involves chaotic theory. Cryptographic algorithm based on low dimensional chaotic systems have low complexity and are easily cracked [5].

Many schemes for encrypting images are proposed in the last few years. Some techniques are suitable and provide good security to images, but some have low complexity. In addition to the classic methods in the design of digital image scrambler based on two-way bijection like schemes centered on chaos [80-81], watermarking [82], scrambling [83], transposition of blocks [84], pixels interchanging and decomposition of matrices [85], some new innovations utilizing the game rules like knight travel path or puzzles alike sudoku or permutation/shuffling based using principles of Rubick's cube/ Poker rules [86-88] for shuffling have their own rightful positions.

The aim of proposed chapter is to utilize the game rules for permuting the location of image pixels bit-wise for creating a massive distortion between the pixels and make it resistant against the attack in combination with the random numbers generated by chaotic map.

3.1.1 Knight's Travel Path

Knight (♘, ♞) is a chess piece in chessboard game which is not allowed to move in a straight line. The normal representation of knight is the neck of horse. In chess piece, Knight has odd pattern of movement. Knight moves two squares horizontally and one vertically, or two vertical squares and one horizontal. A lot of paths exist for the movement of knight but in its movement, it visits every block only one time and not revisit it [5].

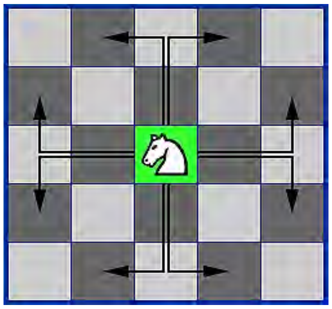
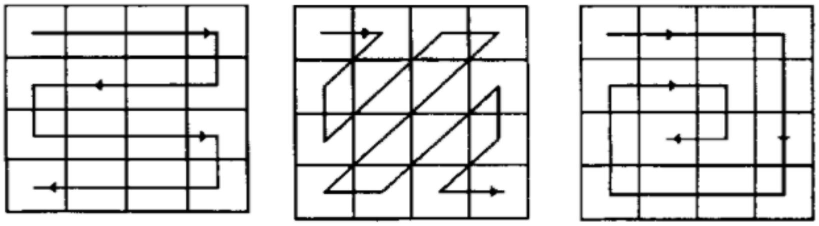


Figure 3.1: Knight Moves

3.1.2 Scan Patterns

Consider an array of two-dimension (2-D) $T_{M\times N} = \{T(i,j): i \in [1,M], j \in [1,N]\}$ is a bijection from $T_{M\times N}$ to set $\{1,2,3, \dots \dots, MN\}$. In other way, a two-dimensional array scan is a pattern where every array element is accessed exactly one time or array elements permutation. For $N \times N$ array there are $(N \times N)!$ scan patterns. A lot of varieties are available for generating scanning pattern by this method [5]. Scan language has basic four scanning patterns i.e., Raster, diagonal, and orthogonal as shown in figure 3.2.



(a) Raster (b) Diagonal (c) Orthogonal

Figure 3.2: Scan Patterns

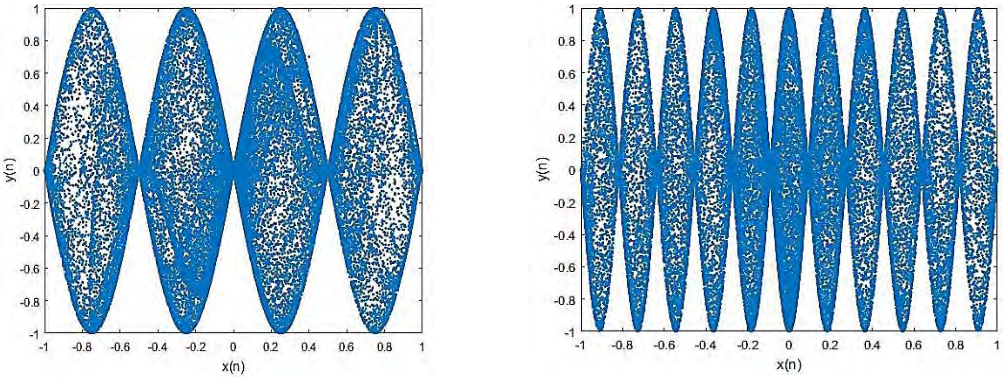
3.1.3 2D Sine Chebyshev Modulation Map (SCMM)

The two-dimensional sine Chebyshev modulation map is defined as [89]:

$$p(i+1) = a\sin[\omega\, q(i) + \varphi] \times \cos\{ccos^{-1}[p(i)]\}$$

$$q(i+1) = a\sin[\omega\, p(i+1) + \varphi] \times \cos\{ccos^{-1}[q(i)]\}$$

where the amplitude a, perturbation frequency c, angular frequency ω, phase φ are the control parameters of above non-linear system of equations and variables p and q are known as state variables. The value of system state variable p, q lies between $(0,1)$. These equations exhibit hyperchaotic behavior at whole range of $a \in (0.355,1], \omega \in [3,9], \varphi \in [0,20]$ but in $c \in [90,110]$ it is hyperchaotic only for even values of c. The initial state variables p_0, q_0 and given control parameters a, c, ω, φ of complete system are solved numerically using Runge-Kutta method (RK-method). The detailed discussion of attractor diagram using different parametric values is given in Ref [89]. The even and odd cavity attractor diagrams of 2D-SCMM are shown in figure 3.3.



(a) (b)

Figure 3.3: Attractor diagrams of 2D-SCMM

3.2 Cryptosystem Design

3.2.1 Initial Key Values by using SHA-256

A function that maps arbitrary data size to data of fixed size is known as hash function. To design one-time pad cryptosystems initial keys are generated by hash value that is, “Secure hash algorithm-256” (SHA-256) [35].

The algorithm uses SHA-256 to generate 256-bit hash value κ of Pepper image.

$$\kappa = \kappa_1, \kappa_2, \kappa_3, \dots \dots . \kappa_{32},$$

where $\kappa_i, i = 1,2,3,4 \dots . . .32$, are 8-bit blocks. The proposed algorithm uses 2D sine Chebyshev modulation map. This map initial values $p_1, q_1, a_1, \omega_1, \varphi_1, c_1$ are calculated by following formulas:

$$p_1 = \frac{\kappa_1 \oplus \kappa_2 \oplus \kappa_3 \oplus \kappa_4}{2^8}$$

$$q_1 = \frac{\kappa_5 \oplus \kappa_6 \oplus \kappa_7 \oplus \kappa_8}{2^8}$$

$$a_1 = (\frac{\kappa_9 \oplus \kappa_{10} \oplus \kappa_{11} \oplus \kappa_{12} \oplus \kappa_{13}}{2^8})$$

$$\omega_1 = \left(\frac{\kappa_{14} \oplus \kappa_{15} \oplus \kappa_{16} \oplus \kappa_{17} \oplus \kappa_{18}}{2^8}\right) + \pi$$

$$\varphi_1 = 2\pi + (\frac{\kappa_{19} \oplus \kappa_{20} \oplus \kappa_{21} \oplus \kappa_{22} \oplus \kappa_{23} \oplus \kappa_{24} \oplus \kappa_{25}}{2^8}) \times 0.1$$

$$c_1 = \left(\frac{\kappa_{26} \oplus \kappa_{27} \oplus \kappa_{28} \oplus \kappa_{29} \oplus \kappa_{30} \oplus \kappa_{31} \oplus \kappa_{32}}{2^8}\right) + 99.5$$

3.2.2 Proposed Image Encryption Scheme

In proposed encryption scheme following phases are used to perform whole encryption and flow diagram is given in figure 3.4:

- Generation of chaotic sequences
- Confusion
- Diffusion

3.2.3 Generation of Chaotic Sequences

1. Apply the method described in section 3.2.1, to compute the variables $p_1, q\ _1, a_1, \omega_1, \varphi_1, c_1$ of 2D-SCMM map.
2. Iterate the map $m \times n$ times with initial conditions $p_1, q_1, a_1, \omega_1, \varphi_1, c_1$ to obtain two chaotic sequences $P' = \{p\}_{mn}$ and $Q' = \{q(i)\}_{mn}$.

3. Again, iterate the map by using the initial conditions randomly selected from previous ones and obtain another set of sequences $P'' = \{p'(i)\}_{mn}$ and $Q'' = \{q'(i)\}_{mn}$ to avoid transitional harmful effects, quantized these sequences as follows:

$$P'' = floor(mod(p'(i) \times 10^{16}, 256));$$
$$Q''= floor(mod(q'(i) \times 10^{16}, 256));$$

4. A new sequence R is obtained as

$$R(i,j) = P''(i,j) \oplus Q''(i,j);$$

where $\oplus$ is used for exclusive OR operation.

3.2.4 Confusion Stage

1) Consider the original image $I(m, n, 3)$.
2) Now sort the chaotic sequences P' and Q' in ascending order. Sort the sequence P' row-wise and sequence Q'column-wise in ascending order and save the index values in matrices M, M' of size $m \times n.$ Check the first row of M and first column of M' and select the position of highest index value. Then write them as order pair (l, r) where l is highest index value position of first row of matrix M and r is highest index value position of first column of matrix M'.
3) Set the order pair (l, r) as starting positions of knight move. After the knight tour a scan pattern is obtained.
4) To create randomness in pixels, extract the first row of plain image and convert the decimal values into binary format. Then apply the scan pattern obtained in step 2 to change the location of binary bits.
5) Now after altering the binary bits position of every pixel, convert binary values of each row back into decimal format hence the permuted row is achieved. Similarly, to change the pixels of second row, move to step 2 and find the starting position for knight move using the position of highest index value of second row and column of matrices M, M'. Repeat the process until the original image pixel values of all rows are permuted/confused. So, the confused image $I'(m, n, 3)$ is obtained. The whole procedure is explained in example given in figure 3.5.

3.2.5 Diffusion

Convert the permuted image $I'(m, n, 3)$ in to three layers i.e.,I'_R, I'_G, I'_B. Apply the exclusive OR operation between $I'_R, I'_G, I'_B$and chaotic sequences P'', Q'' and R as

$$C_1 = bitxor(P'_R, P'')$$
$$C_2 = bitxor(P'_G, Q'')$$

$$C_3 = bitxor(P'_B, R)$$

By combining $\{C_1, C_2, C_3\}$ we obtained a cipher image C. The original and encrypted image are shown in figure 3.6. Applying inverse steps to perform decryption.

	1	2	3	4	5	6	7	8
1	0.1903	0.3433	0.7472	0.4596	0.6725	0.8599	0.1000	0.4790
2	0.3091	0.8145	0.9313	0.2440	0.7036	0.7154	0.3495	0.8671
3	0.6454	0.8729	0.4230	0. 9310	0.2450	0.7059	0.7919	0.6286
4	0.3704	0.4972	0.9535	0.1691	0.5359	0.9486	0.1859	0.5772
5	0.2456	0.9530	0.1708	0.9473	0.5876	0.2669	0.7646	0.7270
6	0.8535	0.4765	0. 9515	0.5532	0. 9427	0.2059	0.3578	0.8764
7	0.4131	0.9247	0.2655	0.7438	0.7572	0.7990	0.9052	0.5131
8	0.8982	0.3487	0.4421	0.9408	0.2125	0.4012	0.9136	0.7892

(a) Chaotic sequence of P'

	1	2	3	4	5	6	7	8
1	0.8725	0.4242	0.9316	0.2430	0.1856	0.7071	0.2775	0.5601
2	0.5000	0.6140	0.1690	0.9847	0.5766	0.4238	0.7819	0.6504
3	0.2274	0.6701	0.8432	0.5042	0.9535	0.1692	0.9535	0.9304
4	0.4248	0.2418	0.6053	0.3086	0.8021	0.2473	0.5852	0.539
5	0.9112	0.8358	0.5234	0.1762	0.3615	0.8819	0.3713	0.2321
6	0.7639	0.9355	0.2065	0.4015	0.2080	0.6080	0.8884	0.1877
7	0.1230	0.3660	0.1886	0.7765	0.6231	0.6924	0.7106	0.4106
8	0.6660	0.7230	0.3545	0.8963	0.1280	0.5596	0.1050	0.9402

(b) Chaotic sequence of Q'

0.1903	0.3433	0.7472	0.4596	0.6725	0.8599	0.1000	0.4790
1	2	3	4	5	6	7	8

(a')

0.1000	0.1903	0.3433	0.4596	0.4790	0.6725	0.7472	0.8599
7	1	2	4	8	5	3	6

(b')

0.8725	0.5000	0.2274	0.4248	0.9112	0.7639	0.1230	0.6660
1	2	3	4	5	6	7	8

(c')

0.1230	0.2274	0.4248	0.5000	0.6660	0.7639	0.8725	0.9112
7	3	4	2	8	6	1	5

(d')

(a') First row Chaotic Sequence of P' with index values (b') Row-wise Sorted Chaotic Sequence of P' with index values (c') First column Chaotic Sequence of Q' with index values (d') Column-wise Sorted Chaotic Sequence of Q' with index values.

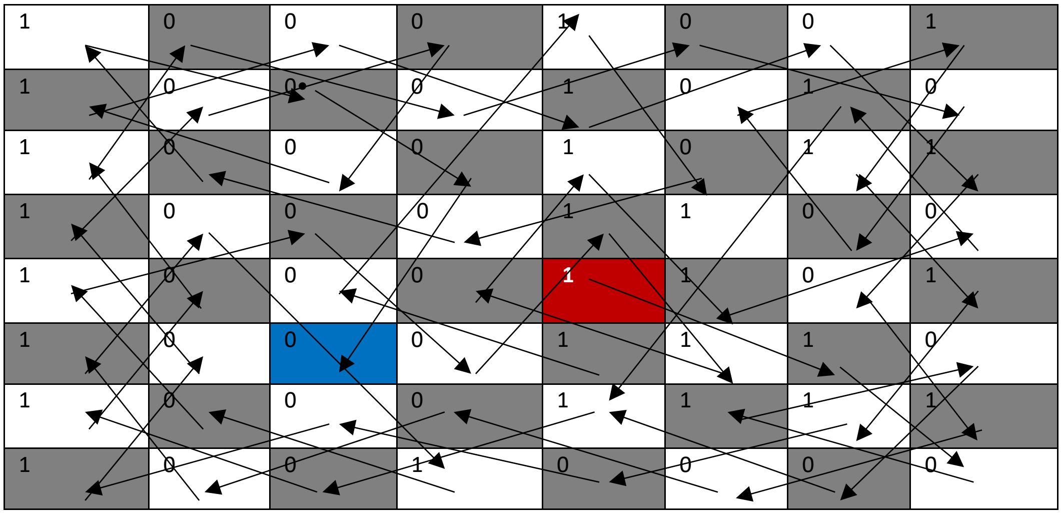
7	1	2	4	8	5	3	6
4	1	7	5	6	2	8	3
5	3	8	1	6	7	2	4
4	7	1	2	5	8	6	3
3	1	6	5	8	7	4	2
6	7	2	4	1	8	5	3
3	1	8	4	5	6	7	2
5	2	6	3	8	1	7	4

(c) Row-wise Sorted index values of P' as matrix (M)

7	4	2	5	8	3	8	6
3	7	7	1	1	4	1	5
4	1	6	4	6	2	5	7
2	2	8	6	5	8	4	4
8	3	5	3	2	6	7	1
6	8	4	7	7	7	2	2
1	5	3	8	4	1	6	3
5	6	1	2	3	5	3	8

(d) column-wise Sorted index values Q' as matrix (M')

The highest index value of row-wise sorted sequence P' lies at 5 place and in (d') location of highest index value of column-wise sorted sequence Q' is also 5, so value of $(l,r) = (5,5)$. Consider (5,5) as starting position of knight.



1	0	0	0	1	0	0	1
1	0	0	0	1	0	1	0
1	0	0	0	1	0	1	1
1	0	0	0	1	1	0	0
1	0	0	0	1	1	0	1
1	0	0	0	1	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	0	0	0	0

(e) Scan Pattern

137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152
153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168
169	170	171	172	173	174	175	176
177	178	179	180	181	182	183	184
185	186	187	188	189	190	191	192
193	194	195	196	197	198	199	200

(f) Input Image

137	138	139	140	141	142	143	144

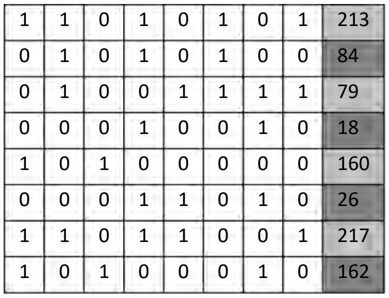
(g) Extract first row

137	1	0	0	0	1	0	0	1
138	1	0	0	0	1	0	1	0
139	1	0	0	0	1	0	1	1
140	1	0	0	0	1	1	0	0
141	1	0	0	0	1	1	0	1
142	1	0	0	0	1	1	1	0
143	1	0	0	0	1	1	1	1
144	1	0	0	1	0	0	0	0

(h) Convert decimal to binary

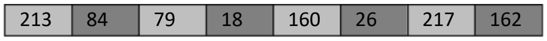
(5,5)	(7,6)	(8,8)	(6,7)	(8,6)	(7,8)	(5,7)	(3,8)
(1,7)	(2,5)	(1,3)	(2,1)	(4,2)	(6,1)	(8,2)	(7,4)
(6,2)	(8,1)	(7,3)	(8,5)	(7,7)	(5,8)	(3,7)	(1,8)
(2,6)	(1,4)	(2,2)	(4,1)	(3,3)	(1,2)	(3,1)	(5,2)
(7,1)	(8,3)	(7,5)	(8,7)	(6,8)	(4,7)	(2,8)	(1,6)
(2,4)	(3,6)	(4,8)	(2,7)	(1,5)	(3,4)	(4,6)	(5,4)
(6,6)	(4,5)	(5,3)	(6,5)	(8,4)	(7,2)	(6,4)	(5,6)
(3,5)	(4,3)	(5,1)	(6,3)	(4,4)	(2,3)	(1,1)	(3,2)

(i) Pixel positions Rearrangement



1	1	0	1	0	1	0	1	213
0	1	0	1	0	1	0	0	84
0	1	0	0	1	1	1	1	79
0	0	0	1	0	0	1	0	18
1	0	1	0	0	0	0	0	160
0	0	0	1	1	0	1	0	26
1	1	0	1	1	0	0	1	217
1	0	1	0	0	0	1	0	162

(j) convert binary to decimal



213	84	79	18	160	26	217	162

(k) first Shuffled row

Figure 3.5 (a-k): Example of Proposed Scheme

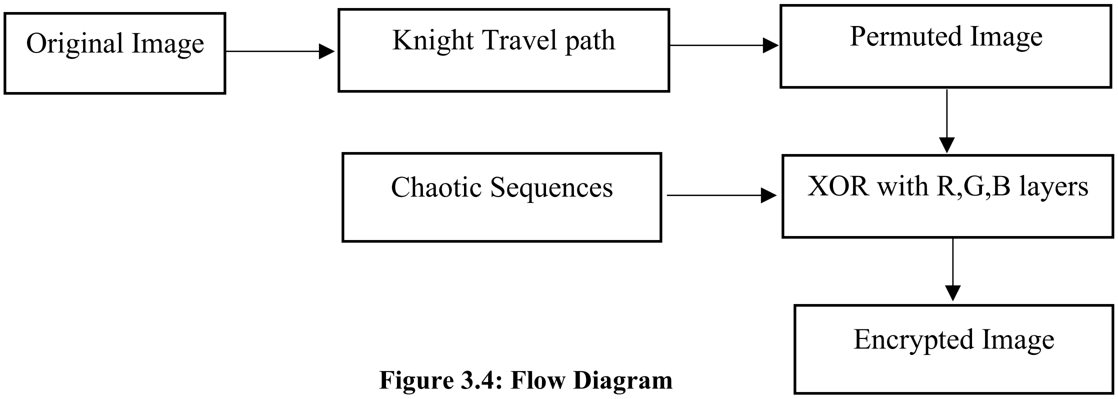
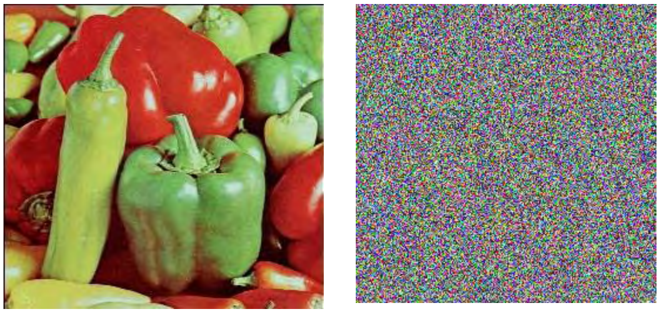


Figure 3.4: Flow Diagram



(a) (b)

Figure 3.6: Pepper (a) Original image (b) Encrypted Image

3.3 Proposed Scheme Analysis

In this section proposed scheme is analyzed by different texture and experimental analysis. A colored Pepper image is used as an input plain-image as illustrated in figure 3.6 (a). MATLAB 9.1.0.441655 (R2016b) is used to implement whole process of encryption/decryption. Let $\chi_o = \{p_1, q_1, a_1, \omega_1, \varphi_1, c_1\}$ represent initial set of keys which are used as secret keys.

3.3.1 Key Space Analysis

The robustness of any cryptosystem highly depends on key space. The large key space of any cryptosystem can provide strong security to resist any brute force attacks. In proposed algorithm, the secret keys are

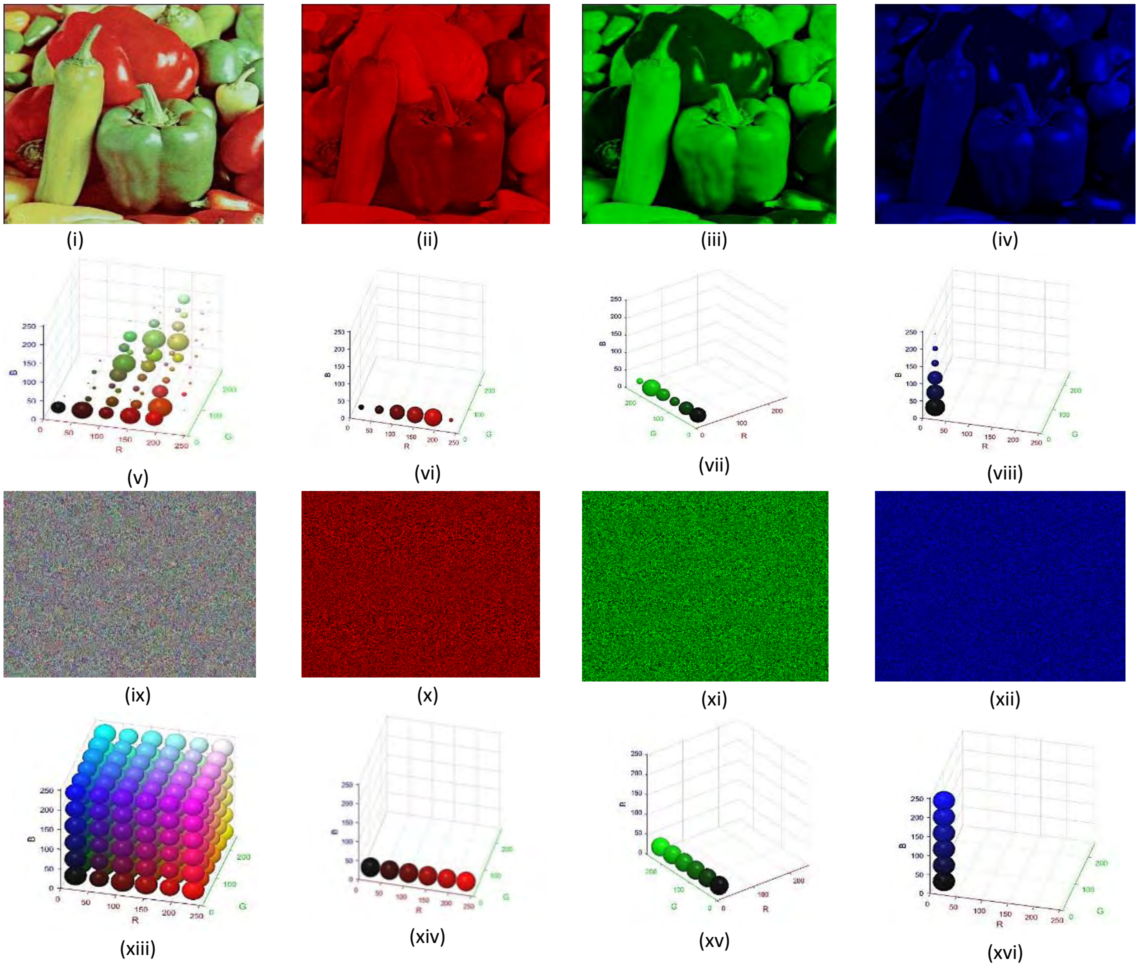
(a) Initial parameters $p_1, q_1, a_1, \omega_1, \varphi_1, c_1$.

