Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing

Muhammad Tanveer

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

2022

Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing

by

Muhammad Tanveer

Supervised by

Dr. Asif Ali

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

2022

Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing

A THESIS SUBMITTED TO THE DEPARTMENT OF MATHEMATICS,
QUAID-I-AZAM UNIVERSITY, ISLAMABAD, IN THE PARTIAL FULFILLMENT OF
THE REQUIREMENT FOR THE DEGREE OF

DOCTORATE OF PHILOSOPHY

in

MATHEMATICS

by

Muhammad Tanveer

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2022

Author's Declaration

I, **Muhammad Tanveer** hereby state that my PhD thesis titled **Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing** 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: **Muhammad Tanveer**

Date: **10-10-2022**

Plagiarism Undertaking

I solemnly declare that research work presented in the thesis titled **"Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing"** 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, Islamabad** 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: **Muhammad Tanveer**

Certificate of Approval

This is to certify that the research work presented in this thesis entitled **Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing** was conducted by **Mr. Muhammad Tanveer** under the kind supervision of **Dr. Asif Ali**. 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: **Muhammad Tanveer** Signature:__________

External committee:

a) **External Examiner 1**: Signature:__________
Name: **Dr. Abdullah Shah**
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 and Statistics, International Islamic University, Islamabad.

c) **Internal Examiner:** Signature:__________
Name: **Dr. Asif Ali**
Designation: Associate Professor
Office Address: Department of Mathematics, QAU Islamabad.

Supervisor Name: Signature:__________
Dr. Asif Ali

Name of Dean/ HOD Signature: Tariq__________
Prof. Dr. Tariq Shah

Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing

By

Muhammad Tanveer

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

Tariq Shah

1. ______________________
Prof. Dr. Tariq Shah
(Chairman)

2. ______________________
Dr. Asif Ali
(Supervisor)

3. ______________________
Prof. Dr. Abdullah Shah
(External Examiner)

4. ______________________
Dr. Tahir Mehmood
(External Examiner)

Department of Mathematics, COMSATS University, Islamabad.

Department of Mathematics, & Statistics, International Islamic University, Islamabad.

Department of Mathematics
Quaid-I-Azam University
Islamabad, Pakistan
2022

Dedication

I am going to dedicate this work to

My Beloved and Last Prophet of Allah,

"HAZRAT MUHAMMAD (PEACE BE UPON HIM)"

About Him Quran says:

"**MUHAMMAD** is not the father of any of your men,

but he is **THE MESSENGER** of **ALLAH** and **KHATIM** of the **PROPHETS**,"

that is, the last of them.

Acknowledgement

All praise for **"ALLAH ALMIGHTY"** the merciful, the beneficent, the Lord of the whole word who has given me the strength to complete this thesis. The sense of He is being with me has been the sole reason of my strength throughout the time of hardships. O my Lord, I can never thank you for what you have blessed me with. Countless Darood O Salam for the "**HOLY PROPHET MUHAMMAD**" (PEACE BE UPON HIM), mercy for all the worlds, his off springs, and his companions. I offer my humblest gratitude and love to the **AHLE BAIT** and **SAHABA E KARAM**.

I express deepest gratitude to my respected and devoted supervisor **Dr. Asif Ali** for their intellectual guidance, constant encouragement, suggestions, and inexhaustible inspiration throughout my research work. His guidance and creative criticism made me what I am today. I would like to convey my heartiest gratitude to Chairman, Department of Mathematics, **Professor Dr. Tariq Shah** for his kind support and guidance that helped me to complete this important work.

What I actually want to say about my family perhaps can't be said. I want to convey my deepest love to my respected parents **Muhammad Hanif** and **Bashiran Bibi** for their 24/7 saying prayers for me during this period.

I am especially indebted to all my friends whose presence around me made my life unforgettable and joyful. I am also grateful to my dear friends **Dr. Yasir Naseer**, **Dr. Mubashir Umar**, **Dr. Muhammad Asif, Dr. Bilal Ahmed, Dr. Sadam Hussain,** and **Dr. Khalil Ur Rehman** with whom I enjoyed different hues of life. I am thankful to my seniors specially **Dr. Atta Ullah, Dr. Fahad Munir, Dr. Jamil Ahmed**, **Dr. Rizwan Ul Haq**, and **Dr. Bilal Ashraf** for their continuous support and love. I will never forget the time which I have spent with them.

I wish to express my special thanks to all of my colleagues specially **Dr. Yasir Naseer, Dr. Dawood Shah**, **Dr. Adnan Javed, Dr. Muhammad Asif,** and **Dr. Sadam Hussain**.

At the end, I would like to pay my gratitude to all others whose names are not mentioned above and have prayed for my success.

Muhammad Tanveer

10-10-2022

Preface

With the evolution of communication, digital media is now widely used throughout the world. Digital libraries containing a huge amount of information have been formed. These libraries contain digital data (books, images, magazines, even video and audio information) that can be accessed by anyone in the world. Due to free access of multimedia data throughout the internet and other accessible sources, the security of information has encouraged researchers to develop secure schemes for transmission as well as for copyright protection. Digital images are one of the major portions of communication happening around the globe. Generally, secure communication is when two individuals are communicating in such a way that no one in the path of communication can have any access to alter the data. There are many schemes available in literature to address this issue, but there is still a large room available for the development of secure, robust, and hassle-free cryptosystems.

The only nonlinear element of the block cipher is the traditional expansion of Boolean functions from sole output to numerous outputs. The role of S-boxes in cryptosystems is to create confusion, which is achieved through substitution operations. The alteration of plaintext values by the S-box certifies resistance to any attempt at cryptanalysis. Constructions of S-boxes based on finite fields are commonly used in literature. Many other algebraic structures, like groups or rings, are also used for such constructions. Cryptography and steganography are the two most important data hiding fields. The former is used to alter the original data into a bogus one, while the latter one is used to hide secret messages in a carrier.

The importance of image encryption in the field of multimedia security is an established fact. Image encryption techniques transform information into an unreadable form to avoid unauthorized access. To improve multimedia security and guarantee secure communication, we in this thesis, emphasize on the construction of dynamical S-boxes from dynamical systems.

The aim of this research is to build secure S-boxes with the additional property of diffusing the data. Based on these S-boxes, new cryptosystems are to be proposed for their practical utilization. With the advancement of computer technology, cryptanalytic schemes are also being designed to either alter the data or to recover secret messages. Therefore, the robustness of a cryptosystem is the ultimate target to be achieved.

In this thesis, three constructions of robust S-boxes are proposed to enhance the security of block ciphers. The first method of construction is based on a newly designed $3D$ chaotic map. The suggested method can produce several types of S-boxes with admirable statistical and algebraic properties. In comparison to other algebraic techniques, the proposed technique is constraint free and simple. Moreover, it generates a large number of S-boxes having the property of confusion and diffusion as well.

In the second method of construction, we designed chaotic S-boxes based on a $3D$ mixed chaotic map. This construction procedure guarantees many constraint-free, highly non-linear, and simple S-boxes. These S-boxes possess the unique property of diffusion along with confusion. These S-boxes yield the same algebraic analyses but different statistical analyses which is the motivation of our work to obtain a large number of highly non-linear S-boxes. These properties of S-boxes are very helpful for improving the multimedia security. In the third construction, we utilized linear fractional transformation for the construction of S-boxes. These S-boxes also preserve all cryptographic properties.

The designed algebraic S-boxes and dynamic S-boxes are utilized in multimedia security through image encryption. Various schemes of image encryption utilizing algebraic and dynamic S-boxes have been designed. These schemes are capable of inducing confusion and diffusion at the same time. Moreover, in these encryption schemes, pixel values of the image are scrambled utilizing algebraic and dynamic S-box transformations to puzzle the connection between the plain and the encrypted image. Their security linked with differential and linear cryptanalysis has also been confirmed. These schemes are robust and have shown excellent outcomes.

Contents

Chapter 1

Symmetric Key Cryptography Developed by Discrete Chaotic Systems and Algebraic Structures

The secure and reliable communication in today's world is a clearly defined goal of communicating parties. On way, this is achieved via the creation of a non-linear element of a block cipher prepared using a chaotic dynamical system, which is the focus of this dissertation. This chapter has two main sections. The first section highlights the goals and structure of the dissertation, while the second section provides an overview of the field of cryptography and chaos, along with the theory of substitution boxes and their cryptographic properties.