(b) Hash-value of 256 bits.

The computational accuracy of presented algorithm is 10^{15}. So, the size of key space is 10^{90}. Also, the SHA-256 security along complexity for excellent attack is equal to 2^{128}.Consequently, the total keys of suggested scheme are equal $2^{128} \times 10^{90}$, which is large enough for preventing the attack on proposed scheme from unauthorized parties. Hence, the computational key attack of brute forces is completely infeasible.

3.3.2 Histogram Analysis

Histograms analyze dispersion of pixel values intensity in a specific image. Here, a colored pepper image is analyzed and its histograms for every layer are given. Each layered 3-D (Three-dimensional) histogram of plain and ciphered pepper image is shown in Fig 3.7. From figures, it is demonstrated that the 3-D histograms of ciphered image and its layers i.e., R, G, B are very consistent and entirely distinct from plain histograms of image. Plain and encrypted image histograms comparison depict encrypted scheme resistance against attacks and leakage of information impossible.


(i) (ii) (iii) (iv)

(v) (vi) (vii) (viii)

(ix) (x) (xi) (xii)

(xiii) (xiv) (xv) (xvi)

Figure 3.7: (i) Pepper Original image (ii),(iii),(iv) are its R,G,B Layers (v), (vi), (vii), (viii) represents histogram of original and layer-wise each channel, (ix),(x),(xi)(xii) are the encrypted images of pepper (xiii),(xiv),(xv)(xvi) are corresponding histograms of encrypted images

3.3.3 Correlation

In encryption schemes correlation coefficients are used to measure correlation of adjust pixels horizontally, vertically, and diagonally. Correlation definition is explained in Chapter 1, section 1.16. From plain and encrypted images, 3000-pixel pairs are randomly elected along each direction (Vertical, horizontal, diagonal). Compute the coefficients of correlation for adjacent pixels. Adjacent pixels correlation coefficients are computed in Table 3.1, As it can be seen that for each layer, correlation value of plain pepper image is near one, but the encrypted values are close to 0. From results it is concluded that the suggested technique can preserve the information of image. Correlation in horizontal, vertical, and diagonal direction is shown in Fig [3.8-3.13].

Table 3.1: Correlation Analysis

	Planes	Horizontal		Vertical		Diagonal	
		Original	Encrypted	Original	Encrypted	Original	Encrypted
	Red	0.8806	-0.00091	0.9506	0.0076	0.8818	-0.000050
Peppers	Green	0.9468	0.00020	0.8848	-0.00038	0.9468	0.00045
	Blue	0.8818	-0.00004	0.8828	0.000006	0.8806	-0.00003

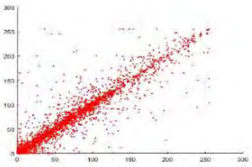


Fig 3.8: Horizontal correlation of original image

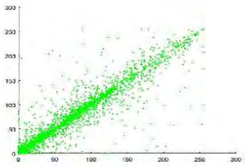


Fig.3.9: Vertical correlation of original image

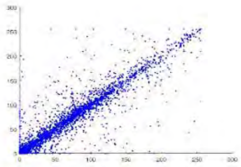


Fig.3.10: Diagonal correlation of original image

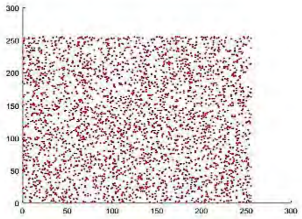


Fig.3.11: Horizontal correlation of encrypted image

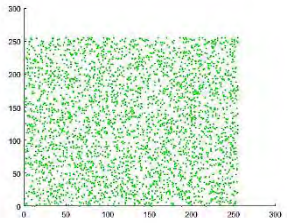


Fig.13.12: Vertical correlation of encrypted image

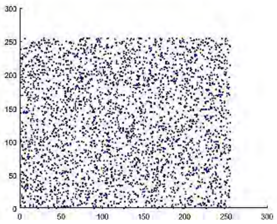


Fig.3.13: Diagonal correlation of encrypted image

3.3.4 Textual Analysis

In the modern world of computer and internet, digital images are one of the most powerful and effective tools of digitalized media. In addition to color, texture is the key factor to what defines a good digital image. Analysis of texture have been done via many different approaches such as Fourier or wavelet transform, but by far the most accurate approaches have been revolving around human system of vision observing texture [43]. To analyze the image texture following analysis are defined commonly known as Energy, Contrast, Homogeneity and Entropy (See section 1.16, Chapter 1). The results of Homogeneity, Energy, Contrast of proposed image are displayed in Table 3.2,

Table 3.2: Textual image analysis

Test	Colored components of plain image			Colored components of ciphered image		
	R	G	B	R	G	B
Contrast	0.28081	0.3024	0.3122	10.5366	10.6188	10.3673
Energy	0.1599	0.0999	0.1674	0.0156	0.0156	0.0156
Homogeneity	0.9068	0.8803	0.8673	03868	0.3903	0.397

3.3.5 Entropy

Entropy can indicate the distribution of pixel values in images. Table 3.3 lists the results of entropy for R, G, B layers of plain and ciphered pepper images. From Table 3.2, it is clearly seen that the entropy values of all ciphered images are near optimal value i.e., 8, which shows that the loss of information in proposed encryption technique is imperceptible, and the proposed encryption scheme is robust against any entropy attacks.

Table 3.3: Entropy analysis of original and encrypted image

		Red	*Green*	*Blue*
Pepper Image	Original	7.3921	7.6149	7.1738
	Encrypted	7.9988	7.9990	7.9992

3.3.6 Differential Analysis

A robust encryption technique must be sensitive to alteration of original image to achieve resistance against attacks i.e., differential attacks. To check the pixels sensitivity, Number of pixel change rate (NPCR) and unified average change intensity (UACI) have been introduced. For the algorithm with strong sensitivity have greater UACI and NPCR values. The average ideal NPCR value is above 99% and UACI has average ideal value near 33%. For the sensitivity measurement of proposed scheme original pepper image is used as first image and by changing single pixel of pepper plain image second image is achieved. Encrypt both images with the same keys. Then measure the NPCR and UACI values of both ciphered images by using the formulas given in chapter 1 section 1.16. The results of proposed algorithm are exhibited in Table 3.3, which indicates that the proposed technique is so sensitive to original image.

Table 3.3: NPCR and UACI analysis of Pepper image

		Red	***Green***	***Blue***
Proposed Algorithm	**NPCR**	99.6698	99.6786	99.6552
	UACI	33.2343	33.0012	33.7612

3.3.7 Sensitivity of Key

Along with analyzation of histogram, another crucial analysis for testing chaos-based encryption is employed which is known as sensitivity analysis. During the decryption process, a small alteration in key value gives different results. If a small change in single parameter is done, data of encrypted image could not be found. The key sensitivity analysis of proposed scheme is presented in Figure 3.14. From figure analysis, it could be observed that by using a small, alteration in set of keys χ_o, another key set χ_1 is achieved in which only the p_1 is modified to $p'_1 + 10^{15}$ while keeping others unchanged, and in result decrypted image reveals no information. So, proposed scheme is very sensitive to keys.

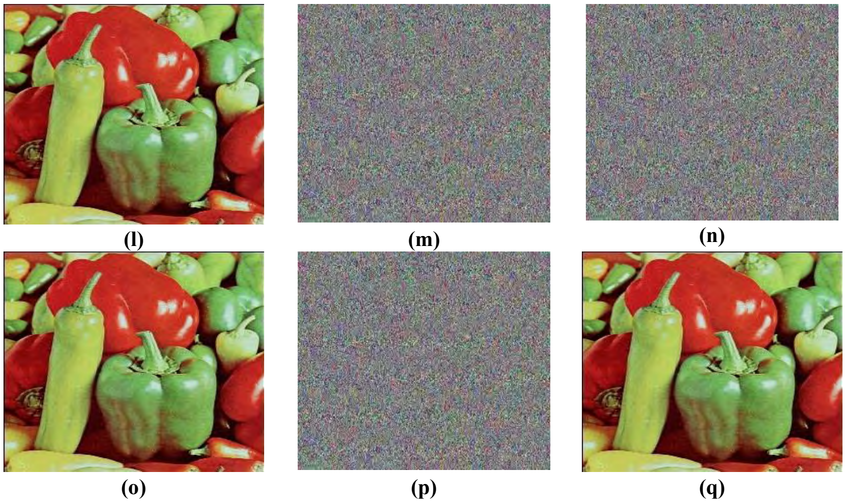

(l) (m) (n)
(o) (p) (q)

Figure 3.14: (l) Original image (m) Encrypted with original key set χ_o (n) Encrypt via simple modification in only one key of χ_o (o) Decrypted image (m) with same key set (p) Decrypted image of (m) via key set via modified key set (q) Decrypted image of (n) using same modified key set

3.3.8 Attack Analysis

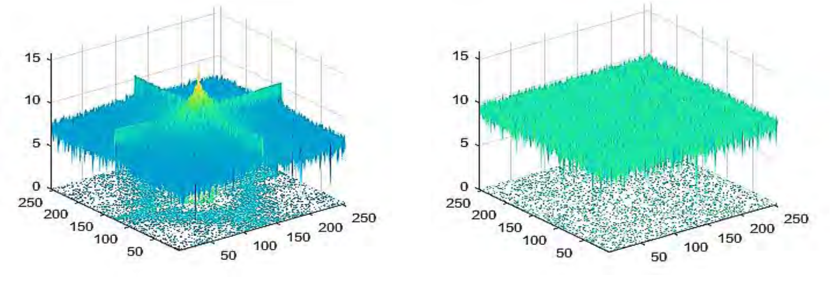
Mostly to hack the information attackers use chosen\known plain-text attacks. So, in proposed technique to secure image information from attacker's, the initial variables and parametric values of SCMM are obtained from hash values of original image. As the keys generated from this map are strongly dependent on image hence, alteration of images also alters the values of secret keys. Therefore, when the secret key values are changed the chaotic sequences are changed which produces different encrypted images. Thus, no information is revealed to the attacker when they try to hack the information using encryption of predesigned images. Consequently, proposed technique is highly resistant against such attacks.

3.3.9 Spectrum Evaluation

To check the cryptosystem effectiveness, two-dimensional (2-D) Discrete Fourier transform is used for analyzation of Pepper original and encrypted images. Mathematical formulation for this is given below [90]:

$$T(r,s) = \sum_{m=1}^{M}\sum_{n=1}^{N} t(m,n)e^{-j(\frac{2\pi}{M})rM}\, e^{-j(\frac{2\pi}{N})sN}$$

here M,N represents image height, width, m,n denotes the pair of image coordinates, $t(m,n)$ signifies location of pixel values of image. Outputs of spectrum evaluation/analysis for original and encrypted images of Pepper are represented in Figure 3.15: it is easily seen from figure that distribution of frequency for original Pepper image is concerted in small region, but ciphered Pepper image has flattened frequency distribution so the chances for leakage of information are very less.



(o) (p)

Figure 3.15: (o) Original image spectrum analysis (p) Encrypted image spectrum analysis

3.3.10 Comparison

In this section proposed scheme analysis with some other schemes is defined and displayed in Table 3.4. Proposed scheme entropy, NPCR, UACI values are compared with other schemes [91-93]. The results depicts that the proposed scheme analysis is better than the others which shows that proposed scheme has strong resistance against the attacks.

Table 3.4: Comparison Analysis

Analysis	Channels	Proposed	[91]	[92]	[93]
	R	7.9988	7.9972	7.9892	7.9892
Entropy	G	7.9990	7.9972	7.9896	7.9896
	B	7.9992	7.9974	7.9896	7.9896
	R	99.6698	99.6414	99.6119	99.6137
NPCR	G	99.6786	99.6032	99.6097	99.6053
	B	99.6552	99.6170	99.6136	99.6079
	R	33.2343	33.4702	33.4811	33.4655
UACI	G	33.0012	33.3418	33.4652	33.4871
	B	33.7612	33.4617	33.4907	33.4746

Chapter 4

Designing of One Time-pad Encryption Scheme using 4D-Dynamical System and Convolution Codes

In this chapter, a novel color image encryption based on permutation and bit-wise exclusive OR (XOR) operation is introduced. The main objective of proposed scheme is to provide technique for safe transmission of image data. A novel technique for creating relation between image pixels and key initial values is proposed in this chapter to minimize the image attacks, as the sensitivity of key to image pixels is enhanced in such a way that if an attacker slightly changes the image pixel, key values are changed too. For this purpose, two random numbers are derived from novel convolution codes technique. These random numbers are then utilized as initial values of four-dimensional (4-D) dynamical system for generation of the chaotic sequences. These sequences are then used in confusion and diffusion phase for segmented images. For the illustration of security level, the proposed scheme is validated via different analysis. The simulation analysis of proposed scheme confirmed the high sensitivity, image pixels uniform distribution and randomness. Also, the classical attack analysis is performed to check security of proposed ciphered image.

4.1 Background

A wide variety of colored image encryption techniques have been developed by the researchers all over the world. A colored image is divided into three components known as R-component, G-component and B-component and their pixel values lies between [0-255], so RGB image has 3-D (three-dimensional) array representation. In cryptography, confusion/diffusions are successfully applied in encryption of images.

Chaos-based systems/scheme are very sensitive to initial values that any small change in them cause completely distinct result. For testing the pseudo-random sequences, standard NIST analysis is used which depicts that for achieving high level security in encryption of images chaos theory based random sequences are best. Many authors used chaos theory in their schemes that have been thoroughly researched and analyzed.

In [94], proposed an algorithm for encryption of images based on chaos and DNA transactions. [95], introduced a chaos-based encryption scheme using cyclic shifts and hash function. In his scheme the author used hash values generated by plain image and used them as keys and for shuffling of pixels cyclic shifts are used. [96], suggested a permutation and diffusion-based image encryption technique utilizing an improved two-dimensional chaotic map. [97] addressed a beta-chaotic map to generate unique groupings in replacement, exchange, and diffusion. Their system effectively advances encryption security. [98] presented an encryption technique and hyperchaotic architecture for input image which is then used to construct key stream. Because of limited space of key this dynamic scheme is easily integrated. A two-dimensional (2-D) Henon-sin-map (HSM) having high characteristic value and its application in encryption scheme is proposed in [99]. [100] presents a hybrid Josephus transversal and four one-dimensional chaotic map-based encryption technique. A securable multi-level permutation algorithm-based color scheme of encryption is introduced in [101]. In this scheme three permutation levels are used to permute image pixels.

Image encryption techniques depend on permutation of pixel bits location are extensively studied to enhance the confusion and diffusion connection and improve the encryption performance. The pixel bits permutation not only alter the stance of bits but also create diffusion in pixel values. In this chapter a secure novel image encryption technique is proposed. Firstly, the generation of initial parametric values is done using the convolution codes based on the pixel values of image. Secondly, the chaotic map sequences generated by using these initial values are used for permuting the location of pixels. Lastly, diffusion is done using bitwise Xor operation between the scrambled image pixels and the keys. Experimental and statistical analysis depicts that the proposed scheme is resistant against attacks and the comparison is also made.

4.1.1 Convolution Codes

In convolution codes simple registers are used for encoding a message. Compared with block codes in convolution the message stream runs continuously through the encoder. Shift registers data of input values set is called state. The input values used for generation of code is called length of constraint. The output set of values are generated by applying XOR operation between the current and shifted input data values. Convolution codes having code rate ($r = k/n'$) which is the ratio of input and output rates. It helps to verify the code efficiency. The input of convolution code is a stream of binary bits and every single bit has double bit output value [102]. In proposed scheme convolution codes having ½ code rate is used having configuration $(n', k, m') = (2,1,3)$ where $n' = number\ of\ output\ bits, k = input\ bits, m' = stages\ of\ shift\ registers.$ Figure 4.1 represents the overall convolution codes scheme

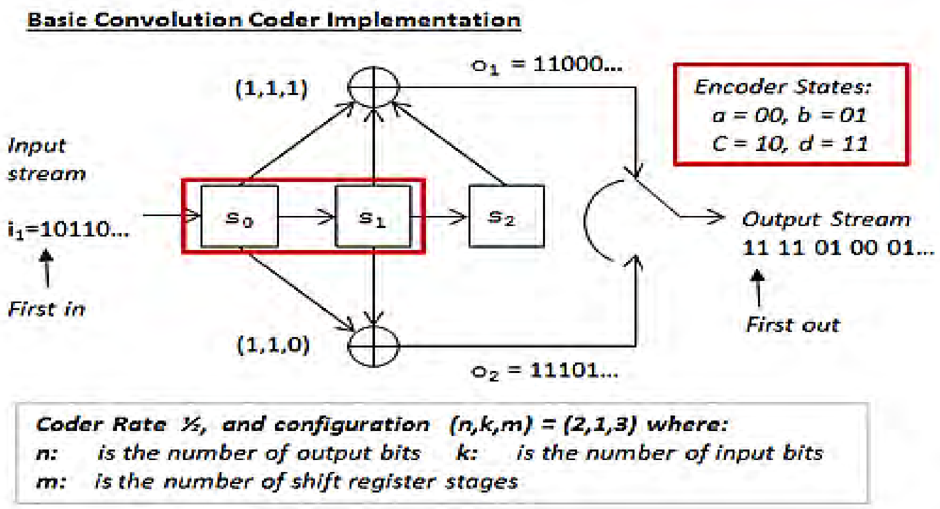

Basic Convolution Coder Implementation
(1,1,1)
o₁ = 11000...
Encoder States:
a = 00, b = 01
C = 10, d = 11
Input
stream
i₁=10110...
First in
s₀
s₁
s₂
Output Stream
11 11 01 00 01...
First out
(1,1,0)
o₂ = 11101...
Coder Rate ½, and configuration (n,k,m) = (2,1,3) where:
n: is the number of output bits
k: is the number of input bits
m: is the number of shift register stages

Figure 4.1 Convolution Codes

4.1.2 Four-dimensional Dynamical System (4D Chaotic map)

A chaotic system having four-dimension is defined as:

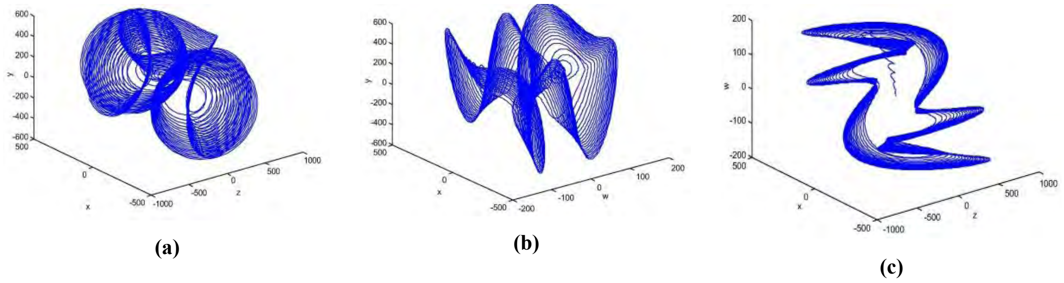
$$\frac{dQ}{dt} = \alpha(R - Q);$$

$$\frac{dR}{dt} = \beta Q - QS;$$

$$\frac{dS}{dt} = QR - RT;$$

$$\frac{dT}{dt} = RS - S;$$

where Q, R, S, T are state variables and α, β are parameters [103]. The three-dimensional chaotic behaviors are shown in figure 4.2.



(a) (b) (c)

Figure 4.2: Chaotic behaviors (a) R-S-T (b) R-S-Q (c) T-Q-S

4.2 Proposed Algorithm

In this section complete technique for encryption of images is described.

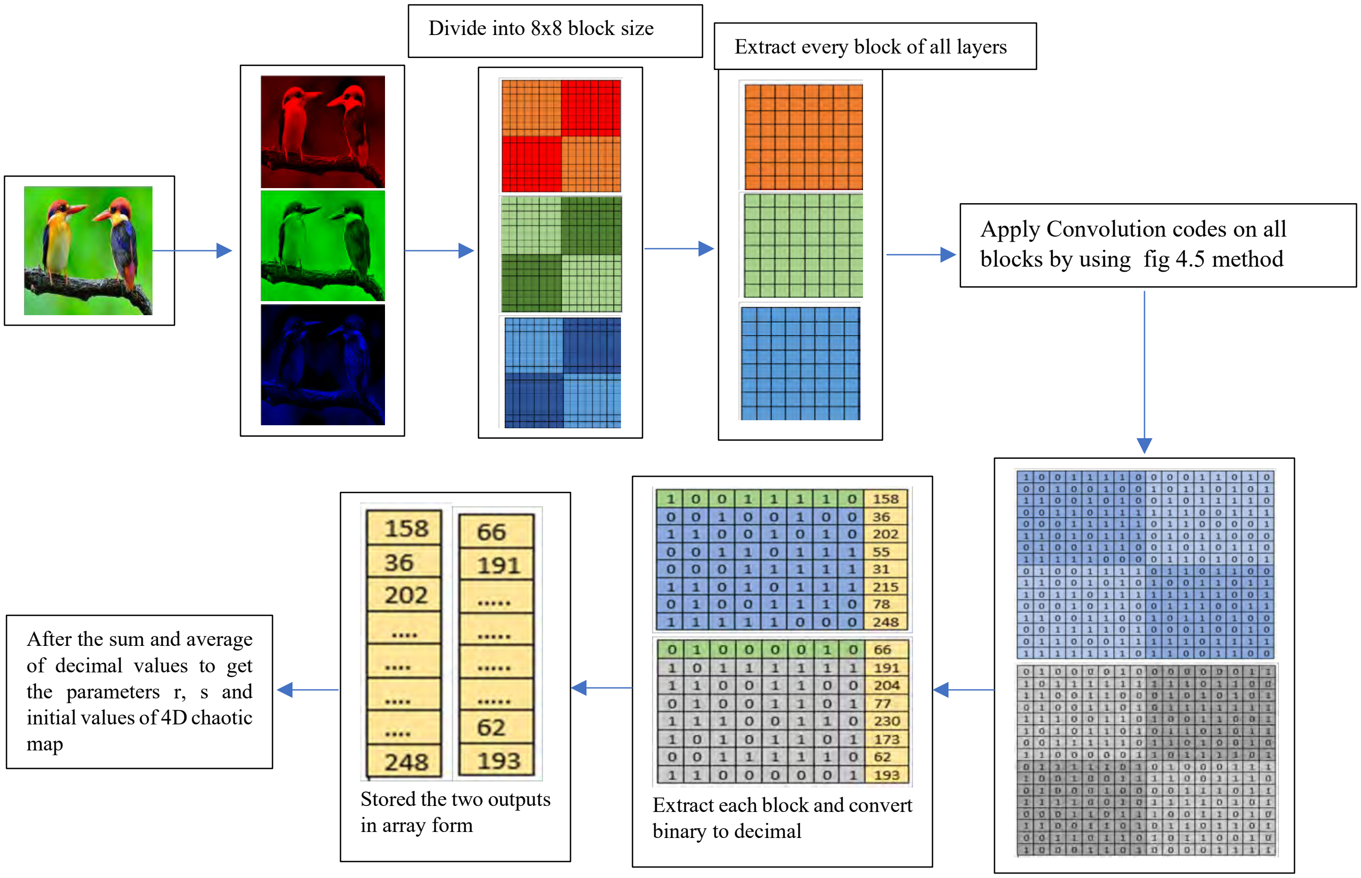
4.2.1 Generation of Initial values of 4D Dynamical System

Here the algorithm for generating the initial values is explained which are then used in the sequence generation of 4-D chaotic map. It involves following steps:

1. First split the image in three layers i.e., R, G, B. Divide each layer into blocks of size 8×8. Consider blocks one by one then convert each pixel into 8-bit binary stream.
2. The binary stream is then used as input value of convolution codes, then after the operations involved in shift register(convolution codes) two outputs are obtained for single input. After these two blocks of 8-bit binary are obtained which are converted to single bits of $0's$ and $1's$ according to the rule that if in 8-bit binary value, the number of $1's$ are greater or equal to zero, replace that entry with 1 otherwise 0. The whole scheme is explained in figure 4.5. by taking example of 2x2 matrix.
3. After step 2, extract each row of blocks and convert the binary values of 8-bit to decimal value as shown in Fig 4.3.
4. Store the decimal values of block one in array v_1 and second block values in array v_2.
5. Reshape the arrays into two matrix forms M and M'.
6. Repeat the steps for each channel i.e. R, G and B. After getting the matrices for each channel take the sum of values and then average of them would generate values of α, β corresponding to matrices M and M'.
7. Now the initial values of state variables $\{Q(0), R(0), S(0), T(0)\}$ are obtained by normalizing the α, β values in range $\{0,1\}$. Normalization of α, β are done by following steps: α value is used for finding initial values of $\{Q(0), R(0)\}$ and β for $\{S(0), T(0)\}$. Now to find the values of $\{Q(0), R(0)\}$divide the value of α with block size value i.e.,

α/BS and the fraction part of the obtained value is used as initial value of $Q(0)$. In same way, initial value $R(0)$ is the fraction part of value when α is divided by plain image size $M \times N \times 3$ $(where\ M\ are\ rows, N\ are\ columns)$. The same process is used for β and the initial values of $\{S(0), T(0)\}$ are attained.

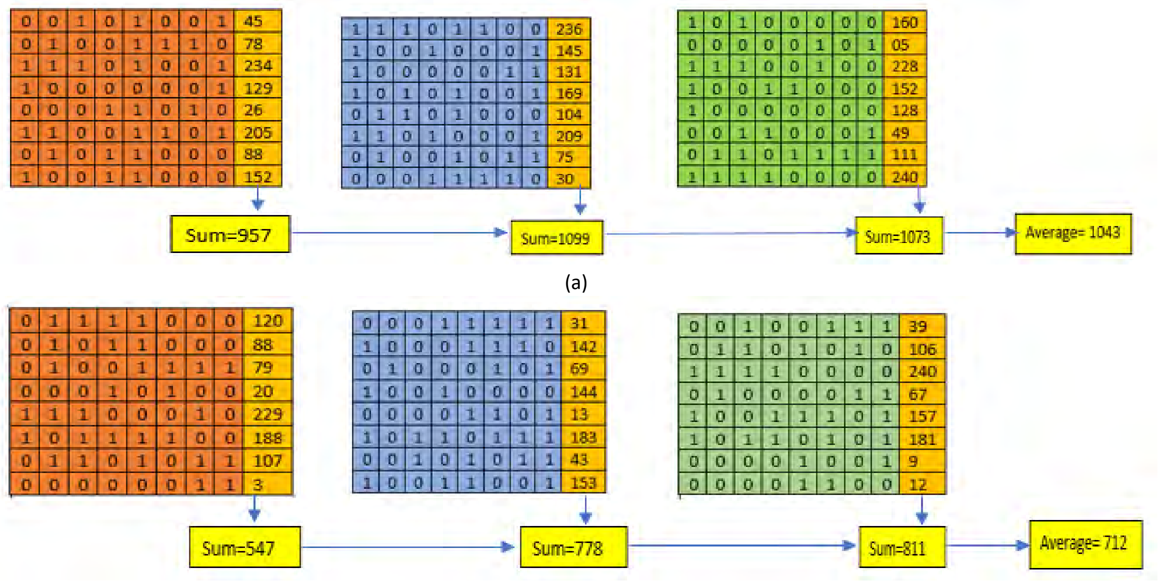
For example, let the values of α, β are $\{225745564, 25127243\}$, block-size= $(M \times 4) \times 3$, size of original image = $M \times N \times 3$, where $M = N = 256$, so the initial value $Q(0)$ is fraction part of 220454.65234375 which is $Q(0) = 0.65234375$ and $R(0) = 73484.884114583$. Similarly, $S(0) = 0.323242187$ and $T(0) = 0.4410807$. The whole process of α, β generation is explained in figure 4.4. And whole procedure for one block is explained in figure 4.3.


Divide into 8x8 block size
Extract every block of all layers
Apply Convolution codes on all blocks by using fig 4.5 method
Extract each block and convert binary to decimal
158
36
202
....
....
....
....
248
66
191
.....
.....
.....
.....
62
193
Stored the two outputs in array form
After the sum and average of decimal values to get the parameters r, s and initial values of 4D chaotic map

1	0	0	1	1	1	1	0	158
0	0	1	0	0	1	0	0	36
1	1	0	0	1	0	1	0	202
0	0	1	1	0	1	1	1	55
0	0	0	1	1	1	1	1	31
1	1	0	1	0	1	1	1	215
0	1	0	0	1	1	1	0	78
1	1	1	1	1	0	0	0	248

0	1	0	0	0	0	1	0	66
1	0	1	1	1	1	1	1	191
1	1	0	0	1	1	0	0	204
0	1	0	0	1	1	0	1	77
1	1	1	0	0	1	1	0	230
1	0	1	0	1	1	0	1	173
0	0	1	1	1	1	1	0	62
1	1	0	0	0	0	0	1	193

Figure 4.3: Methodology for initial values generation



0	0	1	0	1	0	0	1	45
0	1	0	0	1	1	1	0	78
1	1	1	0	1	0	0	1	234
1	0	0	0	0	0	0	1	129
0	0	0	1	1	0	1	0	26
1	1	0	0	1	1	0	1	205
0	1	0	1	1	0	0	0	88
1	0	0	1	1	0	0	0	152

1	1	1	0	1	1	0	0	236
1	0	0	1	0	0	0	1	145
1	0	0	0	0	0	1	1	131
1	0	1	0	1	0	0	1	169
0	1	1	0	1	0	0	0	104
1	1	0	1	0	0	0	1	209
0	1	0	0	1	0	1	1	75
0	0	0	1	1	1	1	0	30

1	0	1	0	0	0	0	0	160
0	0	0	0	0	1	0	1	05
1	1	1	0	0	1	0	0	228
1	0	0	1	1	0	0	0	152
1	0	0	0	0	0	0	0	128
0	0	1	1	0	0	0	1	49
0	1	1	0	1	1	1	1	111
1	1	1	1	0	0	0	0	240

(a)

0	1	1	1	1	0	0	0	120
0	1	0	1	1	0	0	0	88
0	1	0	0	1	1	1	1	79
0	0	0	1	0	1	0	0	20
1	1	1	0	0	0	1	0	229
1	0	1	1	1	1	0	0	188
0	1	1	0	1	0	1	1	107
0	0	0	0	0	0	1	1	3

0	0	0	1	1	1	1	1	31
1	0	0	0	1	1	1	0	142
0	1	0	0	0	1	0	1	69
1	0	0	1	0	0	0	0	144
0	0	0	0	1	1	0	1	13
1	0	1	1	0	1	1	1	183
0	0	1	0	1	0	1	1	43
1	0	0	1	1	0	0	1	153

0	0	1	0	0	1	1	1	39
0	1	1	0	1	0	1	0	106
1	1	1	1	0	0	0	0	240
0	1	0	0	0	0	1	1	67
1	0	0	1	1	1	0	1	157
1	0	1	1	0	1	0	1	181
0	0	0	0	1	0	0	1	9
0	0	0	0	1	1	0	0	12

(b)

Figure 4.4 Generation of $(\boldsymbol{a})\boldsymbol{\alpha}\ (\boldsymbol{b})\boldsymbol{\beta}$

4.2.2 Scheme for Encrypting Images

Encryption of proposed scheme has two steps, Permutations and Bit-wise XOR operation. Flow diagram is shown in Figure 4.6.

4.2.2.1 Image Permutation

Consider the original image $O(m, n, 3)$ where m, n represents the number of rows and columns of image.

Divide the image into four sub-images of equal size as $O1\ , O2, O3, O4$.

Iterate the 4D chaotic map using the initial values obtained in section 4.2.1, to generate the four sequences Q, R, S, T

$$\left.\begin{aligned}
Q &= \{Q_i, Q_{i+1}, Q_{i+2} \ldots \ldots \ldots, Q_{i+(m*n)}\} \\
R &= \{R_i, R_{i+1}, R_{i+2} \ldots \ldots \ldots, R_{i+(m*n)}\} \\
S &= \{S_i, S_{i+1}, S_{i+2} \ldots \ldots \ldots, S_{i+(m*n)}\} \\
T &= \{T_i, T_{i+1}, T_{i+2} \ldots \ldots \ldots, T_{i+(m*n)}\}
\end{aligned}\right\} \quad \ldots\ldots\ldots \quad (1)$$

where $i = 0$.

In proposed scheme permutation is done in such a way that the pixels location of original image for every block are permuted. So, permutation is done using following steps:

- The elements of Q, R sequences (eq 1) are sorted in ascending order and two sorted matrices are obtained. Now take the index values of sorted matrices to obtain the index matrices Q', R'. The process of sorting is given in Figure 4.7.
- The index matrices $Q', R'$are used as permutation matrices P_{ij}, P'_{ij} having size $m \times n$ in proposed scheme. P is used for permuting the pixel positions of block images $O1, O3$ and P' for $O2, O4$ blocks. Permutation matrices P and P' are defined as

$$P = \{P_{ij}\ ;\ P_{ij} \in \{1,2,3, \dots \dots, m \times n\};$$

$$P_{ij}\ are\ distinct; i \in \{1,2, \dots, m\}, j \in \{1,2, \dots, n\}\}$$

$$P' = \{P'_{ij}\ ;\ P'_{ij} \in \{1,2,3, \dots \dots, m \times n\};$$

$$P'_{ij}\ are\ distinct; i \in \{1,2, \dots, m\}, j \in \{1,2, \dots, n\}\}$$

To locate the pixels in new matrix the following row and column formulas are used

$$\left.\begin{aligned} C_{NEW} &= floor\left(\frac{P_{ij} - 1}{n}\right) + 1 \\ R_{NEW} &= mod\left(P_{ij} - 1, m\right) + 1 \end{aligned}\right\} \quad \dots .\ 2(a)$$

$$\left.\begin{aligned} C'_{NEW} &= floor\left(\frac{P'_{ij} - 1}{n}\right) + 1 \\ R'_{NEW} &= mod\left(P'_{ij} - 1, m\right) + 1 \end{aligned}\right\} \quad \dots .\ 2(b)$$

i, j represent the indices of rows and columns.

- Consider the blocks $O1, O3$ and relocate its original pixels by using equation 2 (a), similarly the pixel positions of blocks $O2, O4$ are relocated by using equations 2(b). After these new permuted blocks $O'1, O'2, O'3, O'4$ are obtained.
- Apply the clockwise rotation on O'_1, O'_2, O'_3, O'_4 to achieve the final permuted block images B_1, B_2, B_3, B_4. Figure 4.8, explain the whole permutation process by using an example.

4.2.2.2 Diffusion Process

For diffusion process, quantize the chaotic sequences S, T by following formulas:

$$S(i) = floor(mod(S(i) \times 10^{15}), m)$$

$$T(i) = floor(mod(T(i) \times 10^{15}), n)$$

where m, n are the number of rows and columns of image.

Now apply bit-wise XOR operation by using formulas

$$E_1(i,j) = S(i,j) \oplus B_k(i,j), \qquad where \;\; k = \{1,3\}$$

$$E_2(i,j) = T(i,j) \oplus B_k(i,j), \qquad where \;\; k = \{2,4\}$$

Now the final image is achieved by following equation:

$$E(i,j) = E_1(i,j) \oplus E_2(i,j);$$

Decryption is the reverse step of encryption scheme.

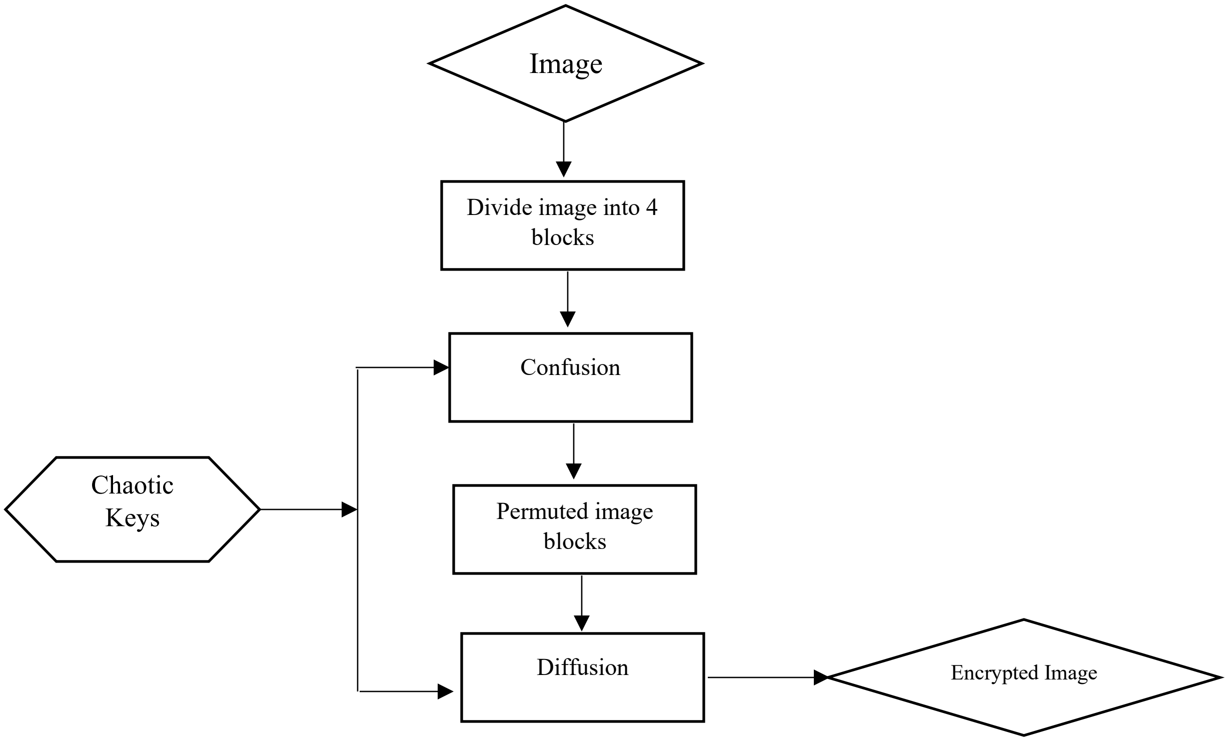


Figure 4.6: Flow Diagram

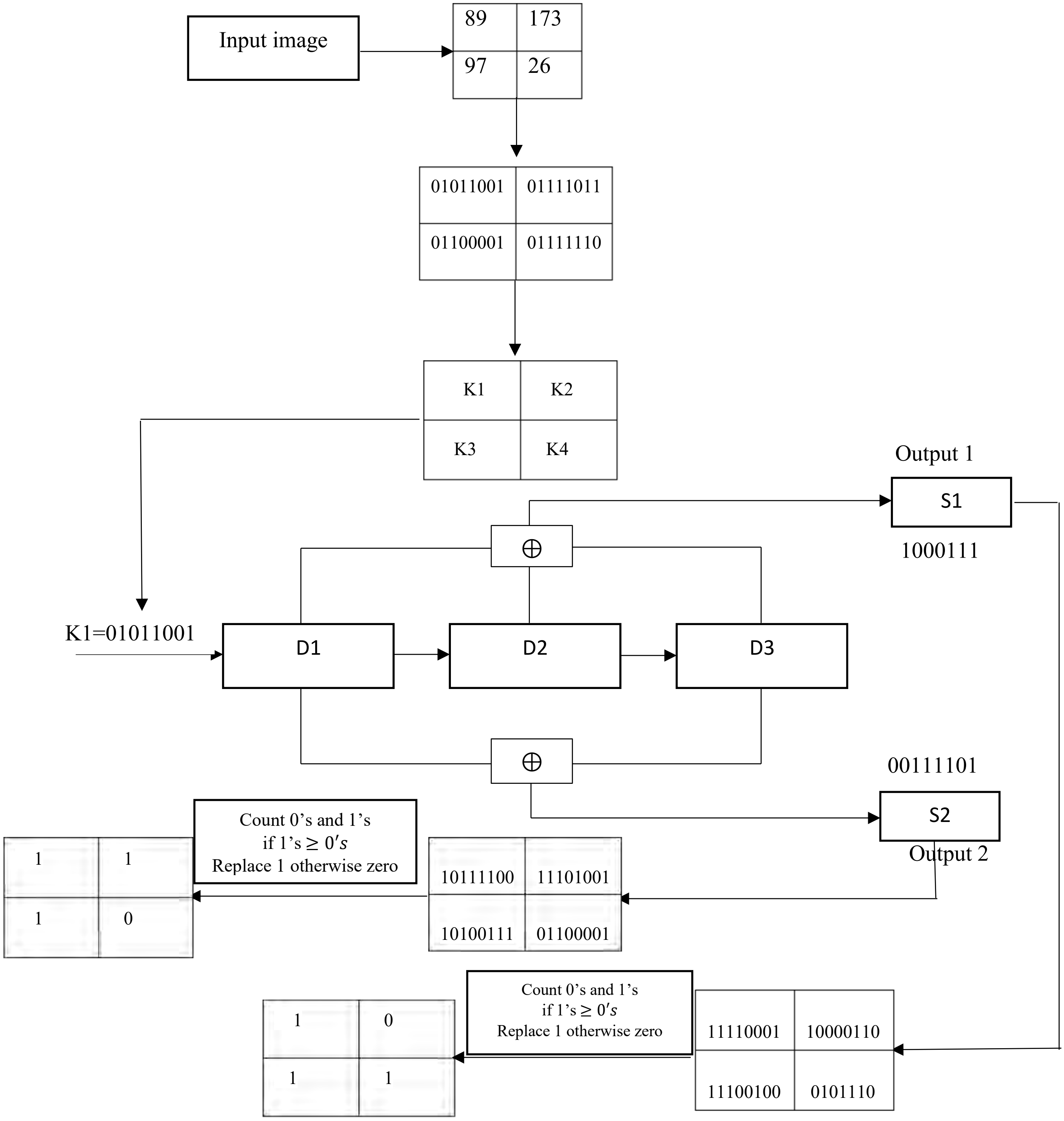
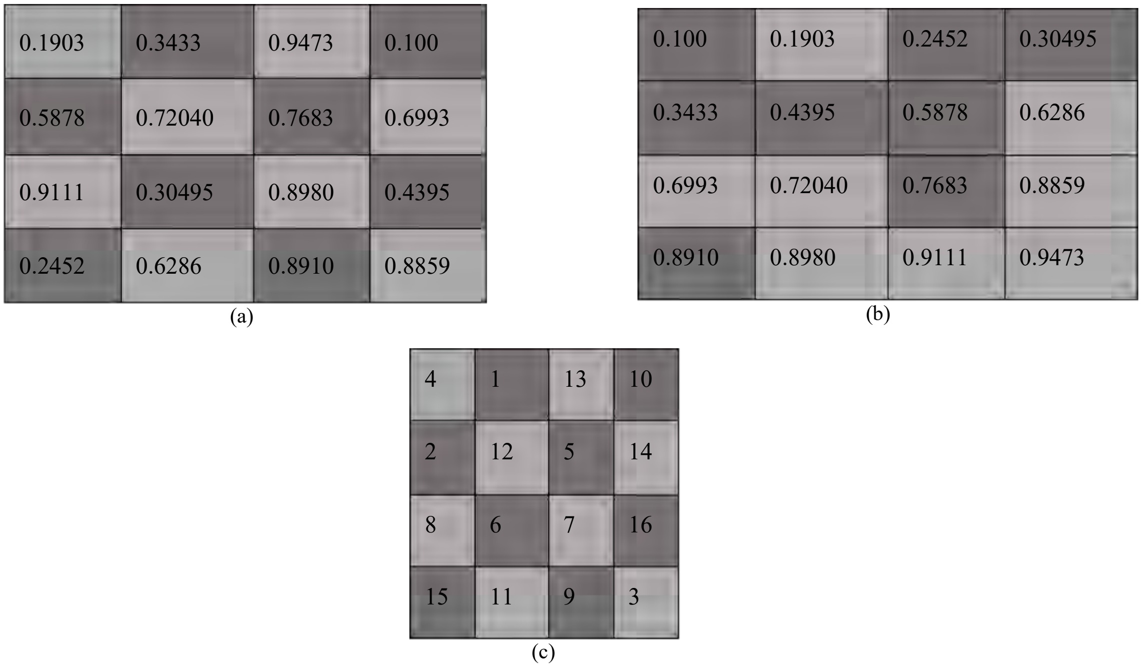


Figure 4.5: Processing of Convolution codes



0.1903	0.3433	0.9473	0.100
0.5878	0.72040	0.7683	0.6993
0.9111	0.30495	0.8980	0.4395
0.2452	0.6286	0.8910	0.8859

(a)

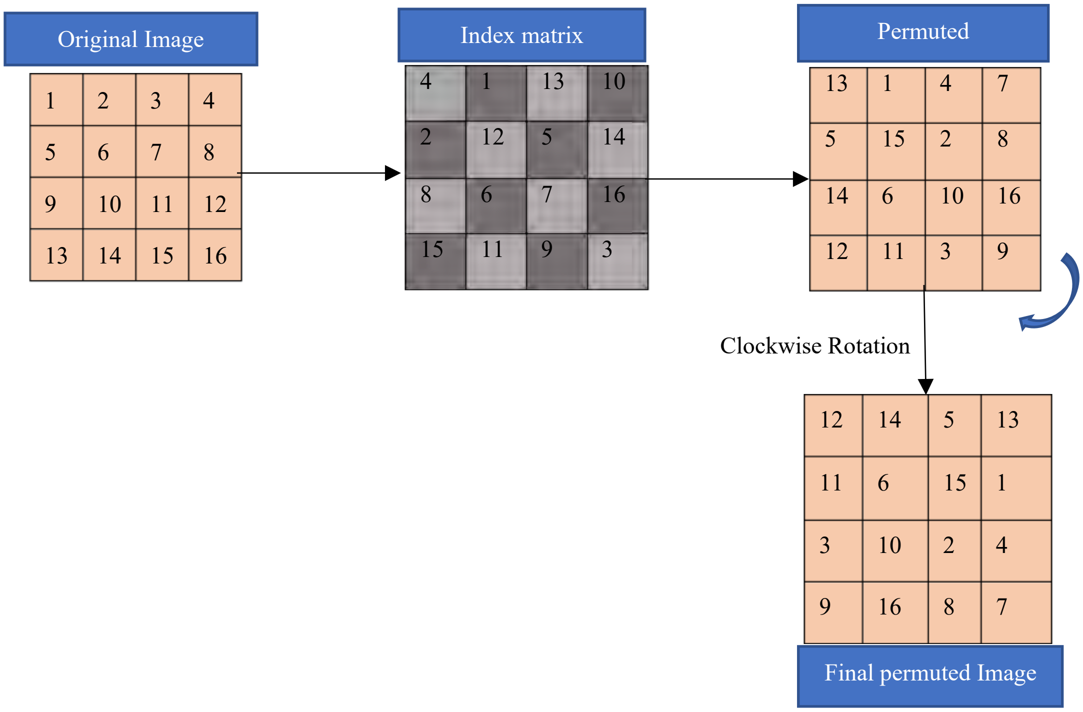
0.100	0.1903	0.2452	0.30495
0.3433	0.4395	0.5878	0.6286
0.6993	0.72040	0.7683	0.8859
0.8910	0.8980	0.9111	0.9473

(b)

4	1	13	10
2	12	5	14
8	6	7	16
15	11	9	3

(c)

Figure 4.7: (a) Chaotic sequence (b) Sorted Sequence (c) Index matrix



Original Image

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

Index matrix

4	1	13	10
2	12	5	14
8	6	7	16
15	11	9	3

Permuted

13	1	4	7
5	15	2	8
14	6	10	16
12	11	3	9

Clockwise Rotation

12	14	5	13
11	6	15	1
3	10	2	4
9	16	8	7

Final permuted Image

Figure 4.8: 4x4 Matrix Example

4.3 Effectiveness of Encryption Scheme

Original Lena and sparrow image and their corresponding encrypted images are shown in Fig 4.9. From the encryption results it is shown that ciphered images have noisy randomness and hence reveal no information.