1.1. Introduction

The huge amount of digital content that is transmitted through an unsecured channel is just the tip of the Iceberg. Leaking confidential and valuable information can sometimes have disastrous consequences for public order. Digital data must be provided when entering the channel and is responsible for transferring ownership. An insecure channel is a matter of concern for many people. There are many issues related to ensuring the security of digital data, but the fact is that it does not have a specific channel and takes part in data transmission. This is the optimal solution to this problem to build a reliable and secure channel.

With the rise of multimedia technology, there is a constant need to develop an interface that serves ease of access to media files. On the other hand, there is the constraint that such ease of use must be accompanied by security features that go beyond mere password protection.

The cryptographic algorithms provide a direct solution for safe and trustworthy digital data transfer. Cryptography is a vast subject of study that encompasses a wide spectrum of innovative and trustworthy cryptosystems. The field is concerned with data security, integrity, and authentication, with the primary goal of supplementing information sent from the recipient to the sender. Converting important information into a false file is one method of doing this. This procedure can be repeated. Finally, the procedure is based on mathematical processes, which creates a vicious loop throughout the entire creation process.

Cryptography is the science that deals with the methods used to enrich copyrighted data and secure communication through channels. This is done with the help of knowledge in the fields of computer science and mathematics, and the development of algorithms that are used in documents and regulations to reliably hide transmitted information. Recovery of the original data is possible only in the case of an exact set of keys that can be used in cryptanalysis. This study is categorized based on the keys: symmetric-key cryptography and asymmetric-key cryptography. The encryption and decryption keys are the same in symmetric-key cryptography, but different keys are used for encryption and decryption in asymmetric key cryptography, also known as public-key cryptography. Input data is in the form of blocks and streams that continue to divide the cipher into block and stream ciphers, respectively. In addition, the hash function will have a different code, splitting the information.

Confusion and diffusion, introduced in [1] are the two main characteristics of a reliable cryptosystem. The first is achieved by an ambiguous relationship between each of the binary bits with the key. The second intends that 50% of the output bits will have to change with a single bit change in input. It is recommended to develop a cryptosystem in which the strength can be increased by slightly changing the parameters that must be implemented through creating confusion and diffusion in the system. Boolean functions are an example of following the criteria specified above, and therefore, their presence in such systems is mandatory.

After the launch of the advanced encryption standard (AES) [2], the need for developing a new standard was minimized, because the application is secure. The substitution box (S-box), whose creation is mathematical, is the sole non-linear component of the AES block cipher. Different mathematical systems are used to develop cryptographically strong S-boxes to ensure the security of the cryptosystem instead of making a new encryption standard. The aim of block cipher confusion is accomplished by employing the S-box to the encrypted text. In addition, S-boxes can also be used in the design of steganography, watermarking, and image encryption [3], [4].

The Boolean function and block cipher are being recognized as important components of a modern cryptosystem. The former gives one output for one input and the latter generates more output bits for one input bit. Both are interlinked by the application of the theory of function.

The S-box is a look-up table constructed from a mathematical system. In the first instance, the text is divided into blocks of data, in bytes. The design of the S-box incorporates original information with S-box entries. If done correctly, the probability of recognizing the input information is close to zero.

The main goal of an attacker is to gain access to all the data that can be transmitted using the security system. In addition, it is forced verification and modification of data that are the hacker's main objectives. The sort of block cipher construction, in this respect, is their primary goal. By using various guesses of linear, differential, and brute-force attacks, the attacker breaks the weak cryptosystem. The biggest obstacle in a block cipher is the S-box. If the non-linear component of the block cipher is stronger, an encryption system is more secure.

Many physical systems are chaotic in the discipline of Biology, Physics, and Engineering, such as weather forecasting and the movement of gases in the atmosphere. Chaos theory is used today in engineering, biology, physics, and economics to evaluate dynamical systems. Discrete systems are easy to navigate in models and can be used for forecasting even for longer periods, unlike chaotic dynamical systems. It has been observed that in any chaotic system, mathematically, there is a non-linear system. Such systems are sensitive to initial parameters, inherently unstable, uncertain, and follow a complex distribution formula. These properties make them difficult to analyze but perfect for application in cryptography. Such applications use features such as unpredictability and randomness in the construction of a cryptosystem that is not predictable.