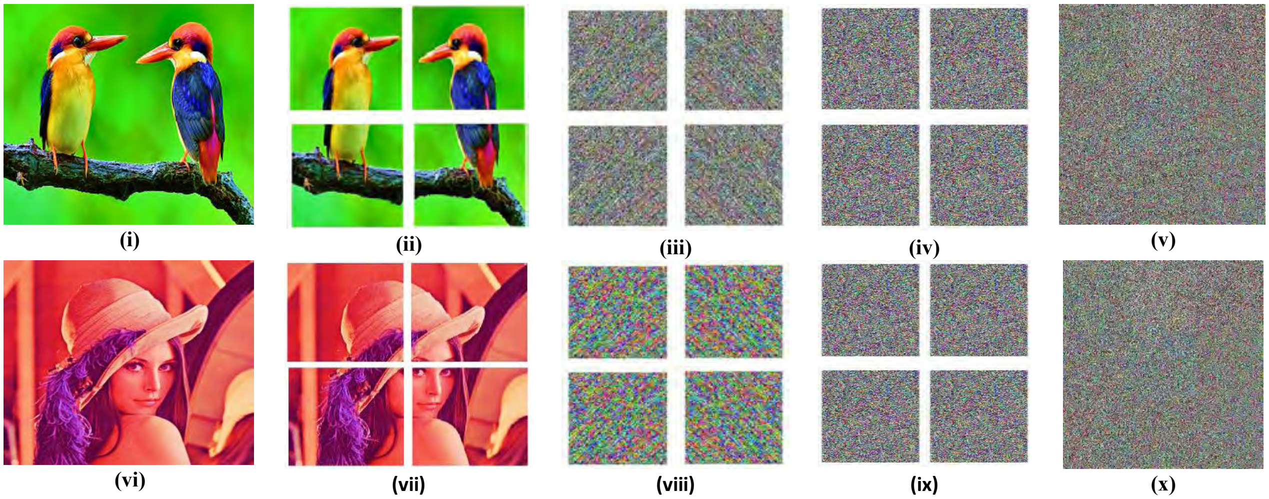


Figure 4.9. (i) Sparrow Image (ii) Block-wise distributed (iii) Permuted block-wise (iv) Blocks after diffusion (v) Combined encrypted Image (vi) Lena Image (vii) Block-wise Lena image (viii) Block-wise permuted Lena image (ix) Block-wise encrypted image (x) Combine image

4.4 Analysis of Proposed Scheme

Proposed scheme is tested via different analysis to check the security and robustness against the attacks is given in this section:

4.4.1 Analysis for Key-Space

Key space is basically total number of keys used in technique of encryption. In presented scheme, the parameters $\{P_0, Q_0, R_0, S_0, T_0, \alpha_0, \beta_0\}$ are used as initial seeds. The suggested algorithm computational accuracy is 10^{15}. So, the size of key space is 10^{105}. Proposed key space is large enough to resist attacks.

4.4.2 Differential Attack

Occasionally, attackers attempt to do small changes in plain images which are used in encryption then observe the changes in its results. In such way, relationship among the plain and ciphered images is observed by attacker. Differential cryptanalysis helps in image decryption. So, the proposed system must be resistant against differential attack, that means no information reveals to attacker (creates difficulty in recognizing the correlation of plain and ciphered image). For this purpose, two parameters are used one is NPCR and other one is UACI. Best value of UACI is close to 0.33. The encryption technique is more sensitive to original plain image if NPCR is greater than 99%. Such values of encryption schemes having large amount of resistance against attacks (i.e., differential-attack). Table 4.1 represents proposed scheme UACI and NPCR values of sparrow and Lena in dataset. In Table 4.1, for Sparrow image, take a random location of pixel for example (27,234,3). The 3 value in colored image indicates blue (B) component of image which state that the pixel location (27,234) lies in B-component. At this point the original pixel value is 191. A slight change in this value of pixel is made and at the location (27,234) a new value 192 is obtained. Now apply encryption on this modified image the UACI, NPCR values of this image are 99.6782% and 33.218% which represent the closeness to values achieved theoretically.

Table 4.1: NPCR and UACI Analysis

Images	Pixel location	Value of pixel	Modified value	NPCR %	UACI %
	(1, 24, 1)	25	26	99.7278	33.321
Sparrow	(126, 232, 2)	228	229	99.6342	33.832
	(56, 134, 3)	221	222	99.6322	33.422
	(2, 34, 1)	92	93	99.7341	33.051
Lena	(127, 253, 2)	109	110	99.6990	33.312
	(92, 130, 3)	120	121	99.5873	33.542

4.4.3 Entropy Evaluation

For proposed image, it is perfect for the image that textual information can be concealed completely when encryption is done, therefore it is difficult for opponents to perform attacks on it. The uncertainty or complexity of proposed images is measured via entropy indicator known as information entropy. For the complicated sequences, the entropy value is higher, and the chances of information leakage are less.

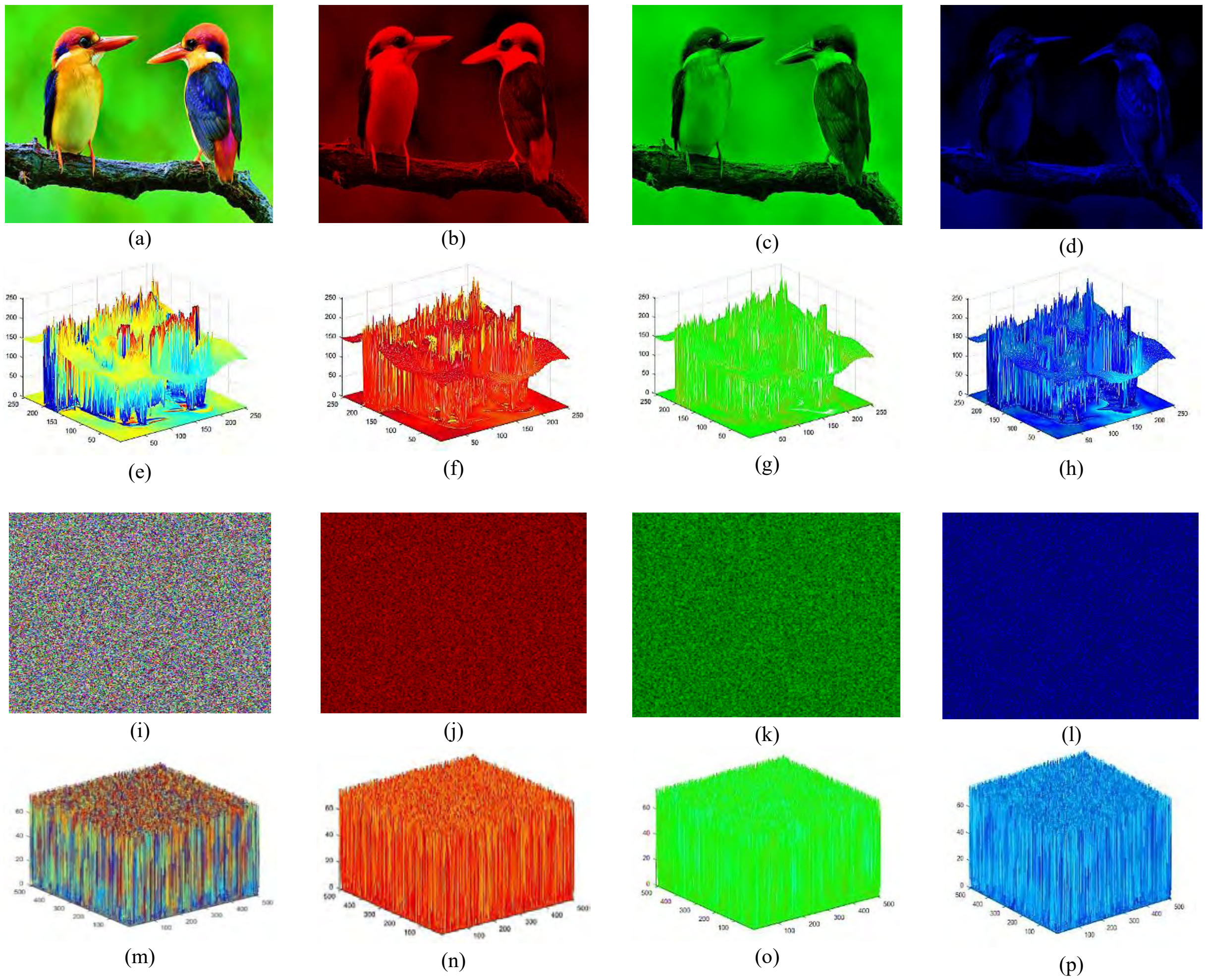
By the indication of entropy information, it is concluded that proposed scheme has strong resistance a large amount of randomness because the cipher images of Lena and Sparrow have theoretical entropy values near 8 as shown in Table 4.2.

Table 4.2: Entropy Analysis

Images		Lena			Sparrow	
Channels	**R**	**G**	**B**	**R**	**G**	**B**
Original	7.27620	7.58342	7.01628	7.4141	7.2998	6.4873
Encrypted	7.99921	7.99891	7.99933	7.99921	7.99921	7.9993

4.4.4 Intensity 3D Histogram Analysis

The digital images appearance is observed via image different layers intensity values of pixels. Image intensity values describes image information also it ensures the algorithm strength against any kind of attacks. Proposed "Lena" and "Sparrow" images each layered intensity histograms are given in Figure 4.10-4.11.



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

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

(i) (j) (k) (l)

(m) (n) (o) (p)

Figure 4.10: (a) Sparrow original Image (b) Sparrow Red layer (c) Sparrow Green layer (d) Sparrow Blue layer (e) Histogram Original Image (f) Histogram Red layer (g) Histogram Green layer (h) Histogram Blue layer (i) Encrypted Sparrow image (j) Encrypted Red image (k) Encrypted Green image (l) Blue encrypted image (m) Histogram of encrypted image (n) Histogram Red encrypted image (o) Encrypted Green image (p) Encrypted Blue image

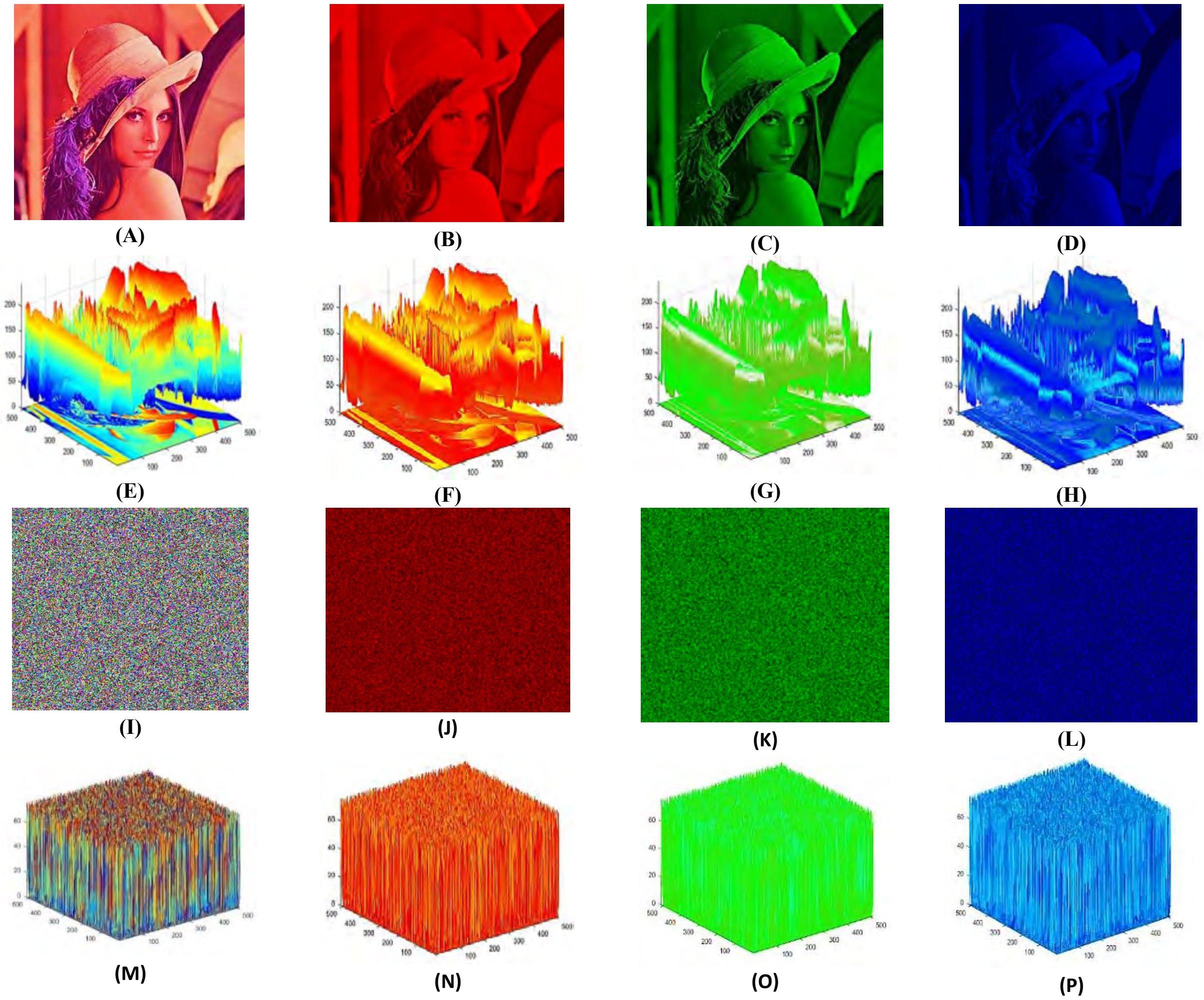


Figure 4.11: (A) Lena original Image (B) Lena Red layer (C) Lena Green layer (D) Lena Blue layer (E) Histogram Plain Lena Image (F) Histogram Red layer (G) Histogram Green layer (H) Histogram Blue layer (I) Encrypted Sparrow image (J) Encrypted Red image (K) Encrypted Green image (L) Blue encrypted image (M) Histogram of encrypted image (N) Histogram Red encrypted image (O) Encrypted Green image (P) Encrypted Blue image

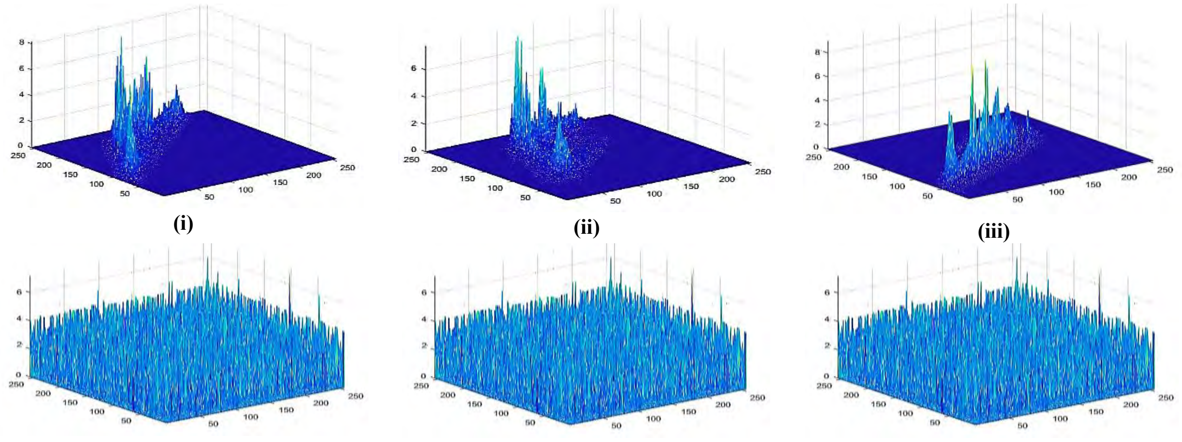
4.4.5 Analysis of Adjacent pixels Correlation and joint-distribution

To examine efficiency and security, the joint distribution and correlation among adjacent pixels analysis is done. All adjacent-pixel pairs along vertical (V), diagonal (D), and horizontal (H) directions for both original and ciphered images is computed by the formula explained in chapter 1 section 1.16.

The nearby pixels correlation coefficients in encrypted images are lower (near zero) in comparison with original images (near 1) and are displayed in Table 4.2. As experimental analysis image of Lena is taken, from Figure 4.12, it could be easily viewed that joint-distribution of original Lena adjacent pixels along three directions are near the coordinate plan diagonal. The original image experimental view shows that the pixels are highly correlated, while the results of ciphered image joint-distribution along three directions exhibit uniform behavior. So, it is concluded from analysis of figure and table that ciphered image nearby pixels correlation is reduced greatly for this reason any kind of statistical attack over proposed scheme is infeasible.

Table 4.2: Horizontal, Vertical, Diagonal Correlation

Images	Channels	Original (H)	Encrypted (H)	Original (V)	Encrypted (V)	Original (D)	Encrypted (D)
Lena	R (Red)	0.9764	0.00023	0.9276	0.00132	0.9654	0.0002
	G (Green)	0.9774	-0.00172	0.9367	-0.0051	0.9703	0.00007
	B (Blue)	0.9741	0.00010	0.9410	0.00076	0.9691	-0.000005
Sparrow	R (Red)	0.8689	-0.000043	0.9690	-0.0003	0.8766	0.000054
	G (Green)	0.8572	0.000102	0.9666	0.00005	0.8739	0.00201
	B (Blue)	0.8629	0.000006	0.9693	0.0000062	0.8815	-0.00073



(i) (ii) (iii)

(iv) (v) (vi)

Figure 4.12: (i) Original image Joint horizontal correlation (ii) Original image Joint Vertical correlation (iii) Original image Joint Diagonal correlation (iv) Encrypted image Joint horizontal correlation (v) Encrypted image Joint vertical correlation (vi) Encrypted image Joint Diagonal correlation

4.4.6 Structural Similarity

Index structural similarity (abbreviated as SSIM) measures plain and ciphered images similarity value. Idea for testing pixels inter-dependency is known as structural based information when there is graphically strong relationship between them. Any object structural information is carried in dependencies while seeing it visually. SSIM values lies between -1 and 1. It is computed by following formula:

$$SSIM(X,Y) = \frac{(2\varphi_X\varphi_Y + C_1)(2\mu_{XY} + C_2)}{({\varphi_X}^2 + {\varphi_Y}^2 + C_1)({\mu_X}^2 + {\mu_Y}^2 + C_2)}$$

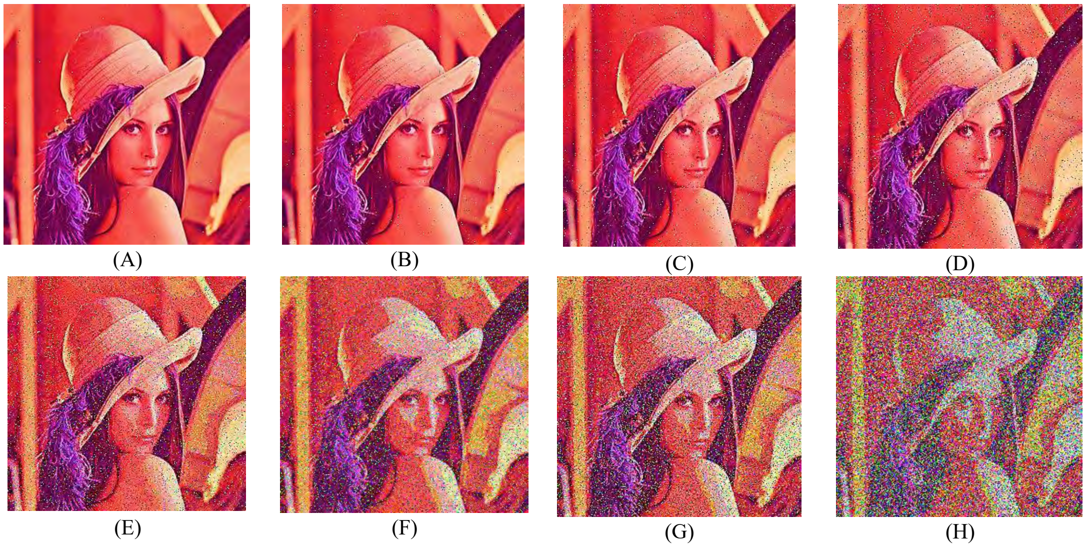
where, φ_X, φ_Y represent average values of X, Y, μ_X, μ_Y represent variances of X, Y , μ_{XY} is X, Y covariance, $C_1 = (K_1 l)^2, C_2 = (K_2 l)^2$ denoted variables having weak denominator for division stabilization, dynamical pixel values range is represented by l, the values for $(K_1, K_2) = (0.01,0.03)$. Proposed encrypted and plain image of “Lena”, SSIM and PSNR results are shown in Table 4.3 also its comparison is given. From results and comparison, it is seen that the encrypted images SSIM values are near zero , PSNR are less than $10\ dB, and\ MSE$ values are greater which indicates that the encrypted images by proposed scheme have low quality, so from encrypted images it is difficult to predict original plain images.

Table 4.3: Proposed Image SSIM, MSE, PSNR analysis and comparison

	Proposed			[134]		
	SSIM	**MSE**	**PSNR**	**SSIM**	**MSE**	**PSNR**
R	0.01002	10661.1	7.8218	0.0103	10630	7.8653
G	0.00952	9243.60	8.2727	0.0092	9155.2	8.5141
B	0.00936	7198.46	9.3821	0.0096	7196.8	9.5593

4.4.7 Against Noise Stability

Ciphered images usually can be affected by some noises during transmission. Cipher images attacked by noise are very hard to retrieve. Therefore, evaluated method for encryption must be resistant against noise. A better encryption scheme is presented so it could have resistance against noise attacks. The noise analysis of “Salt & pepper” having intensity values “0.001,0.005,0.02,0.2, and “Gaussian-white” noise attack having mean value “0” and variances “0.001,0.005,0.01,0.1” are added into ciphered images of “Lena” in presented analysis. The results are shown in Figure 4.13, which depicts that after adding noises, ciphered images of Lena are still identified. PSNR analysis is used to check the ciphered image quality when it is decrypted after adding noise. PSNR analysis between the original and decrypted “Lena” image is given in Table 4.4, decrypted images after adding noises are identified. Hence, proposed technique for encryption have strong resistance against the noise attacks.



(A) (B) (C) (D)

(E) (F) (G) (H)

Figure 4.13: Decrypted Lena with salt & pepper noise (A) 0.001 intensity (B) 0.005 intensity (C) 0.02 intensity (D) 0.2 intensity (E) Gaussian (0, 0.001) (F) Gaussian (0, 0.005) (G) Gaussian (0, 0.01) (H) Gaussian (0, 0.1)

Table 4.4: PSNR analysis for decrypted and original Lena image

Noise	Parameters	PSNR(DB)
Salt & pepper	0.001	38.7007
	0.005	31.5504
	0.02	28.1397
	0.2	19.8955
Guassian	0, 0.005	37.372
	0, 0.001	35.162
	0, 001	29.325
	0, 0.1	23.624

4.4.8 Occasional Attack

Mostly in transmitting data from one network to another, few data information is lost. For this, an attack analysis i.e., occasional is used for testing recovered plain-images capacity even small amount of data has gone occluded. In figure 4.14, random occlusion analysis is performed, which indicates that during transmission few amounts of information is lost in small part of image. The recovered or decrypted images are also shown in that figure, so one can easily see that the recovered images are still in readable format even if some data is lost.

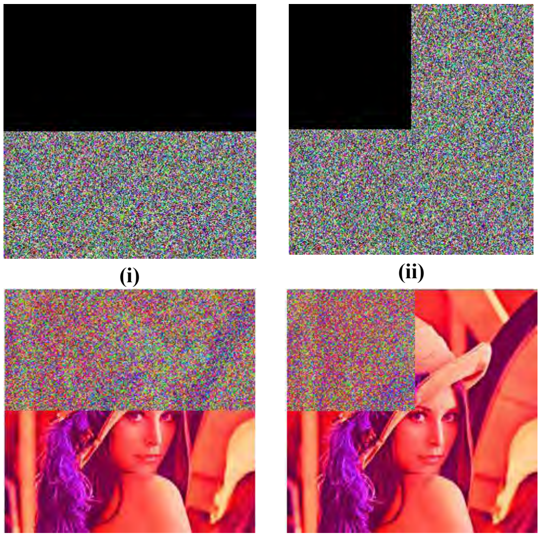


Figure 4.14 Occasional Attack analysis of Lena image

4.4.9 Chosen Plain-text Attack Analysis

Any attacker has clear idea about proposed work and methodology by its research. However, to comprehend secret keys is quiet tough task in comparison with basic variables realization of any cryptosystem. Mostly, attacker focuses on extraction of intermediate variables/parameters. In proposed work, the initial parameters of four-dimensional chaotic maps are correlated with plain image pixel values. So, in case of different images the parametric values are also changed, for each encryption. Hence, the proposed scheme is resistant against such type of attacks.

Chapter 5

Color Multiple Image Encryption Scheme Based on 3D-Chaotic Maps

In many research areas, production of images is increasing with every day. These days, the prime focus of researchers is on the security of digital images. Motivated by grey multiple image encryption algorithms, this chapter suggests a novel Chaos-based color multiple image encryption technique. A 3D histogram equalization method has been applied to equalize the chaotic sequences histograms of Lorenz system. Confusion/diffusion of image data have been implemented by using sequences generated by histogram equalized Lorenz and Rossler system. In confusion stage, the input image-colored pixels have been scrambled. Then in diffusion stage, pixel replacement is done by scrambled images and sequences of Rossler system. The proposed scheme efficiency is validated via key sensitivity, key space, entropy, horizontal, vertical, diagonal correlation, UACI and NPCR tests. Furthermore, the overall security analysis and experimental results shows that the proposed encryption technique have achieved confidentiality and have resistance against classical attacks.

5.1 Introduction

With the fast modification of civilization, need of the hour is to formulate strategies for preserving information. Presently, security of data is of prime importance. The use of electronic devices demands various cryptographic methods for their security. Currently, online dealings, online banking and alternate credit cards numbers play a vibrant role in our everyday life. Therefore, to resolve security issues, cryptography plays a substantial role for hiding data into an unreadable format. Recently, only security of data is not important but also the image security issue is of great importance. As, by the vast developments many military forces kept their secret information related to their country in images. Image's confidentiality and copywriting have a great impact on everybody ease [104]. To solve the security problem of images many authors have proposed single image-based encryption techniques using chaotic maps.

Q. Yin et al. [105] offered a single-image encryption technique based on Breadth-First Search along with diffusion of dynamics. Permutation stage is done via applying Breadth-First Search and diffusion by dynamic-diffusion algorithm. For the improvement of images security, H. Liu et al.

[106] suggested a technique for color image encryption. In this technique, one-time keys along with chaotic maps are used. Meanwhile, an encryption scheme using DNA sequences along with chaotic maps is proposed by X.Y. Wang [107]. Beside the simple chaotic systems some authors introduced hyperchaotic chaotic maps, image encryption schemes. For example, [108] M. Zhou et al. offered a hyperchaotic based encryption scheme in such a way that for changing pixels in blocks process, closed loop diffusion is used. Utilized hyperchaotic map and diffusion-permutation algorithm, RGB (Red, Green, Blue) image-based encryption algorithm is proposed by G. Cheng et al. [109]. Some new work has been done on multiplex networks, such as: X. Wang et al. investigated a semi tensor matrix product theory application and Boolean system based encryption technique [110]. Also, X. Wang et al. examined some coupled logistic map lattices as key generators for diffusion and permutation for encryption process [111]. [112] X.Y. Wang et al. described encryption process based on Hope-field neural chaotic networks. Several chaos theory-based encryption techniques using different methodologies were proposed by many authors in recent years see [113,114]. But these are encryption techniques of single-images in which the features of giant images are not used completely.

In current era, encryption techniques of multiple images are a prime focus for the security of multimedia experts. Many multiple optical images techniques are pointed out by many authors [115]. Multiple image encryption (MIE) techniques involving asymmetric cryptosystems [116], Fourier domain [117], Fourier transform [118] and wavelet lifting transform [119]. But according to encryption of digital images these optical designed image features are not appropriate. So, for the security and protection of digital images these authors also pay attention on MIE techniques for digital images. In [120], X. Li et al. presented a MIE technique using transform domains of wavelet. But its decrypted image has low plain image coefficients' distribution.[121] X. Zhang et al. proposed a securable technique of MIE by using operations of DNA which is quiet bit complex due to encoding/decoding of DNA operations. After detail analysis of breaking methods, the drawbacks of image encryption algorithms are concluded as follows:

1) In single-image encryption techniques all the features of massive images are not completely utilized.

2) In MIE techniques, some are only designed for optical images, have low plain image coefficients distribution in decrypted images. The objectives of proposed scheme are to overcome the limitations and draw backs of above encrypted schemes.

Since every pixel of color image is divided into three planes i.e., R, G, B. In the comparison with grey images, RGB carries more information and appeal much attention. Motivated by above mentioned MIE schemes for grey images, this paper proposed a novel multiple color image encryption technique based on simple 3D chaotic Lorenz and Rossler system. Firstly, to improve security histogram equalization method is applied on non-uniform histograms of Lorenz chaotic sequences to make them uniform. The sequences generated by this technique are then used for scrambling the pixels of RGB image which ensures the reliability and randomness of proposed scheme. Secondly, the most important part of proposed scheme is the replacement of pixels after scrambling to make it more resistant against the classical attacks and attain good results. For this, chaotic sequences generated by Rossler Chaotic system are used. Both the systems (i.e., Lorenz and Rossler) are not only used for increment of key sensitivity or key space but it also creates high randomness in image pixels. Higher key space value can enhance the resistance against attacks of brute-force and information leakage amount is reduced by increased randomness. Also, Simulation and comparison results depicts the supremacy and high proficiency of presented encryption technique.

5.2 Proposed Image Cryptosystem

In this section, we presented a complete detailed novel technique of proposed cryptosystem based on 3D chaotic maps. The overall encryption scheme depends on following steps:

A. 3D Lorenz Chaotic system generation
B. Chaotic Lorenz system Histogram Equalization
C. Scrambling
D. 3D Rossler chaotic system generation
E. Diffusion Stage

A. 3D Lorenz Chaotic System Generation

In 1960, Edward Lorenz firstly offered the Lorenz Chaotic system. The system of non-linear ordinary differential of this dynamical system is given as follows [122]:

$$\frac{dX}{dt} = a(Y - X),$$

$$\frac{dY}{dt} = (\sigma - Z)X - Y,$$

$$\frac{dZ}{dt} = XY - bZ,$$

where the control parameters of above system of non-linear equations are σ, a, b and the variable X, Y, Z are known as state variables and t is time. These equations exhibit chaotic behavior at $a = 10, \sigma = \frac{8}{3}, b = 28.$ With the help of numerical Runge-Kutta method, initial state variables X_0, Y_0, Z_0 and given control parameters a, b, σ of whole system are solved. The two-dimensional (2D) and three-dimensional (3D) chaotic attractors of this dynamical system are shown in Figure 5.1. The chaotic behavior of Lorenz sequences is shown in Figure 5.2.

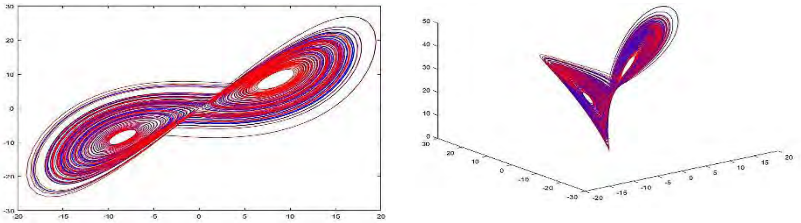


Figure 5.1: 2D and 3D chaotic attractors of Lorenz Chaotic

B. Chaotic Lorenz System Histogram Equalization:

It should be clear from figure 5.3, that the histogram of X, Y, Z has non-uniform distribution. For the improvement of security level, the equalization of histogram should be done. So, the equalization should be done by following steps:

- Take a color multiple images of dimensions $M \times N \times 3$, where M denotes number of image rows and N are the number of image columns.
- Equalize the histogram by following formula:

$$X = \left(ceil(X \times P1)\right) mod\ M, \tag{1}$$

$$Y = \left(ceil(Y \times P2)\right) mod\ N, \tag{2}$$

$$Z = \left(ceil(Z \times P3)\right) mod\ \ 256, \tag{3}$$

where, $P1, P2, P3$ are random numbers generally greater than 10000. But here in our case we use $P1 = P2 = P3 = 150000.$

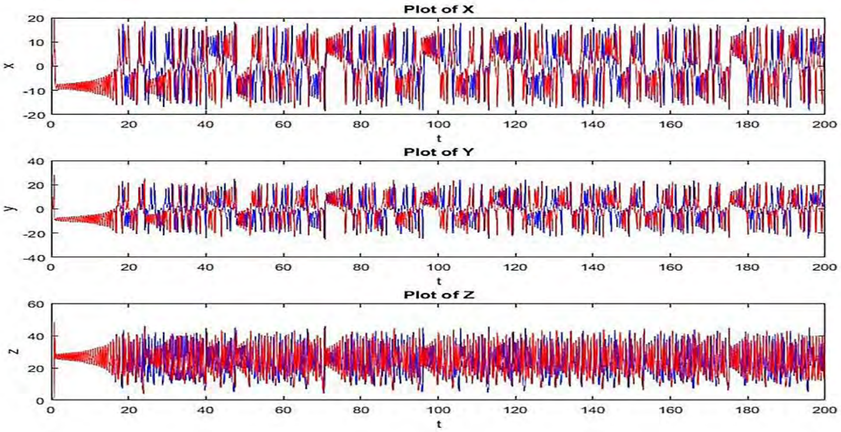


Figure 5.2: Chaotic behavior of Lorenz chaotic system X, Y, Z sequences

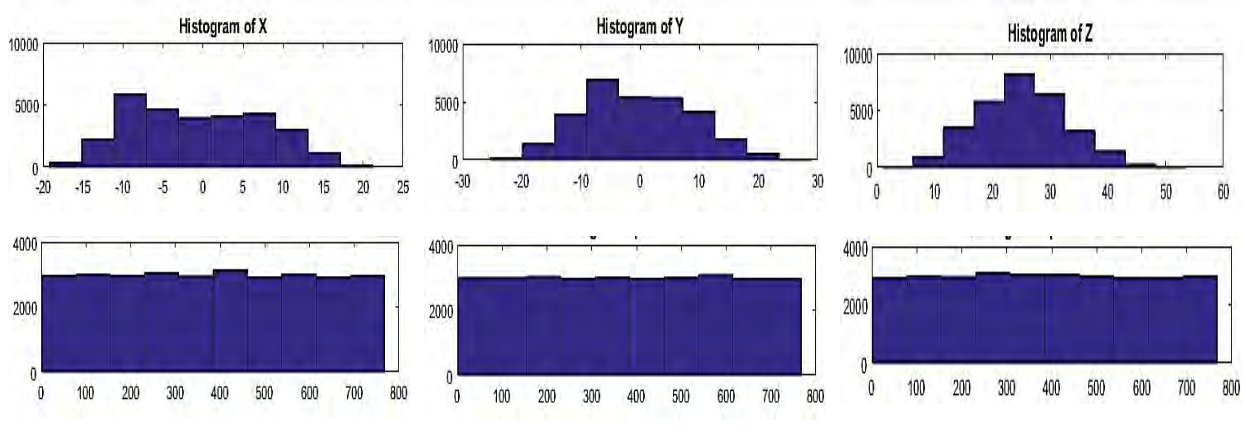


Figure 5.3: Histograms and Equalized Histograms of sequences X, Y, Z

C. Scrambling

Scrambling is basically the rearrangement of pixels position. In this work, for the reduction of adjust pixels correlation the histogram equalized Lorenz chaotic sequences are used as keys.

Step 1: Convert the original image $I(m, n, 3)$ into $R(m, n), G(m, n), B(m, n)$ channels.

Step2:Generate three keys $X = \{x_1, x_2, x_3, \dots \dots x_k\}$; $Y = \{y_1, y_2, y_3, \dots \dots y_k\}$ and$Z = \{z_1, z_2, z_3, \dots \dots z_k\}$, using equations obtained in section (A) where $k = M \times N$.

Step 3: Prepare the chaotic sequences X, Y, Z as:

$$[X1, f_x\ ] = sort(X),$$

$$[Y1, f_y\ ] = sort(Y),$$

$$[Z1, f_z\ ] = sort(Z),$$

where $[\star,\star] = sort(\star)$ indicates index sequencing function, f_x, f_y, f_z are squences obtained after ascending to $X1, Y1, Z1$ and $X1, Y1, Z1$ are the f_x, f_y, f_z index values.

Step 4: Now to scramble three channels i.e. R, G, B, combination of $(X1, Y1, Z1)$ are selected. By using following equation scrambling is done:

$$R(i,j) \leftrightarrow R(X1(i), Y1(j)),$$

$$G(i,j) \leftrightarrow G(Y1(i), Z1(j)),$$

$$B(i,j) \leftrightarrow B(Z1(i), X1(j)),$$

where $i = 1,2,3, \ldots .m, j = 1,2,3, \ldots .n$ and $R(i,j), G(i,j), B(i,j)$ represents the values of pixels (i,j) from three channels R,G,B.

D. Rossler Chaotic System:

Rossler is one of continuous chaotic system. The chaotic behavior of Rossler is generated by following ordinary differential equations:

$$\frac{dp}{dt} = -(q + r),$$

$$\frac{dq}{dt} = p + \alpha * q,$$

$$\frac{dr}{dt} = \beta + r(p - \gamma),$$

where α, β, γ are parameters having chaotic behavior at $\alpha = \beta = 0.2, \gamma = 5.7$ [123]. The 3D chaotic attractor of Rossler dynamical system is shown in figure 5.4:

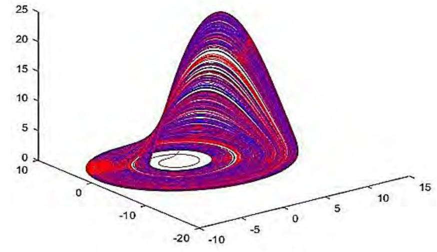


Figure 5.4: 3D chaotic attractors of Rossler Chaotic map

E. Diffusion Stage

In this stage of encryption exclusive OR operation is used**.** The main contribution of OR operation is that it completely change the pixels values with new ones and if the chaotic key is not known, reversible steps are not possible. Iterate the sequences p, q, r obtained in section (D) L times and after each iteration the initial values of p, q, r are changed. New initial values for p, q, r are calculated as:

$$p_0{}' = p_L \oplus p_{L-1} \oplus p_{L-2},$$

$$q_0{}' = q_L \oplus q_{L-1} \oplus q_{L-2},$$

$$r_0{}' = r_L \oplus r_{L-1} \oplus r_{L-2},$$

where, $p_0{}', q_0{}', r_0{}'$ are the new initial values, p_L, p_{L-1}, p_{L-2}, q_L, $q_{L-1}, q_{L-2}, r_L, r_{L-1}, r_{L-2}$ are the outputs after $L, L-1, L-2$ iterations.

Now restrict values of chaotic sequences $p(i,j), q(i,j), r(i,j)$ between 0-255 by using following formulas:

$$p(i,j) = (mod(p(i,j) \times 10^{15}), 256),$$
$$q(i,j) = (mod(q(i,j) \times 10^{15}), 256),$$
$$r(i,j) = (mod(r(i,j) \times 10^{15}), 256),$$

Generate new chaotic sequence $T(i,j)$ by using chaotic keys as:

$$T(i,j) = p(i,j) \oplus q(i,j) \oplus r(i,j),$$

Apply bitwise Xor operation between the pixels of plain and scrambled images attained in section (C) then pixels of new imge $E'(i,j)$ are replaced by the sequence $T(i,j)$ as follows:

$$E'(i,j) = I(i,j) \oplus I'(i,j),$$

$$E(i,j) = T(i,j) \ \oplus E'(i,j),$$

Where I , I' are original plain and scrambled images and $\oplus$ is indication of bitwise Exclusive OR operation.

5.2.1 Pseudo code for Proposed Encryption Technique

Input: Original plain Image **(I)** of size $m \times n \times 3$.

Output: Encrypted Image **(E)** of size $m \times n \times 3$.

```
 1. $I \rightarrow R, G, B$ (Split color plain image (I) to red (R), green (G), blue (B) channels of size $m \times n$)
 2. Generate three chaotic sequences of $mn$ size using 3D Lorenz chaotic map given below
 3. $x_{i+1} = a * (y_i - x_i); y_{i+1} = (\sigma - z_i) * x_i - y_i;\ z_{i+1} = x_i * y_i - b * z_i;$
    with $a = 10, \sigma = \frac{8}{3}, b = 28, x_0 = 1.10, y_0 = 1.30, z_0 = 1.50, i = \{1,2,3,4, \dots \dots mn\}$
    % Equalize the histograms of Lorenz sequences
 4. $x = mod((ceil(x * P1), m),\ y = mod((ceil(y * P2), n), z = mod((ceil(z * P3), 256),$
    with $P1 = P2 = P3 = 150000.$
    %Prepare chaotic sequences
 5. $[X1, f_x\ ] = sort(X)$; where $X1 = X_{f_x}$;
 6. $[Y1, f_y\ ] = sort(Y)$; where $Y1 = Y_{f_y}$;
 7. $[Z1, f_z\ ] = sort(Z)$; where $Z1 = Z_{f_z}$;
    % Scramble image three channels via $(X1, Y1, Z1)$ combinations
 8. For $i = 1,2,3, \dots . m, j = 1,2,3, \dots . n$
 9. $R(i,j) \leftrightarrow R(X1(i), Y1(j))$, %Red channel pixels scrambling
10. $G(i,j) \leftrightarrow G(Y1(i), Z1(j))$, %Green channel pixels scrambling
11. $B(i,j) \leftrightarrow B(Z1(i), X1(j))$, %Blue channel pixels scrambling
12. $I'(i,j) = cat(3, R, G, B)$; % Scrambled image
13. Generate three chaotic sequences of $mn$ size using 3D Rossler's chaotic map by using equations given in step 14,15,16.
14. $p_{i+1} = -(q_i + r_i)\ ;\ q_{i+1} = p_i + \alpha * q_i\ ;\ r_{i+1} = \beta + r * (p - \gamma),$
    with $\alpha = \beta = 0.2, \gamma = 5.7, p_0 = 1, q_0 = 1, r_0 = 1, i = \{1,2, \dots \dots, mn\}$
15. $L(i,j) = (mod(L(i,j) \times 10^{15}), 256)$, %Restrict sequence of values $p.q.r$ between (0-255), where $L = p, q, r$
16. $T'(i,j) = bitxor(p(i,j), q(i,j))$ %Generate new sequence
17. $T(i,j) = bitxor(T'^{(i,j)}, r(i,j))$ %Generate new sequence
%Diffusion process using exclusive OR operation
```

18. $E'(i,j) = bitxor(I(i,j), I'(i,j))$ %Xor operation between plain image and Scrambled image pixels.
19. $E(i,j) = bitxor(T(i,j), E'(i,j))$ % Replacement of image obtained in step 21 by sequence T obtained in step 20.
20. Encrypted image E of size $m \times n \times 3$.
21. End.

5.2.2 Algorithm of Encryption Process

The proposed encryption algorithm flow chart is given in Fig 5.5.

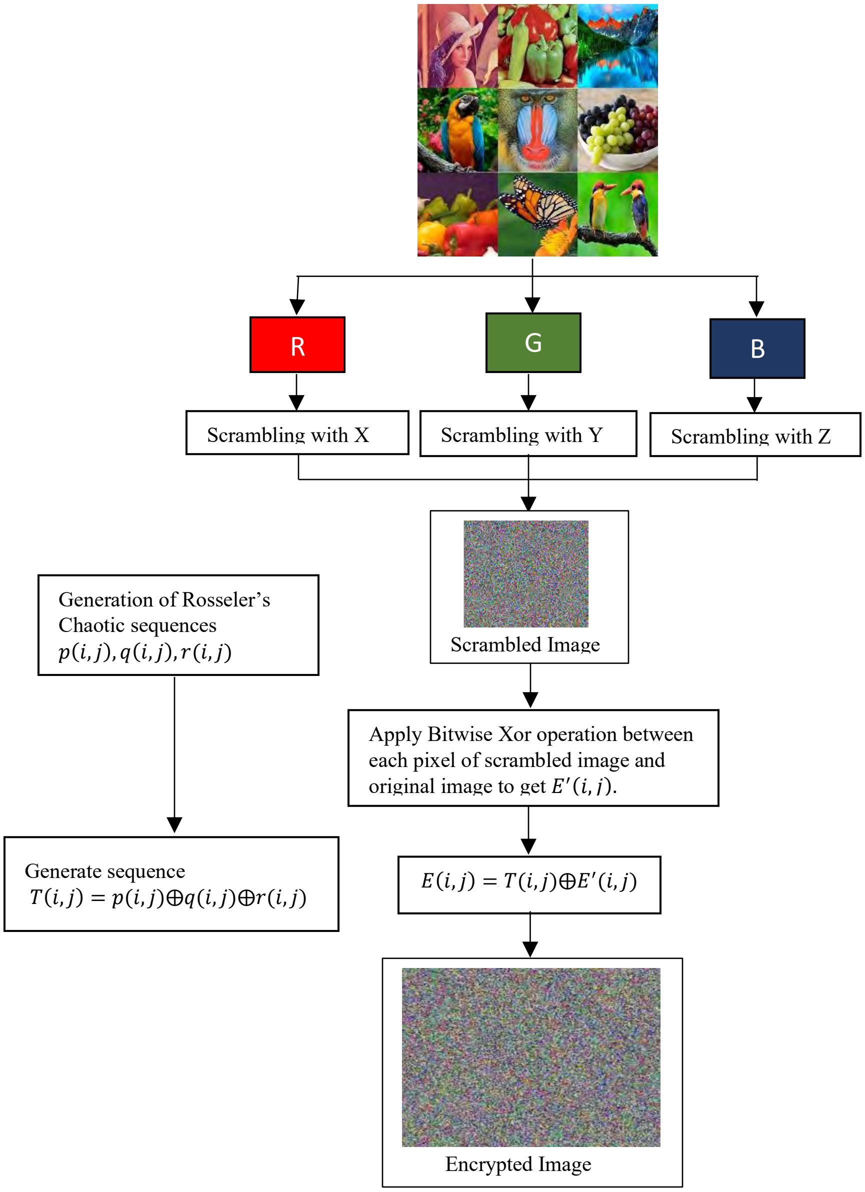

R
G
B
Scrambling with X
Scrambling with Y
Scrambling with Z
Scrambled Image
Generation of Rosseler's Chaotic sequences $p(i,j), q(i,j), r(i,j)$
Apply Bitwise Xor operation between each pixel of scrambled image and original image to get $E'(i,j)$.
Generate sequence $T(i,j) = p(i,j) \oplus q(i,j) \oplus r(i,j)$
$E(i,j) = T(i,j) \oplus E'(i,j)$
Encrypted Image

Figure 5.5: Flow chart for Encryption Process

Decryption scheme is reverse of proposed encryption scheme. The Combine multiple images encryption and decryption is shown in figure 5.6. From the proposed diagram it is easily seen that no relationship is shown between encrypted and original image, but the decrypted image completely looks like original image. The figure 5.7(A-B), shows the original and encrypted diagrams of Lena, Peppers, Nature, Bird, Baboon, Grapes, Deblur, Butterfly, Sparrows. The proposed image encryption algorithm presented in the figure 5.6 and figure 5.7, depicts that it has excellent encryption as well as decryption effects.