This thesis involves the use of chaotic dynamical systems in multimedia security to build cryptographically strong S-boxes. In addition, these S-boxes are used for encryption, its sole purpose is to increase the security of the encryption systems.

1.2. Research Goals

This study aims to achieve the following goals:

1. Identification of chaotic dynamical systems that are well suited for creating rich and complex dynamics based on mathematical schemes.
2. Instead of using a $1D$ system to create a stream of pseudorandom numbers, the use of multidimensional systems is proposed to produce more than two streams of pseudorandom numbers.
3. The systems are built with the goal of producing a large number of S-boxes with certain cryptographic properties.
4. To examine the effectiveness of these systems and applications in multimedia security, image encryption schemes must be developed.
5. The ultimate goal is to achieve all of the above goals with low computational complexity.

The non-linear components of a block cipher have a particularly important role and are at the heart of the methods of this thesis. The aim of this thesis is to develop new S-boxes with compatible/improved cryptographic properties. In addition, their effectiveness can be determined by utilizing them in image encryption schemes and analysing experimental results and observations. This can be achieved with various mathematical structures or processes used to obtain the necessary randomness. Our goal is to design new chaotic dynamical systems and use them for S-box construction as well as encryption schemes. In this way, we expect that we will have to develop new systems for the security of information data using novel chaotic systems.

1.3. Thesis Layout

This thesis consists of six chapters. Detail information about all the chapters is provided below.

Cryptography, Chaos, and Substitution box theory are mostly discussed in Chapter 1. Some key concepts in cryptography, Boolean algebra, Substitution box theory and block ciphers, have been explained in detail.

The second chapter is divided into two parts. In the first part, we investigated a three-dimensional ($3D$) chaotic map in detail. A dynamic S-box is created using the $3D$ chaotic map, which is then evaluated using standard measures of substitution boxes. The created S-box retains all cryptographic characteristics, whereas a $3D$ mixed chaotic map is presented in the second section. The S-boxes are then constructed using a $3D$ mixed chaotic map. As the algorithm runs, each dimension of the $3D$ mixed chaotic map generates an S-box. To explain the procedure, we only went over three s-boxes. This approach can create infinite S-boxes. To ensure that all created S-boxes retain cryptographic characteristics, the test S-boxes are examined using standard analyses.

In Chapter 3, the S-boxes built in Chapter 2 are used to design two different image encryption schemes. S-boxes are utilized to create confusion in these schemes. Image encryption includes a significant amount of confusion. These encryption schemes are also subjected to standard analysis to determine the strength of the image encryption algorithm.

The small algebraic S-boxes are thought to be better for lightweight cryptography. For this purpose, Chapter 4 describes a small S-box construction technique and its application to image encryption. S-boxes are constructed using the linear fractional transformation. These S-boxes are later employed in an image encryption technique to cause confusion. Security analysis determines the strength of suggested encryption algorithm.

The Legendre chaotic map, its chaotic behaviour, and its use in image encryption are all covered in Chapter 5. The design of the image encryption technique consists of five steps. These five steps provide the essential confusion and diffusion for every encryption method. The security analysis is also examined critically.

In Chapter 6, the conclusion of the work presented in this dissertation is explored.

1.4. Preliminaries of Cryptography

The term cryptography is derived from the Greek word "Kryptos", which means "hidden". Consequently, cryptography is concerned with concealing information so that unlawful users cannot read it. It is, in fact, a study that comprises the concepts and strategies for transforming understandable/meaningful information into a meaningless one and then restoring that meaningless message to its original form. Cryptography provides information security resources as well as a set of techniques. The basic idea of cryptography is given below in Fig. 1.1.