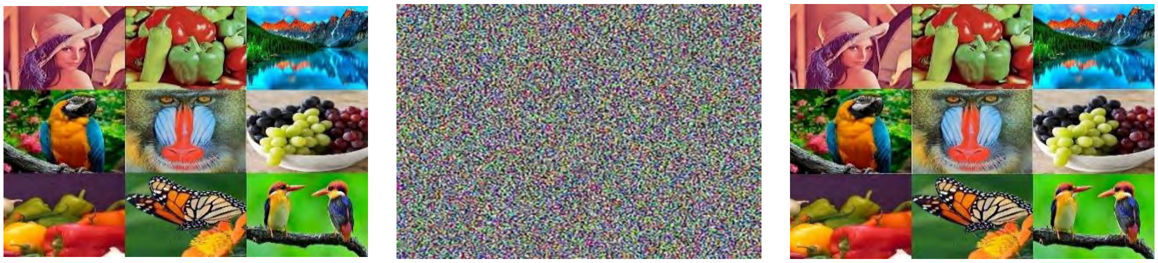
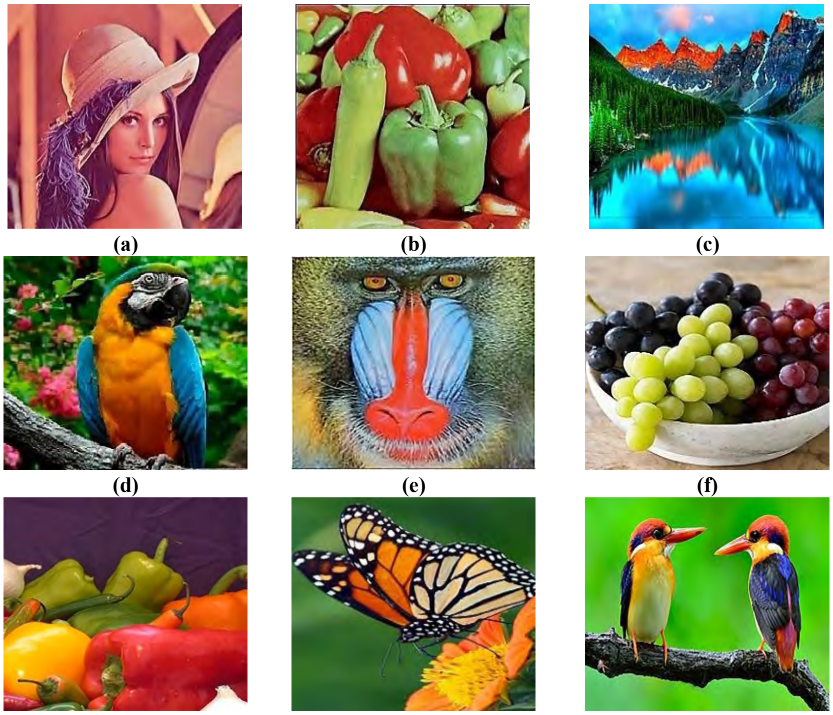


Figure 5.6: (a)Combine Original image **(b)Combine Encrypted image** **(c)Combine decrypted image**



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

(d) **(e)** **(f)**

(g) **(h)** **(i)**

Figure 5.7 (A): Experimental Analysis results: (a) plain Lena image (b) plain Pepper's image (c) plain Nature image (d) plain Bird image (e) plain Baboon image (f) plain Grape's image (g) plain Deblur image (h) plain Butterfly image (i) plain Sparrows image

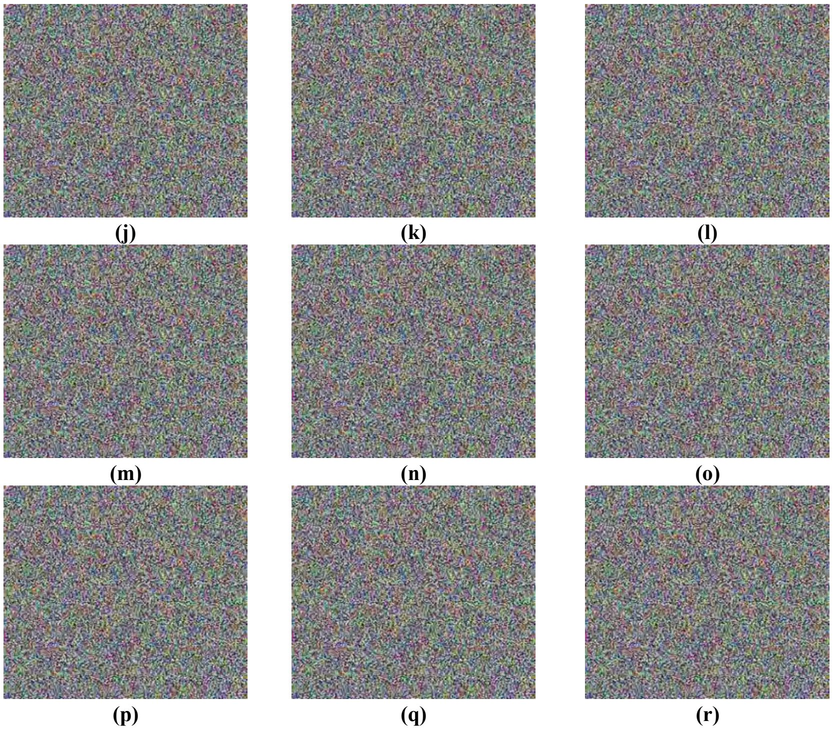


Figure 5.7 (B): Experimental Analysis results (j) encrypted Lena image (k) encrypted Pepper's image (l) encrypted Nature image (m) encrypted Bird image (n) encrypted Baboon image (o) encrypted Grape's image (p) encrypted Deblur image (q) encrypted Butterfly image (r) encrypted Sparrows image

5.3 Simulation Analysis and Results

In our proposed work, standard $256 \times 256 \times 3$ color images of "Lena", "Peppers", "Nature", "Bird", "Baboon", "Grapes ", "Deblur", "Butterfly", "Sparrows" are used as input plain-images as shown in 5.7(A) (a)-(i), and combined multiple images is given in Fig 5.6(a). For implementation of encryption/decryption process the simulation is done in MATLAB 9.1.0.441655 (R2016b) by setting initial values and parameters as: $x_0 = 1.10, y_0 = 1.30,\ z_0 = 1.50, p_0 = 1, q_0 = 1, r_0 = 1, \alpha = \beta = 0.2, \gamma = 5.7, a = 10, \sigma = \frac{8}{3} and\ b = 28.$ Let $\rho_o = \{x_0, y_0, z_0, p_0, q_0, r_0\ , \alpha, \gamma, a, b, \sigma\}$ denote the set of secret keys. And the encrypted of combine and splitted images are given in fig 5.6(b),5.7(B) (j)-(r). The decrypted combined image is also shown in fig 5.6(c). As it is easily seen from the original and encrypted images of fig 5.6 and fig 5.7(A-B) that no relationship is found between them.

5.4 Security Analysis

To check the robustness of any proposed encryption algorithm, security analysis plays very important role. A strong encryption algorithm has ability to resist against any kind of attacks i.e., Brute force attack, Statistical attacks, Differential attacks and so on. In this section, a detail security of proposed encryption algorithm is presented.

5.4.1 Key Space Analysis

Robustness of any cryptographic system is highly dependent on its key space. A greater key space of any cryptosystem provides a great security against any brute force attack. In presented technique, the secret key includes eleven parameters $x_0, y_0, z_0, p_0, q_0, r_0, \alpha, \gamma, a, b, and\ \sigma.$ Our proposed encryption scheme has computational accuracy 10^{15}. As a result the total secret keys of proposed algorithm are approximately $(10^{15})^{11} = 10^{165}$. The proposed encryption scheme and other encryption schemes comparison is provided in Table 5.1, which depicts that the proposed encryption technique has large key space to resist any attack of brute forces.

Table 5.1: Key space Analysis of Proposed algorithm and its comparison

Algorithm	**Key space**
Proposed	10^{165}
[124]	10^{84}
[125]	10^{70}
[126]	$> 10^{96}$

5.4.2 Key sensitivity analysis

For every cryptosystem key plays a very important. The security of the algorithm is ensured by its key. To examine the robustness of algorithm, key sensitivity analysis is very important and against any attack of brute-force it ensures the security of cryptosystem [127]. A cryptosystem having high key sensitivity proposed that if an attacker used slightly different keys for the encryption of similar plain images both ciphered images are completely independent from one another. For the assessment of key sensitivity, the first encryption round is performed by using the key set ρ_o of initial values. Now we performed encryption eleven times by slightly changing any one parameter of secret key set ρ_o while the others remain unchanged.

Sensitivity test of key x_0:Firstly, the initial set key ρ_o to encrypt original colored Lena image of size 256x256 shown in Fig 5. 8 (a), is used in proposed scheme. The result of encrypted image by using initial set key ρ_o is shown in figure 5.8 (b). For example, now we applied a small change in secret key x_0 i.e., $x_0 = x_0 + 10^{-15}$ and the other remains unchanged. Another secret key set say ρ_1, is generated. Now we use ρ_1 to same plain image encryption, another cipher image is obtained as shown in Fig 5.8 (c). The difference of pixels is shown in Fig 5.8 (d). The rate of difference between fig 5.8 (b) and fig 5.8 (c) is 99.6231%. It shows that a small modification in secret key set results in a remarkable change in ciphered image. Also, ρ_o and ρ_1 are used for the decryption of encrypted images in fig 5.8 (b) and fig 5.8 (c). The correct key sets are applied on fig 5.8 (b) and fig 5.8 (c) for the decryption of encrypted images, their results are presented in fig 5.8 (e) and fig 5.8 (h). Now it is easily seen form figure 5.8 (f) and (g) that by using a slight changed secret key for decryption of image will give the same encrypted images. It depicts that the encrypted images are not correctly decrypted by slightly changed keys. Therefore, it indicates that the cryptosystem proposed in this technique is highly sensitive to the secret key x_1 in both the process of encryption and decryption.

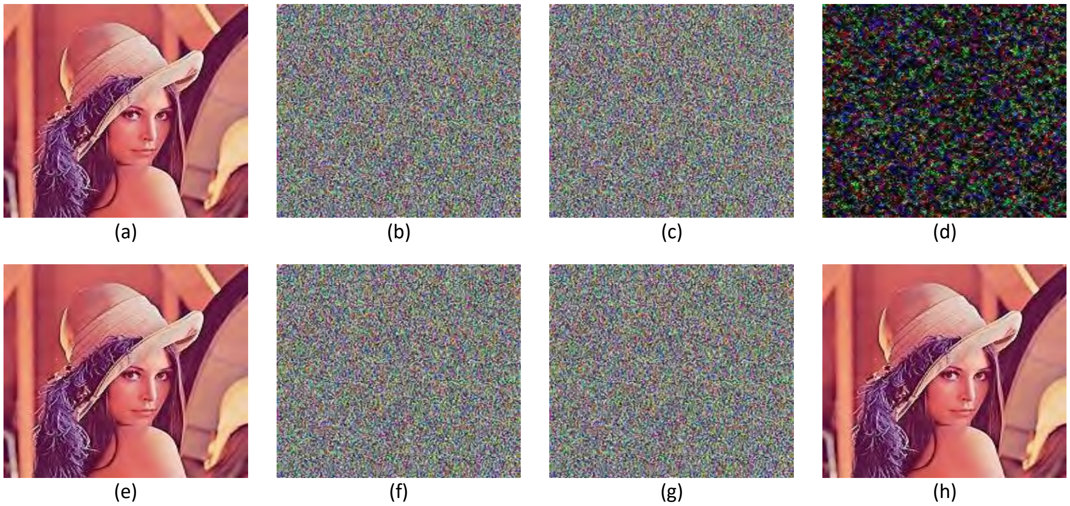


Figure 5.8: Key Sensitivity analysis x_0: (a) Original image of Lena (b) Encrypted image using original keyset ρ_o (c) Encrypted image using ρ_1 (d) pixel by pixel difference b/w (b) and (c) (e) decrypted image(b) using correct key set ρ_o (f) decrypted image (b) using wrong key set ρ_1(g) decrypted image (c) using wrong key ρ_o (h) decrypted image (c) using key ρ_1.

Sensitivity test of key p_0: For the sensitivity analysis of p_0, the initial set key ρ_o to encrypt original Pepper's image of size 256x256 shown in Fig 5.9 (a), is used. The result of encrypted image by using initial set key ρ_o is shown in fig 5.9 (b). Now we applied a small change in secret key p_0 i.e., $p_0 = p_0 - 10^{-15}$ and let the others unchanged. It generates another secret set key say ρ_1. Now we use ρ_1 to encrypt the same plain image, we get another cipher image shown in fig 5.9(c). The difference of pixels is shown in fig 9(d). The rate of difference between fig 5.9(b) and fig 5.9(c) is 99.5788%. It shows that a small change in secret key results in a remarkable change in ciphered image. Also, ρ_o and ρ_1 are used for the decryption of encrypted images in fig 5.9(b) and fig 5.9(c). The correct keys are applied on fig 5.9(b) and fig 9(c) for the decryption of encrypted images, their results are presented in fig 5.9(e) and fig 5.9(h). Now it is easily seen form figure 5.9(f) and 5.9(g) that by using a slight changed secret key for decryption of image will give the same encrypted images. It depicts that the encrypted images are not correctly decrypted by slightly changed keys. Therefore, it indicates that the cryptosystem proposed in this technique is highly sensitive to the secret key in both the process of encryption and decryption.

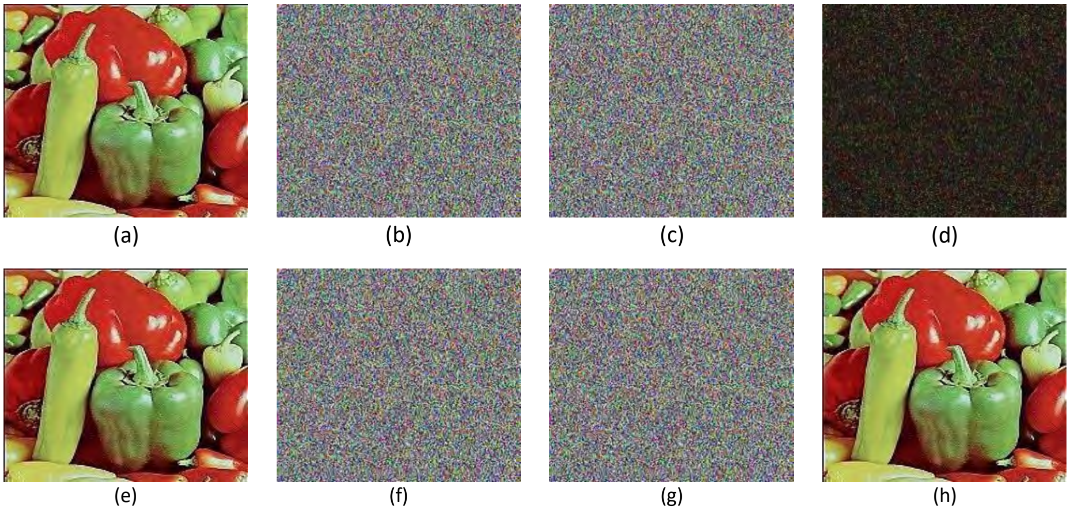


Figure 5.9: Key Sensitivity analysis p_0: (a) Original image of peppers (b) Encrypted image using original key ρ_o(c) Encrypted image using ρ_1 (d) pixel by pixel difference b/w (b) and (c) (e) decrypted image(b) using correct set of key ρ_o (f) decrypted image (b) using wrong key ρ_1(g) decrypted image (c) using wrong key ρ_o (h) decrypted image (c) using key ρ_1.

The complete sensitivity analysis results of all secret keys are not presented due to paper length limitation. But the rate of differences of two encrypted images by using set of initial keys ρ_o and slightly changed secret key set $\rho_i, i = (1,2,3, \dots .11)$ are shown in Table5. 2. It is easily seen from the difference rates between two encrypted images presented in Table 5.2, is greater than 99.56% which proves that a small change in key will give a remarkable change in decrypted images. So, from the results it is concluded that the proposed encryption algorithm is highly sensitive to all secret keys.

Table 5.2: Two encrypted images difference rates by slightly altered keys

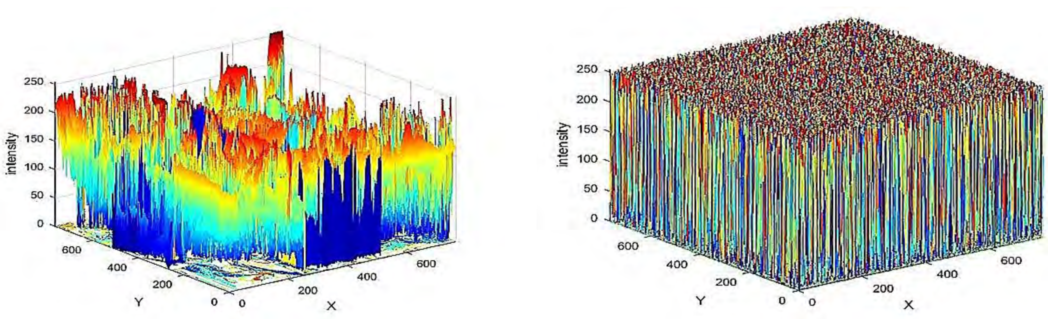
Secret Keys	Difference Rates%								
	Lena	**Peppers**	**Nature**	**Bird**	**Baboon**	**Grapes**	**Deblur**	**Butterfly**	**Sparrow**
$\boldsymbol{\rho_1(x_1 = x_0 + 10^{-15})}$	99.6122	99.6600	99.5714	99.6351	99.5983	99.5821	99.6345	99.6014	99.6608
$\boldsymbol{\rho_2(y_1 = y_0 + 10^{-15}}$	99.6676	99.6516	99.6127	99.5969	99.5992	99.5992	99.5992	99.5834	99.6286
$\boldsymbol{\rho_3(z_1 = z_0 - 10^{-15})}$	99.6741	99.6340	99.5932	99.5821	99.6054	99.6612	99.5823	99.5926	99.5988
$\boldsymbol{\rho_4\ (p_1 = p_0 - 10^{-15})}$	99.6001	99.6060	99.6016	99.6104	99.6255	99.6566	99.5981	99.6320	99.6012
$\boldsymbol{\rho_5(q_1 = q_0 + 10^{-15})}$	99.6352	99.6500	99.6512	99.6256	99.5889	99.5788	99.6008	99.6607	99.6543
$\boldsymbol{\rho_6(r_1 = r_0 + 10^{-15})}$	99.6200	99.6690	99.6603	99.6652	99.6024	99.6612	99.6223	99.6667	99.5990
$\boldsymbol{\rho_7(\alpha_1 = \alpha_0 + 1)}$	99.5990	99.6312	99.6712	99.6890	99.6600	99.6123	99.6200	99.5992	99.6556
$\boldsymbol{\rho_8(\gamma_1 = \gamma_0 - 1)}$	99.5775	99.5992	99.5982	99.5728	99.5892	99.6032	99.6143	99.6623	99.6012
$\boldsymbol{\rho_9(a_1 = a_0 + 1)}$	99.5908	99.6699	99.6012	99.6347	99.5977	99.5878	99.6228	99.6566	99.6542
$\boldsymbol{\rho_{10}(b_1 = b_0 - 1)}$	99.6286	99.6592	99.6432	99.6687	99.6652	99.6543	99.6500	99.6032	99.6635
$\boldsymbol{\rho_{11}(c_1 = c_0 + 1)}$	99.5884	99.6001	99.5881	99.5799	99.6311	99.5590	99.5810	99.5897	99.6066

5.5 Statistical analysis

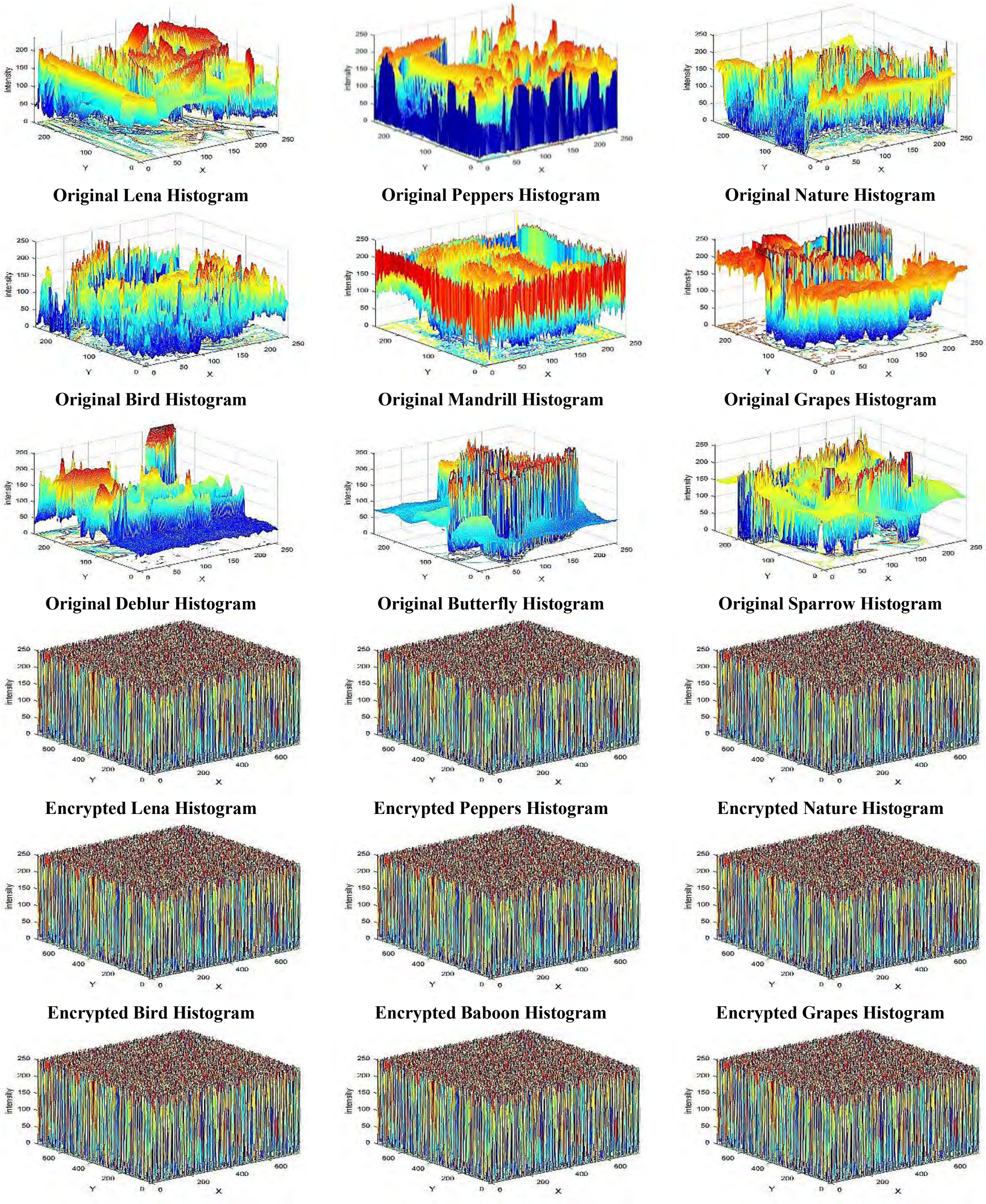
In this section the statistical and Texture analysis of proposed technique is presented which includes, Histogram analysis, Correlation, entropy, Contrast, homogeneity, Energy.

5.5.1 Histogram Analysis

The image encryption process is examined by histogram analysis. Histogram analysis is used to check the dispersion of pixel values in given image. A strong image encryption scheme has balanced histograms of encrypted images. The 3D Histogram of combined plain and encrypted image is shown in Fig 5.10. Also, the 3D histogram of separated plain and encrypted images i.e., Lena, Peppers, Nature, Bird, Baboon, Grapes, Deblur, Butterfly and Sparrow are shown in Fig 5.11. All the figures shown that the 3D histograms of encrypted images are very uniform and completely distinct from plain image histograms. The comparison of plain and encrypted image histogram presented that the given encrypted scheme has powerful resistance against algebraic attack and reveals no important information.



Figures 5.10: 3D Histogram representation of Original and Encrypted Multiple



Original Lena Histogram

Original Peppers Histogram

Original Nature Histogram

Original Bird Histogram

Original Mandrill Histogram

Original Grapes Histogram

Original Deblur Histogram

Original Butterfly Histogram

Original Sparrow Histogram

Encrypted Lena Histogram

Encrypted Peppers Histogram

Encrypted Nature Histogram

Encrypted Bird Histogram

Encrypted Baboon Histogram

Encrypted Grapes Histogram

Encrypted Deblur Histogram

Encrypted Butterfly Histogram

Encrypted Sparrow Histogram

Figures 5.11: 3D Histogram representation of Original and Encrypted

5.5.2 Histogram Variance Analysis

The variance histogram analysis is defined as [128]:

$$Var(V) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(v_i - v_j)^2,$$

where V represents the histogram values vector and $V = \{v_1, v_2, v_3 \ldots\ldots.. v_{256}\}$, and v_i, v_j are pixels numbers having equal i and j values.

To analyze each key quantity value, we perform histogram variance analysis to check the encrypted images uniformity. The lower variance value is the indication of highly uniformed encrypted images. Two closer variance values of ciphered images obtained by varying secret key set for same original image shows that the ciphered image histograms and more uniformed. In Table 5.3, histogram variance values of different encrypted images are given. The variance values of first row in Table 5.3, are computed by the initial set key ρ_o, while the remaining row values are obtained by slightly modifying any one of secret key $\rho_i(i = 1,2,3 \ldots 11)$ given in section 5.3.1.2, respectively. From Table 3, it is easily seen that the histogram variances values of encrypted images are about 255.28. However, the plain image variances are about 58115. 597.The proposed scheme has less variance values as compared to [129-130]. Furthermore, the modification of secret keys impact on the uniformity of cipher images is also investigated. To investigate it, we calculate the percentage of the two cipher images variance differences. First encrypted image is obtained by using the initial key set ρ_o and other one is by using the key set $\rho_i(i = 1,2,3 \ldots 11)$. The results of proposed scheme are given in Table 5.4. From the values of Table 5.4, it can be easily seen that the average value of percentage of histogram variances of two cipher images is 3.433% which shows better result in comparison with [130]. The amplitude fluctuation of proposed scheme has maximum variance value 9.172% which is smaller than [130]. So, proposed encryption scheme is quite efficient.

Table 5.3: Histogram variance analysis of encrypted images by slightly changing secret key

Keys	Lena	Peppers	Nature	Bird	Baboon	Grapes	Deblur	Butterfly	Sparrow	Average	Average all
ρ_o	266.2812	250.1576	254.6907	256.6542	246.0521	249.7321	269.5467	259.6725	248.7172	255.7227	255.28
ρ_1	255.6010	264.3201	261.6523	258.4657	253.6542	255.1045	273.6432	260.0001	235.2143	257.5173	
ρ_2	256.8234	252.5432	240.876	253.1910	254.5412	249.9934	282.8765	257.1823	240.1345	254.2402	
ρ_3	270.5571	263.0991	265.4565	255.3796	245.291	259.6876	275.6677	249.5671	239.8334	258.2821	
ρ_4	268.1634	259.4562	255.8771	249.1591	252.6577	252.6389	270.2315	243.7216	248.9992	255.6561	
ρ_5	253.5532	270.5022	246.6572	261.4325	259.7821	259.7281	265.7654	238.9991	252.7271	256.5719	
ρ_6	250.189	275.0019	234.7456	262.9745	260.9243	247.8667	269.4321	236.2161	245.9243	253.6972	
ρ_7	249.6832	265.9955	270.3456	256.9976	249.1023	244.9965	280.1788	242.7934	244.9364	256.1144	
ρ_8	262.1644	261.1735	251.4100	249.9998	243.6584	255.4578	262.8721	246.7712	239.9188	252.6029	
ρ_9	260.0323	259.999	244.3721	252.1465	245.3721	258.3004	260.8932	242.7666	242.6456	251.8364	
ρ_{10}	256.1465	262.8231	239.1753	260.7122	259.2763	260.0035	269.0045	237.1000	235.5667	253.312	
ρ_{11}	252.4521	263.4123	249.9876	274.1000	261.0003	257.8923	275.0000	249.9876	236.4261	257.8065	

Table 5.4: Difference of Percentage variance histogram values of encrypted images

Keys	Lena	Peppers	Nature	Bird	Baboon	Grapes	Deblur	Butterfly	Sparrow	Average	Average all
ρ_1 %	4.176	5.538	2.722	0.708	2.972	2.100	1.601	0.128	5.280	2.803	3.433
ρ_2 %	3.698	0.932	5.402	1.354	3.319	0.102	5.212	0.973	3.356	2.705	
ρ_3 %	1.672	5.060	4.209	0.498	0.297	3.893	2.393	3.951	3.474	2.827	
ρ_4 %	0.736	3.636	0.463	2.930	2.583	1.136	0.267	6.237	0.110	2.011	
ρ_5 %	4.977	7.955	3.141	1.868	5.369	3.908	1.478	8.084	1.568	4.261	
ρ_6 %	6.292	9.715	7.799	2.471	5.815	0.729	0.044	9.172	1.092	4.792	
ρ_7 %	6.490	6.193	6.121	0.134	1.192	1.851	4.157	6.600	1.478	3.802	
ρ_8 %	1.609	4.307	1.282	2.602	0.936	2.239	2.610	5.045	3.440	2.674	
ρ_9 %	2.443	3.848	4.035	1.762	0.265	3.350	3.383	6.611	2.374	3.119	
ρ_{10}%	3.963	4.952	6.067	1.586	5.171	4.016	0.212	8.826	5.142	4.437	
ρ_{11}%	5.407	5.183	1.839	6.822	5.845	3.191	2.132	3.787	4.806	4.335	

5.6 Texture analysis of image

In this section, the following five features are computed; energy, contrast, homogeneity, correlation, and Entropy, to describe the texture.

5.6.1 Correlation

The correlation analysis divided into three different categories. It is performed in vertical, diagonal, and horizontal formats. This analysis measures the association of pixel to its neighbor pixels. The upshots of all image’s correlation analysis are given in Table 5.5. The best encryption scheme has the correlation values equal or approaches to zero. According to results of Table 5. 5, the original image correlation values are almost close to 1 and proposed encrypted images are closer to 0. So, it indicates that proposed encrypted scheme has better results as compared to other schemes [131,124,132,112,133] presented in Table 5.11. Figure 5.12-5.17 presented the Horizontal, Vertical and Diagonal correlation of original and encrypted images.

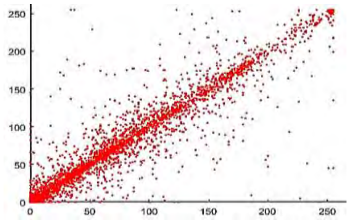


Fig.5.12: Horizontal correlation of original image

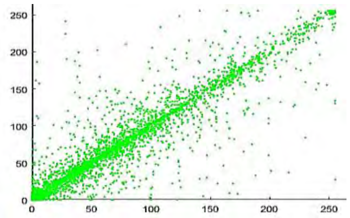


Fig.5.13: Vertical correlation of original image

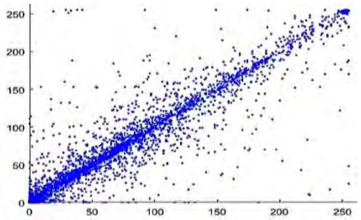


Fig.5.14: Diagonal correlation of original image

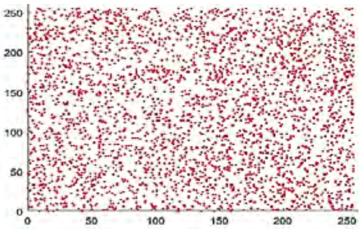


Fig.5.15: Horizontal correlation of encrypted image

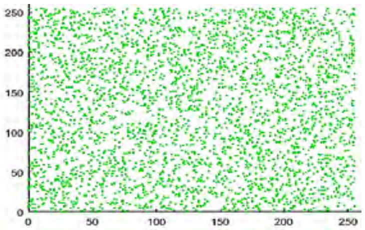


Fig.5.16: Vertical correlation of encrypted image

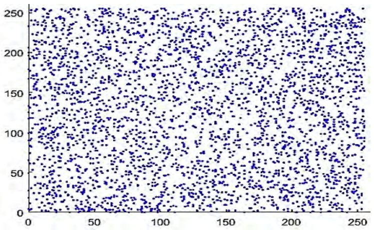


Fig.5.17: Diagonal correlation of encrypted image

5.6.2 Entropy

In Table 5.6, the entropy results of different plain and ciphered images are presented. From the table 5.6, it can be easily seen that the entropy values of all ciphered images are near optimal value i.e., 8, which shows that the loss of information in proposed encryption technique is imperceptible and it is highly robust against entropy attacks. Also, the comparison of proposed scheme presented in Table 5.11 shows that the proposed technique has much closer entropy values to optimal value than others.

Table 5.6: Entropy analysis of original and encrypted images

Images	Original Values	Encrypted Values
Lena	7.7637	7.9993593
Peppers	7.7447	7.9994499
Nature	7.5599	7.9993142
Bird	7.3321	7.9994421
Baboon	7.6792	7.9993802
Grapes	7.8067	7.9993678
Deblur	7.4240	7.9993893
Butterfly	7.5369	7.9994988
Sparrow	7.5745	7.9992008

Table 5. 5: Correlation analysis of Original and Encrypted images

Images	Planes	Horizontal		Vertical		Diagonal	
		Original	Encrypted	Original	Encrypted	Original	Encrypted
Lena	Red	0.9468	-0.000006	0.9716	0.00010	0.9216	0.000006
	Green	0.9404	-0.005602	0.9701	-0.00002	0.9303	-0.000055
	Blue	0.9064	0.000010	0.9458	0.00081	0.8754	0.000098
Peppers	Red	0.9274	-0.000004	0.9294	0.00030	0.8745	0.00043
	Green	0.9661	-0.000345	0.9703	-0.00003	0.9309	-0.00007
	Blue	0.9280	0.002223	0.9242	0.00010	0.8917	0.00020
Nature	Red	0.9442	-0.0010	0.9480	0.00012	0.9044	-0.00009
	Green	0.8932	0.00307	0.9265	-0.00009	0.8657	0.0002
	Blue	0.9655	0.00007	0.9656	-0.00077	0.9481	0.00004
Bird	Red	0.9754	0.00018	0.9696	0.00008	0.9515	-0.0007
	Green	0.9609	-0.0003	0.9556	0.00002	0.9175	0.00456
	Blue	0.9599	-0.00451	0.9479	0.00003	0.9245	-0.00043
Baboon	Red	0.9504	-0.00006	0.9417	-0.000005	0.9111	0.00055
	Green	0.9215	0.007530	0.9108	-0.00028	0.8535	-0.00009
	Blue	0.9510	-0.00020	0.9493	0.00001	0.9105	0.00076
Grapes	Red	0.9838	-0.0048	0.9801	0.00004	0.9564	0.00908
	Green	0.9848	0.0003	0.9768	-0.00063	0.9624	0.00053
	Blue	0.9738	-0.00042	0.9696	0.00001	0.9538	-0.00056
Deblur	Red	0.9933	0.000160	0.9903	0.00099	0.9867	-0.00058
	Green	0.9918	0.000300	0.9871	-0.0022	0.9756	0.00010
	Blue	0.9860	-0.00003	0.9736	0.0231	0.9631	0.00067
Butterfly	Red	0.9477	-0.000065	0.9892	-0.0007	0.8747	-0.0034
	Green	0.8938	0.00090	0.8217	0.0021	0.7602	0.00089
	Blue	0.8780	0.00034	0.7992	0.00006	0.7336	0.000009
Sparrow	Red	0.8892	0.0056	0.9162	-0.0004	0.8917	-0.000045
	Green	0.9477	-0.00055	0.8217	0.00003	0.9348	0.000057
	Blue	0.9259	-0.0006	0.7992	-0.00076	0.8312	0.000003

Table 5.7: Texture analyses for original combine plain and encrypted image

	Plain color components of image			Cipher color components of image		
	Red	Green	Blue	Red	Green	Blue
Contrast	0.5439	0.500	0.4726	10.5114	10.4770	10.4894
Homogeneity	0.8723	0.8715	0.8907	0.38933	0.38912	0.38933
Entropy	7.7893	7.7585	7.1434	7.999762	7.999770	7.999751
Correlation	0.9487	0.9391	0.9400	-0.0002134	-0.00001783	0.0000356
Energy	0.0779	0.0821	0.1708	0.01563	0.0155	0.01560

5.6.3 Differential analysis

For extraction of image important information, most attackers use a strategy where they slightly change the original plain image and then applied the proposed algorithm to encrypt the original as well as already encrypted image (which they want to crack). As a result, the two encrypted images are obtained. In this way, mostly attackers can crack cryptosystem by finding the difference of both encrypted images and this methodology is referred as Differential attack. To have a robust encryption technique, the proposed algorithm must be highly sensitive to secret key and plain text, thus any slight change in secret key or plain text would result in complete change in cipher text. For encrypted image strength estimation against the differential attacks can be calculated by two techniques; number of pixels change rate (NPCR) and unified average changing (UACI).

The sensitivity of proposed algorithm plain text is evaluated as: Firstly, the encryption is performed on original image. Then choose any random pixel in original plain image and slightly change it to get another modified original image. Now by using the same secret keys the encryption is performed on modified original image. Hence, by using these two ciphered images the NPCR and UACI values for the R, G, B planes are calculated. In order to obtain robust encryption technique for images, NPCR values should be greater than 99% and the values of UACI should be closer to 33%. NPCR and UACI results for multiple images is given in Table 5.8. And Table 5.9, presents the results of different plain images by using the proposed algorithm. The results shown in Table 8 and Table 5.9, offered that the presented encryption has high NPCR and relevant UACI values. The NPCR higher values have shown that every position of pixel is exaggeratedly randomized. And UACI pertinent values presented that nearly each gray level pixel in proposed encrypted scheme is altered. So, from the results shown in Table 5.8 and Table 5.9, it is concluded that the proposed cryptosystem has high resistance against the selected and the known plain text attacks.

Table 5.8: NPCR and UACI analysis of Combine image

		Red	*Green*	*Blue*
Proposed Algorithm	**NPCR**	99.6931	99.6943	99.6603
	UACI	33.6742	33.3248	33.6721

Table 5.9: NPCR and UACI analysis of Different images

		Red	Green	Blue
Lena	**NPCR**	99.6848	99.6672	99.7510
	UACI	33.5523	33.5210	33.5342
Peppers	**NPCR**	99.6043	99.6273	99.5987
	UACI	33.4865	33.4824	33.5836
Nature	**NPCR**	99.6634	99.6521	99.6732
	UACI	33.6553	33.5001	33.6646
Bird	**NPCR**	99.5587	99.5957	99.6922
	UACI	33.4598	32.9931	32.9542
Baboon	**NPCR**	99.6584	99.6569	99.6724
	UACI	33.6632	33.6023	33.7432
Grapes	**NPCR**	99.5998	99.6165	99.5893
	UACI	32.8956	33.0042	32.9873
Deblur	**NPCR**	99.6004	99.6492	99.6772
	UACI	33.4187	33.4269	33.5042
Butterfly	**NPCR**	99.6248	99.6155	99.6567
	UACI	33.5412	32.9587	31.9973
Sparrow	**NPCR**	99.6099	99.6475	99.5993
	UACI	32.8990	32.9999	33.0678

5.7 Randomness Test for Cipher

For assessment of cryptosystem security some properties, like long period, high intricacy, uniform distribution, and productivity NIST is used. The ciphered data is obtained by the strongly blended encryption scheme of a colored combined plain multiple images of dimension 768×768. The outcomes of the tests are seemed in Table 5.10. By breaking down these outcomes, it could be derived our expected digital image encryption tool efficiency passes the NIST test.

Table 5.10: NIST test results for strongly blended encrypted image

Test		**P – values for color encryptions of ciphered image**			**Results**
		Red	**Green**	**Blue**	
Frequency		0.80028	0.77595	0.19479	Pass
Block frequency		0.91602	0.95258	0.85069	Pass
Rank		0.29191	0.29191	0.29191	Pass
Runs ($\mathbf{M = 10,000}$)		0.042877	0.5488	0.012624	Pass
Long runs of ones		0.7127	0.7127	0.7127	Pass
Overlapping templates		0.85988	0.85988	0.85988	Pass
No overlapping templates		0.96777	0.99999	0.9983	Pass
Spectral DFT		0.042221	0.38399	0.78464	Pass
Approximate entropy		0.87635	0.24819	0.47035	Pass
Universal		0.98733	0.98343	0.98701	Pass
Serial	**p values 1**	7.2176e-05	0.85797	9.8645e-05	Pass
Serial	**p values 2**	0.0013093	0.82335	0.32965	Pass
Cumulative sums forward		0.24246	0.24244	0.31765	Pass
Cumulative sums reverse		1.0293	1.0652	0.4441	Pass
Random excursions	$\mathbf{X = -4}$	0.31944	0.011986	0.56727	Pass
	$\mathbf{X = -3}$	0.031883	0.07885	0.31625	Pass
	$\mathbf{X = -2}$	0.077929	0.011245	0.83392	Pass
	$\mathbf{X = -1}$	0.62009	0.43054	0.88576	Pass
	$\mathbf{X = 1}$	0.70841	0.45466	0.54077	Pass
	$\mathbf{X = 2}$	0.32202	0.55178	0.71311	Pass
	$\mathbf{X = 3}$	0.02052	0.19495	0.56931	Pass
	$\mathbf{X = 4}$	0.11156	0.1622	0.74306	Pass
Random excursions variants	$\mathbf{X = -5}$	0.55706	0.60043	0.22823	Pass
	$\mathbf{X = -4}$	0.84167	0.6776	0.24157	Pass
	$\mathbf{X = -3}$	0.49474	0.59816	0.27266	Pass
	$\mathbf{X = -2}$	0.17506	0.58621	0.41228	Pass
	$\mathbf{X = -1}$	0.06023	0.69444	0.60558	Pass
	$\mathbf{X = 1}$	0.31815	0.38746	0.89728	Pass
	$\mathbf{X = 2}$	0.68413	0.52539	0.70939	Pass
	$\mathbf{X = 3}$	0.8336	0.67329	1	Pass
	$\mathbf{X = 4}$	0.67324	1	0.59144	Pass
	$\mathbf{X = 5}$	0.42224	0.61877	0.54687	Pass

5.8 Classical types of Attacks

To cryptanalyze a cryptosystem, generally it is assumed that a cryptanalyst exactly knows the working and design of understudy cryptosystem, except secret key everything is known to him. To break any cryptosystem four well-known attacks are applied by attackers termed as: the known-plain text attack, chosen plain-text attack, ciphertext only attack, chosen cipher-text attack.

The proposed encryption algorithm is highly sensitive to parameters and initial values $x_0, y_0, z_0, p_0, q_0, r_0, \alpha, \gamma, a, b, and\ \sigma.$ If any one of them is slightly changed then sequences X, Y, Z, T are totally changed. In diffusion stage, bitwise XOR operation is applied between the original image I and scrambled image I' to create a new ciphered image which is then Xored with an unknown sequence T. The Xor operation between the unknown sequence values and ciphered image pixels creates a relationship that linked all the former ciphered pixels values with new values. So, it is difficult for attacker to find the current values if the former values are unknown. Therefore, the proposed scheme has resistance against chosen plaintext attacks.

5.9 Comparison

The proposed encrypted technique is compared with other given techniques by using Entropy, NPCR, UACI and Correlation analysis for each R, G, B plane for Lena image in Table 5.11. In this table, the proposed scheme is compared with other schemes presented by Ashish [131], by Liu [124], by Zhang [132], by Wang [112], by Wei [133].

Table 5.11: Performance evaluation and comparison with other methods (best values are shown in bold)

Measures	Planes	Proposed	[131]	[124]	[132]	[112]	[133]
Entropy	**Red**	**7.999532**	7.9974	7.999236	7.9968	7.9993	7.9971
	Green	**7.999532**	7.9969	7.999378	7.9965	7.9994	7.9969
	Blue	**7.999440**	7.9979	7.999304	7.9965	7.9993	7.9962
NPCR	**Red**	**99.6848**	99.623	99.60	-	**99.65**	99.58649
	Green	**99.6672**	99.606	99.60	-	99.52	99.21722
	Blue	**99.6710**	99.652	99.59	-	**99.70**	98.84746
UACI	**Red**	**33.5523**	33.245	33.51	-	33.43	33.48347
	Green	33.5210	33.362	33.50	-	33.49	**33.6399**
	Blue	**33.5342**	33.521	33.49	-	33.51	33.26891
Horizontal correlation	**Red**	**-0.000006**	**-0.00009**	-	-0.0065	-0.0131	0.0054
	Green	0.005602	-0.0011	-	**0.0009**	-0.0007	0.0059
	Blue	**0.000011**	-0.0010	-	-0.0008	0.0036	0.0013
Vertical Correlation	**Red**	**0.00010**	0.0026	-	0.0033	0.0142	0.0062
	Green	**-0.00002**	0.00009	-	0.0018	-0.0167	0.0016
	Blue	**0.00081**	-0.0030	-	-0.0033	0.0083	0.0022
Diagonal Correlation	**Red**	**0.000006**	-0.0053	-	-0.0037	-0.0044	0.0017
	Green	**-0.000055**	0.0026	-	-0.0043	-0.0145	0.0029
	Blue	**0.000980**	-0.0051	-	-0.0016	-0.0214	0.0026

Chapter 6

Conclusion and Future Work

In the proposed dissertation, our focus is to achieve the images transmissions confidentiality through public channels by designing cryptosystem using random numbers and chaos. Therefore, such systems are designed and implemented which have real-time applications and high-level security.

Chapter 1 addresses some background definitions, role of chaos in cryptography, image encryption, survey of encryption scheme, main goals, contributions, thesis structure, and some quality measures for images.

The main contributions of proposed thesis are given in Chapters 2-5.

In Chapter 2, firstly a design to generate binary pseudorandom sequences based on LFSR and modified quadratic map is presented. The technique has main advantage that it avoids any kind of interference in communication channels, also it is used in real-time applications of protecting confidential image information, internet banking and military service sector. The patterns generated by this scheme are highly non-linear which is the important property of S-boxes (i.e., non-linearity). Moreover, a cryptosystem based on substitution and permutation encryption scheme is introduced. Secondly, S-box is constructed over binary stream of pseudo random sequences, and the cryptographic strength of proposed S-box is tested. The analysis confirms the S-box effectiveness. Lastly, design of colored image encryption based on modified quadratic chaotic map sequence and S-boxes is proposed. The new encryption scheme is done in two phases i.e., Substitution and permutation, and the strategy of key association with image content is introduced. This strategy can bring “one-time pad” effect and make algorithm resistant to chosen-plain-text attack (CPA). Also, the analysis of proposed S-boxes is done and compared with other recent S-boxes techniques which depicts that proposed S-box has strong algebraic properties and highly non-linear behavior.

In Chapter 3, we proposed An RGB chaos-based Image encryption scheme using SHA-256 and Scan patterns. The designed algorithm is comprised of confusion and diffusion. In this scheme, firstly the hash values of original image are used to generate the initial values of chaotic map. The main part of proposed scheme is the confusion of binary values of image pixels. To achieve this, a new formulation is introduced which have high level security. In this technique by utilization of chaotic sequences, two index matrices based on sorted index values (Row/column wise) are attained. Then these matrices are used for achieving scan patterns (based on knight travel path), then via these patterns permutation of pixel values is done. In the end bit-wise xor is applied between three channels (i.e., R, G, B) and keys to create diffusion. This procedure transforms the original image statistical traits drastically, which creates difficulty for unauthorized person to attack\break proposed encryption. The performance and simulation analysis depicts that the proposed scheme encrypt images of any size, achieve high-robustness, uniformity and security.

In the development of strong cryptosystems, key is an important feature. With this aim, a design for generating strong keys is proposed in Chapter 4. To achieve this goal first we presented an algorithm for the initial values of key utilizing the information of image channels i.e., R, G, B. For this each layer of image is divided into blocks, then after applying convolution codes initial key values are obtained. Using these initial values, four keys are generated. Now, to create a large amount of randomness original image is divided into four blocks then the permutation step is done via two chaotic keys. The other two are used in diffusion step. Encrypted image is analyzed by different analysis like Entropy, adjacent pixels correlation analysis, Key space, key sensitivity, Differential attack analysis, Histograms, and some quality measure analysis. Also, the comparison with different schemes is done which ensures the resistance and high-level security of proposed algorithm.

Beside the single image encryption schemes, to provide more security to cryptosystem designs and make them more complex a colored multiple image encryption scheme is presented in Chapter 5. For the confusion purpose, the generated sequences of equalized histogram of Lorenz map are used to scramble the color input image subpixels. Then in diffusion stage, pixel replacement is done by scrambled images and sequences of Rossler system. An extensive security analysis that includes pixels distribution uniformity, high security level and large key space have been carried out which demonstrates a competent security of suggested scheme. The computational proficiency comparison results have shown the best performance of the anticipated encrypted scheme. The proposed scheme is resistant against the classical types of attacks and for key it is highly sensitive. The statistical simulations show that the proposed novel technique provided a safe encryption/decryption file. At the end to examine excellence of statistical properties of proposed scheme we used NIST SP 800-22, which helps in resistance of many attacks.

6.1 Future directions

In the end of this chapter, the possible directions for future work are summarized as follows:

- In random numbers generation based on hybrid PBNG's, another way for implementation of this design is to use Quantum Linear feedback shift register in combination with chaos.
- S-boxes generated by hybrid technique can also be used for multiple image encryption techniques in substitution phase to further enhance security.
- Our aim is to utilize these techniques in quantum cryptography (QC) because it helps to improve security and efficiency of image data protection due to the qubit's characteristics.
- Also, some mathematical structures in combination with puzzle games like Rubick cube are also used for designing high-resolution secure schemes for images in real-time handling conditions.

References

1. Fridrich, J. (1997, October). Image encryption based on chaotic maps. In *1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation* (Vol. 2, pp. 1105-1110). IEEE.
2. Yasser, I., Khalifa, F., Mohamed, M. A., & Samrah, A. S. (2020). A new image encryption scheme based on hybrid chaotic maps. *Complexity*, *2020*.
3. Menon, A. S., & Sarila, K. S. (2013). Image encryption based on chaotic algorithms: An overview. *International Journal of Science, Engineering and Technology Research*, *2*(6), 1328-1332.
4. Yavuz, E., Yazıcı, R., Kasapbaşı, M. C., & Yamaç, E. (2016). A chaos-based image encryption algorithm with simple logical functions. *Computers & Electrical Engineering*, *54*, 471-483.
5. Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6-21.
6. Hussain, I., & Shah, T. (2013). Literature survey on nonlinear components and chaotic nonlinear components of block ciphers. *Nonlinear Dynamics*, *74*(4), 869-904.
7. Denning, D. R. (1982). Cryptography and data security, ISBN: 0-201-10150-5.
8. McDonald, N. (2009). Past, present, and future methods of cryptography and data encryption. *A Research Review[Electronic resource]/ McDonald, N.– Mode of access: http://www. eng. utah. edu/~ nmcdonal/Tutorials/EncryptionResearchReview. pdf.*
9. Sumathi, M., Nirmala, D., & Rajkumar, R. I. (2015). Study of Data Security Algorithms using Verilog HDL. *International Journal of Electrical & Computer Engineering (2088-8708)*, *5*(5).
10. Kenekayoro Patrick, T. (2010). The data encryption standard thirty four years later: An overview. *African Journal of Mathematics and Computer Science Research*, *3*(10), 267-269.
11. Rijmen, V., & Daemen, J. (2001). Advanced encryption standard. *Proceedings of Federal Information Processing Standards Publications, National Institute of Standards and Technology*, 19-22.
12. Pointcheval, D. (2002). Asymmetric cryptography and practical security. *Journal of Telecommunications and Information Technology*, 41-56.

13. Rakeshkumar, S. K. (2013). Performance analysis of data encryption standard algorithm & proposed data encryption standard algorithm. *International Journal of Engineering Research and Development*, *7*(10), 11-20.

14. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal*, *28*(4), 656-715.

15. Carlet, C. (2015, October). S-boxes, boolean functions and codes for the resistance of block ciphers to cryptographic attacks, with or without side channels. In *International Conference on Security, Privacy, and Applied Cryptography Engineering* (pp. 151-171). Springer, Cham.

16. Detombe, J., & Tavares, S. (1992, December). Constructing large cryptographically strong S-boxes. In *International Workshop on the Theory and Application of Cryptographic Techniques* (pp. 165-181). Springer, Berlin, Heidelberg.

17. Shah, T., Jahangir, S., & de Andrade, A. A. (2017). Design of new 4x4 S-box from finite commutative chain rings. *Computational and Applied Mathematics*, *36*(2), 843-857.

18. Adams, C., & Tavares, S. (1990). The structured design of cryptographically good S-boxes. *Journal of cryptology*, *3*(1), 27-41.

19. Shah, T., Qamar, A., & Hussain, I. (2013). Substitution box on maximal cyclic subgroup of units of a Galois ring. *Zeitschrift für Naturforschung A*, *68*(8-9), 567-572.

20. Sosa, P. M. (2016). Calculating Nonlinearity of Boolean Functions with Walsh-Hadamard Transform. *UCSB, Santa Barbara*, 1-4.

21. Seberry, J., Zhang, X. M., & Zheng, Y. L. (1995). Nonlinearity and propagation characteristics of balanced boolean functions. *Information and Computation*, *119*(1), 1-13.

22. Bardis, N. G., Mitrouli, M., & POLYMENOPOULOS, A. (2004). Methods for design of balanced boolean functions satisfying strict avalanche criterion(SAC). *WSEAS Transactions on Communications*, *3*(2), 770-776.

23. Dawson, M. H., & Tavares, S. E. (1991, April). An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 352-367). Springer, Berlin, Heidelberg.

24. Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

25. Matsui, M. (1993, May). Linear cryptanalysis method for DES cipher. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 386-397). Springer, Berlin, Heidelberg.

26. Trappe, W. (2006). *Introduction to cryptography with coding theory*. Pearson Education India.

27. Liu, H., Kadir, A., & Sun, X. (2017). Chaos-based fast colour image encryption scheme with true random number keys from environmental noise. *IET Image Processing*, *11*(5), 324-332.

28. Safi, H. W., & Maghari, A. Y. (2017, October). Image encryption using double chaotic logistic map. In *2017 International Conference on Promising Electronic Technologies (ICPET)* (pp. 66-70). IEEE.

29. Radhika, K. R., & Nalini, M. K. (2017, March). Biometric Image Encryption Using DNA Sequences and Chaotic Systems. In *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)* (pp. 164-168). IEEE.

30. Khrisat, M. S., Alqadi, Z., & Khawatreh, S. A. (2020). Improving WPT color image decomposition. *International Journal of Computer Science and Information Security (IJCSIS)*, *18*(7).

31. Eltous, Y., Hamarchi, A. M., Khrisat, M. S., Khawatreh, S. A., & Alqadi, Z. Color Image Encryption-Decryption using RANDOM Noise and PMT.

32. Zhang, J., & Huo, D. (2019). Image encryption algorithm based on quantum chaotic map and DNA coding. *Multimedia Tools and Applications*, *78*(11), 15605-15621.

33. Liu, H., & Jin, C. (2017). A novel color image encryption algorithm based on quantum chaos sequence. *3D Research*, *8*(1), 4.

34. Sivakumar, T., & Venkatesan, R. (2016). A New Image Encryption Method Based on Knight's Travel Path and True Random Number. *Journal of Information Science & Engineering*, *32*(1).

35. Stallings, W. (2006). *Cryptography and network security, 4/E*. Pearson Education India.

36. Schneier, B. (2000). A self-study course in block-cipher cryptanalysis. *Cryptologia*, *24*(1), 18-33.

37. NIST, S. H. S. (1995). *Federal information processing standard*. Tech. rep., FIPS-180-1 April.

38. De Canniere, C., & Rechberger, C. (2006, December). Finding SHA-1 characteristics: General results and applications. In *International Conference on the Theory and Application of Cryptology and Information Security* (pp. 1-20). Springer, Berlin, Heidelberg.
39. Alligood, K. T., Sauer, T. D., & Yorke, J. A. (1996). *Chaos* (pp. 105-147). Springer New York.
40. Pietraszek, J., Kołomycki, M., Szczotok, A., & Dwornicka, R. (2016, September). The fuzzy approach to assessment of ANOVA results. In *International Conference on Computational Collective Intelligence* (pp. 260-268). Springer, Cham.
41. Zeng, X., Pielke, R. A., & Eykholt, R. (1993). Chaos theory and its applications to the atmosphere. *Bulletin of the American Meteorological Society*, *74*(4), 631-644.
42. Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of atmospheric sciences*, *20*(2), 130-141.
43. Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International journal of bifurcation and chaos*, *16*(08), 2129-2151.
44. Haralick, R. M., Shanmugam, K., & Dinstein, I. H. (1973). Textural features for image classification. *IEEE Transactions on systems, man, and cybernetics*, (6), 610-621.
45. Sara, U., Akter, M., & Uddin, M. S. (2019). Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. *Journal of Computer and Communications*, *7*(3), 8-18.
46. Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: from error visibility to structural similarity. *IEEE transactions on image processing*, *13*(4), 600-612.
47. Biryukov, A., & Wagner, D. (2000, May). Advanced slide attacks. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 589-606). Springer, Berlin, Heidelberg.
48. Tang, Z., Cui, J., Zhong, H., & Yu, M. (2016). A Random PRESENT encryption algorithm based on dynamic S-BOX. *International journal of security and its applications*, *10*(3), 383-392.
49. Cassal-Quiroga, B. B., & Campos-Cantón, E. (2020). Generation of dynamical S-boxes for block ciphers via extended logistic map. *Mathematical Problems in Engineering*, *2020.*

50. Carlet, C. (2015, October). S-boxes, boolean functions and codes for the resistance of block ciphers to cryptographic attacks, with or without side channels. In *International Conference on Security, Privacy, and Applied Cryptography Engineering* (pp. 151-171). Springer, Cham.
51. Detombe, J., & Tavares, S. (1992, December). Constructing large cryptographically strong S-boxes. In *International Workshop on the Theory and Application of Cryptographic Techniques* (pp. 165-181). Springer, Berlin, Heidelberg.
52. Shah, T., Qamar, A., & Hussain, I. (2013). Substitution box on maximal cyclic subgroup of units of a Galois ring. *Zeitschrift für Naturforschung A*, *68*(8-9), 567-572.
53. Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., & Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. *Nonlinear Dynamics*, *87*(2), 1081-1094.
54. Farhan, A. K., Ali, R. S., Natiq, H., & Al-Saidi, N. M. (2019). A new S-box generation algorithm based on multistability behavior of a plasma perturbation model. *IEEE Access*, *7*, 124914-124924.
55. Guesmi, R., Farah, M. A. B., Kachouri, A., & Samet, M. (2014, November). A novel design of Chaos based S-Boxes using genetic algorithm techniques. In *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)* (pp. 678-684). IEEE Computer Society.
56. Khan, M., & Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. *Neural Computing and Applications*, *29*(4), 993-999.
57. Liu, G., Yang, W., Liu, W., & Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaotic system. *Nonlinear Dynamics*, *82*(4), 1867-1877.
58. Tian, Y., & Lu, Z. (2016). S-box: Six-dimensional compound hyperchaotic map and artificial bee colony algorithm. *Journal of Systems Engineering and Electronics*, *27*(1), 232-241.
59. Ullah, A., Jamal, S. S., & Shah, T. (2018). A novel scheme for image encryption using substitution box and chaotic system. *Nonlinear Dynamics*, *91*(1), 359-370.

60. Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V. T., Jafari, S., ... & Nguyen, X. Q. (2019). S-box based image encryption application using a chaotic system without equilibrium. *Applied Sciences*, *9*(4), 781.

61. Wang, Y., Wong, K. W., Liao, X., & Xiang, T. (2009). A block cipher with dynamic S-boxes based on tent map. *Communications in Nonlinear Science and Numerical Simulation*, *14*(7), 3089-3099.

62. Jakimoski, G., & Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers based on chaotic maps. *Ieee transactions on circuits and systems i: fundamental theory and applications*, *48*(2), 163-169.

63. Zhang, X. P., Guo, R., Chen, H. W., Zhao, Z. M., & Wang, J. Y. (2018). Efficient image encryption scheme with synchronous substitution and diffusion based on double S-boxes. *Chinese Physics B*, *27*(8), 080701.

64. Zhu, S., Wang, G., & Zhu, C. (2019). A secure and fast image encryption scheme based on double chaotic S-boxes. *Entropy*, *21*(8), 790.

65. Wang, X., Çavuşoğlu, Ü., Kacar, S., Akgul, A., Pham, V. T., Jafari, S., ... & Nguyen, X. Q. (2019). S-box based image encryption application using a chaotic system without equilibrium. *Applied Sciences*, *9*(4), 781.

66. Hussain, I., Anees, A., Alkhaldi, A. H., Aslam, M., Siddiqui, N., & Ahmed, R. (2019). Image encryption based on Chebyshev chaotic map and s8 s-boxes. *Optica Applicata*, *49*(2).

67. Tanyildizi, E., & Özkaynak, F. (2019). A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps. *IEEE Access*, *7*, 117829-117838.

68. Falih, S. M. (2016). A Pseudorandom Binary Generator Based on Chaotic Linear Feedback Shift Register. *Iraq J. Electrical and Electronic Engineering*, *12*, 155-160.

69. Rahimov, H., Babaei, M., & Farhadi, M. (2011). Cryptographic PRNG based on combination of LFSR and chaotic logistic map. *Applied Mathematics*, *2*(12), 1531.

70. Ramadan, N., Ahmed, H. E. H., Elkhamy, S. E., & El-Samie, F. E. A. (2016). Chaos-based image encryption using an improved quadratic chaotic map. *American Journal of Signal Processing*, *6*(1), 1-13.

71. Mahmood, S., Farwa, S., Rafiq, M., Riaz, S. M. J., Shah, T., & Jamal, S. S. (2018). To study the effect of the generating polynomial on the quality of nonlinear components in block ciphers. *Security and Communication Networks*, *2018*.
72. Zhu, S., Wang, G., & Zhu, C. (2019). A secure and fast image encryption scheme based on double chaotic S-boxes. *Entropy*, *21*(8), 790.
73. Liu, L., Zhang, Y., & Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. *Applied Sciences*, *8*(12), 2650.
74. Belazi, A., & Abd El-Latif, A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik*, *130*, 1438-1444.
75. ul Haq, T., & Shah, T. (2020). 12× 12 S-box design and its application to RGB image encryption. *Optik*, *217*, 164922.
76. Chai, X. L., Gan, Z. H., Lu, Y., Zhang, M. H., & Chen, Y. R. (2016). A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system. *Chinese Physics B*, *25*(10), 100503.
77. Wu, J., Liao, X., & Yang, B. (2017). Color image encryption based on chaotic systems and elliptic curve ElGamal scheme. *Signal Processing*, *141*, 109-124.
78. Pareschi, F., Rovatti, R., & Setti, G. (2012). On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution. *IEEE Transactions on Information Forensics and Security*, *7*(2), 491-505.
79. Diaconu, A. V., Costea, A., & Costea, M. A. (2014). Color image scrambling technique based on transposition of pixels between RGB channels using Knight's moving rules and digital chaotic map. *Mathematical Problems in Engineering*, *2014*.
80. Li, S., Zhao, Y., & Qu, B. (2013). Image scrambling based on chaotic sequences and Veginère cipher. *Multimedia tools and applications*, *66*(3), 573-588.
81. Ye, G. (2010). Image scrambling encryption algorithm of pixel bit based on chaos map. *Pattern Recognition Letters*, *31*(5), 347-354.
82. Loan, N. A., Hurrah, N. N., Parah, S. A., Lee, J. W., Sheikh, J. A., & Bhat, G. M. (2018). Secure and robust digital image watermarking using coefficient differencing and chaotic encryption. *IEEE Access*, *6*, 19876-19897.

83. Zhang, X., Wang, L., Cui, G., & Niu, Y. (2019). Entropy-based block scrambling image encryption using DES structure and chaotic systems. *International Journal of Optics*, *2019*.
84. Muslim, M., Salim, Y., Alwi, E. I., & Azis, H. (2018, November). Modified Transposition Cipher Algorithm for Images Encryption. In *2018 2nd East Indonesia Conference on Computer and Information Technology (EIConCIT)* (pp. 1-4). IEEE.
85. Ping, P., Fan, J., Mao, Y., Xu, F., & Gao, J. (2018). A chaos based image encryption scheme using digit-level permutation and block diffusion. *IEEE Access*, *6*, 67581-67593.
86. Sun, S. (2018). A novel hyperchaotic image encryption scheme based on DNA encoding, pixel-level scrambling and bit-level scrambling. *IEEE Photonics Journal*, *10*(2), 1-14.
87. Wu, Y., Zhou, Y., Noonan, J. P., Panetta, K., & Agaian, S. (2010, April). Image encryption using the sudoku matrix. In *Mobile Multimedia/Image Processing, Security, and Applications 2010* (Vol. 7708, p. 77080P). International Society for Optics and Photonics.
88. Helmy, M., El-Rabaie, E. S. M., Eldokany, I. M., & Abd El-Samie, F. E. (2018). Chaotic encryption with different modes of operation based on Rubik's cube for efficient wireless communication. *Multimedia Tools and Applications*, *77*(20), 27337-27361.
89. Arpacı, B., Kurt, E., Çelik, K., & Ciylan, B. (2020). Colored Image Encryption and Decryption with a New Algorithm and a Hyperchaotic Electrical Circuit. *Journal of Electrical Engineering & Technology*, 1-17.
90. Liu, X., Xiao, D., & Liu, C. (2020). Quantum image encryption algorithm based on bit-plane permutation and sine logistic map. *Quantum Information Processing*, *19*(8), 1-23.
91. Niyat, A. Y., & Moattar, M. H. (2020). Color image encryption based on hybrid chaotic system and DNA sequences. *Multimedia Tools and Applications*, *79*(1), 1497-1518.
92. Wu, X., Wang, K., Wang, X., Kan, H., & Kurths, J. (2018). Color image DNA encryption using NCA map-based CML and one-time keys. *Signal Processing*, *148*, 272-287.
93. Wang, X., Wang, S., Zhang, Y., & Luo, C. (2018). A one-time pad color image cryptosystem based on SHA-3 and multiple chaotic systems. *Optics and Lasers in Engineering*, *103*, 1-8.
94. Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in engineering*, *88*, 197-213.

95. Wang, X., Wang, S., Wei, N., & Zhang, Y. (2019). A novel chaotic image encryption scheme based on hash function and cyclic shift. *IETE Technical Review*, *36*(1), 39-48.

96. Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, A. (2019, April). A novel image encryption scheme based on permutation/diffusion process using an improved 2D chaotic system. In *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)* (pp. 1-6). IEEE.

97. Zahmoul, R., Ejbali, R., & Zaied, M. (2017). Image encryption based on new Beta chaotic maps. *Optics and Lasers in Engineering*, *96*, 39-49.

98. Liao, X., Hahsmi, M. A., & Haider, R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. *Optik-International Journal for Light and Electron Optics*, *153*, 117-134.

99. Wu, J., Liao, X., & Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. *Signal Processing*, *153*, 11-23.

100. Wang, X., Zhu, X., & Zhang, Y. (2018). An image encryption algorithm based on Josephus traversing and mixed chaotic map. *IEEE Access*, *6*, 23733-23746.

101. Patro, K. A. K., & Acharya, B. (2018). Secure multi–level permutation operation based multiple colour image encryption. *Journal of information security and applications*, *40*, 111-133.

102. Dholakia, A. (2012). *Introduction to convolutional codes with applications* (Vol. 275). Springer Science & Business Media.

103. Ababneh, M. (2018). A new four-dimensional chaotic attractor. *Ain Shams Engineering Journal*, *9*(4), 1849-1854.

104. Karawia, A. A. (2018). Encryption algorithm of multiple-image using mixed image elements and two dimensional chaotic economic map. *Entropy*, *20*(10), 801.

105. Yin, Q., & Wang, C. (2018). A new chaotic image encryption scheme using breadth-first search and dynamic diffusion. *International Journal of Bifurcation and Chaos*, *28*(04), 1850047.

106. Liu, H., & Wang, X. (2010). Color image encryption based on one-time keys and robust chaotic maps. *Computers & Mathematics with Applications*, *59*(10), 3320-3327.

107. Wang, X. Y., Zhang, Y. Q., & Bao, X. M. (2015). A novel chaotic image encryption scheme using DNA sequence operations. *Optics and Lasers in Engineering*, *73*, 53-61.

108. Zhou, M., & Wang, C. (2020). A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. *Signal Processing*, *171*, 107484.

109. Cheng, G., Wang, C., & Chen, H. (2019). A novel color image encryption algorithm based on hyperchaotic system and permutation-diffusion architecture. *International Journal of Bifurcation and Chaos*, *29*(09), 1950115.

110. Wang, X., & Gao, S. (2020). Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory. *Information sciences*, *507*, 16-36.

111. Wang, X., Feng, L., & Zhao, H. (2019). Fast image encryption algorithm based on parallel computing system. *Information sciences*, *486*, 340-358.

112. Wang, X. Y., & Li, Z. M. (2019). A color image encryption algorithm based on Hopfield chaotic neural network. *Optics and Lasers in Engineering*, *115*, 107-118.

113. Javeed, A., Shah, T., & Ullah, A. (2020). Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group. *Wireless Personal Communications*, 1-14.

114. Ullah, A., Javeed, A., & Shah, T. (2019). A scheme based on algebraic and chaotic structures for the construction of substitution box. *Multimedia Tools and Applications*, *78*(22), 32467-32484.

115. Zhang, X., & Wang, X. (2018). Multiple-image encryption algorithm based on the 3D permutation model and chaotic system. *Symmetry*, *10*(11), 660.

116. Liu, W., Xie, Z., Liu, Z., Zhang, Y., & Liu, S. (2015). Multiple-image encryption based on optical asymmetric key cryptosystem. *Optics Communications*, *335*, 205-211.

117. Xiong, Y., Quan, C., & Tay, C. J. (2018). Multiple image encryption scheme based on pixel exchange operation and vector decomposition. *Optics and Lasers in Engineering*, *101*, 113-121.

118. Deng, P., Diao, M., Shan, M., Zhong, Z., & Zhang, Y. (2016). Multiple-image encryption using spectral cropping and spatial multiplexing. *Optics Communications*, *359*, 234-239.

119. Li, C. L., Li, H. M., Li, F. D., Wei, D. Q., Yang, X. B., & Zhang, J. (2018). Multiple-image encryption by using robust chaotic map in wavelet transform domain. *Optik*, *171*, 277-286.

120. Li, X., Meng, X., Yang, X., Wang, Y., Yin, Y., Peng, X., ... & Chen, H. (2018). Multiple-image encryption via lifting wavelet transform and XOR operation based on compressive ghost imaging scheme. *Optics and lasers in engineering*, *102*, 106-111.

121. Zhang, X., & Wang, X. (2019). Multiple-image encryption algorithm based on DNA encoding and chaotic system. *Multimedia Tools and Applications*, *78*(6), 7841-7869.

122. Wang, X. Y., Yang, L., Liu, R., & Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics*, *62*(3), 615-621.

123. Mandal, M. K., Kar, M., Singh, S. K., & Barnwal, V. K. (2014). Symmetric key image encryption using chaotic Rossler system. *Security and Communication Networks*, *7*(11), 2145-2152.

124. Liu, L., Zhang, Y., & Zhang, H. (2018, September). A color image encryption algorithm based on DNA computation and Chen system. In *Journal of Physics: Conference Series* (Vol. 1074, No. 1, p. 012096). IOP Publishing.

125. Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, *85*(2), 290-299.

126. Wang, X., Liu, L., & Zhang, Y. (2015). A novel chaotic block image encryption algorithm based on dynamic random growth technique. *Optics and Lasers in Engineering*, *66*, 10-18.

127. Bashir, Z., Wątróbski, J., Rashid, T., Zafar, S., & Sałabun, W. (2017). Chaotic dynamical state variables selection procedure based image encryption scheme. *Symmetry*, *9*(12), 312.

128. Zhang, Y. Q., & Wang, X. Y. (2014). A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice. *Information Sciences*, *273*, 329-351.

129. Kulsoom, A., Xiao, D., & Abbas, S. A. (2016). An efficient and noise resistive selective image encryption scheme for gray images based on chaotic maps and DNA complementary rules. *Multimedia Tools and Applications*, *75*(1), 1-23.

130. Liao, X., Hahsmi, M. A., & Haider, R. (2018). An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. *Optik-International Journal for Light and Electron Optics*, *153*, 117-134.

131. Girdhar, A., & Kumar, V. (2018). A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences. *Multimedia Tools and Applications*, *77*(20), 27017-27039.

132. Zhang, Q., & Wei, X. (2013). RGB color image encryption method based on Lorenz chaotic system and DNA computation. *IETE Technical Review*, *30*(5), 404-409.

133. Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S. (2012). A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. *Journal of Systems and Software*, *85*(2), 290-299.

134. Shah, T., Haq, T. U., & Farooq, G. (2020). Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation. *IEEE Access*, *8*, 52609-52621.

Turnitin Originality Report

Cryptosystems Designs over Random Number Generator and Chaos Theory: Image Encryption Applications by Dania Saleem Malik .

turnitin

From DRSM (DRSM L)

- Processed on 30-Aug-2021 12:08 PKT
- ID: 1638124401
- Word Count: 35570

Tariq Shah

Similarity Index
14%
Similarity by Source

Internet Sources:
9%
Publications:
9%
Student Papers:
3%

Focal Person (Turnitin)
Quaid-i-Azam University
Islamabad

sources:

1 4% match (publications)
Saira Jahangir, Tariq Shah. "A novel multiple color image encryption scheme based on algebra M(2, F2[u]/⟨u8⟩) and chaotic map", Journal of Information Security and Applications, 2021

2 < 1% match (Internet from 16-Sep-2020)
https://link.springer.com/article/10.1007%2Fs11831-018-9298-8

3 < 1% match (Internet from 29-Feb-2020)
https://link.springer.com/article/10.1007%2Fs00521-017-3195-1

4 < 1% match (Internet from 21-Nov-2019)
https://link.springer.com/article/10.1007%2Fs11045-019-00689-w

5 < 1% match (Internet from 24-Feb-2020)
https://link.springer.com/article/10.1007%2Fs11277-019-06474-z

6 < 1% match (Internet from 25-Mar-2020)
https://link.springer.com/article/10.1007%2Fs11042-014-2221-x

7 < 1% match (Internet from 23-Sep-2020)
https://link.springer.com/chapter/10.1007%2F978-3-030-38700-6_1

8 < 1% match (Internet from 23-Dec-2019)
https://link.springer.com/article/10.1007%2Fs11042-018-5782-2

9 < 1% match (Internet from 14-Jun-2019)
https://link.springer.com/article/10.1007%2Fs11042-017-4885-5

< 1% match (Internet from 25-Mar-2020)