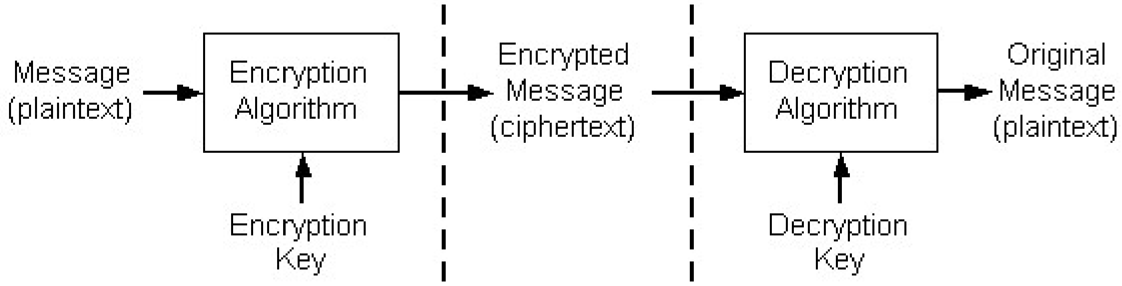


Figure 1.1: Basic idea of cryptography

Basically, in cryptography, the initial form of an understandable message is transformed into some meaningless and non-understandable form using some key. This key is known as an encryption key and the process is called **encryption**. The authorized person only knows how to get the original information using some key from the transformed message. Here, the used key is known as a decryption key and the process is called **decryption**.

In cryptography, mainly two methods are used for transforming a message, viz. transposition and substitution. The process of rearranging the characters of a message using some rules is called transposition, while the process of replacing all the characters of the message with some other characters under some rules is called substitution. In the substitution method, the main idea is to pick out a permutation p of letters that are used to compose the plaintext and then substitute each letter e in the plaintext with $p(e)$. This permutation p is called a key.

Cryptography is an inter-disciplinary study of Mathematics, Computer Science, and Electrical Engineering.

1.4.1. Basic Terminologies in Cryptography

Here, some basic notions of cryptography are described.

Definition 1. The text or message which is in understandable/readable form is called **plaintext**.

The plaintext can be a text file, numerical data, a stream of bits, or an audio or video file. We can say that plaintext is simply binary data that a computer uses, which is denoted by M.

For example, "MATH IS GREAT FUN". The characters used to write plaintext are called the plaintext alphabet. These characters may be the English alphabet, punctuation marks, and numerals.

Definition 2. The text or message which has been transformed into a meaningless/non-readable form is called the **ciphertext**.

The ciphertext is also binary data and usually the size of the ciphertext is the same as the plaintext M but may be larger. It is denoted by C.

For example, "NQCKFDNLGHFDSDFGH". The characters used to write converted messages are called the ciphertext alphabet. These characters may be the same as the plaintext alphabet or different.

Definition 3. A set of rules which transform an understandable/readable message into a meaningless form and vice versa by means of transposition and/or substitution is called a **cipher**.

Definition 4. A **substitution cipher** is one that uses the substitution technique for encryption, whereas a **transposition cipher** uses the process of transposition for encryption.

Definition 5. Some uncertain data or information known to the sender and receiver used by the cipher is called a **key**. It is denoted by K .

Definition 6. The method of transforming an understandable/readable message into a meaningless form is called **enciphering**. It is also known as encryption or encoding.

Definition 7. The method of transforming a meaningless/non-readable message into an understandable/readable form is called **deciphering**. It is also known as decryption or decoding.

Definition 8. A mathematical process that converts a meaningful message into a meaningless form by different transformations and substitutions is called the **Encryption algorithm**.

Definition 9. A mathematical process that converts a meaningless message into a meaningful message by different transformations and substitutions is called the **Decryption algorithm**.

Definition 10. **Cryptology** is a field of mathematics that studies cryptography and cryptanalysis.

Definition 11. **Cryptanalysis** is the process of retrieving an intelligible message from an unintelligible message without knowing the key, but with the help of known principles and methods of transformation. It is also known as "**Breaking of Code".**

1.4.2. Fundamental Goals of Cryptography

Understanding the challenges related with information security is required to become acquainted with cryptography. All parties engaged in a transaction must have assurance that specific information security goals have been accomplished. The fundamental goals of secure communications are confidentiality, data integrity, authentication, and non-repudiation.

1.4.2.1. Confidentiality

As the name implies, the term signifies the restriction of use to authorized parties (sender and receiver), both of whom can only see the data. The data is kept secret from all unauthorized parties (for instance, hackers, interceptors). That is, if X and Y are two people and they want to have a conversation between themselves, then X sends messages to Y, then these sent messages should be readable by Y only and they should not be readable by any unauthorized person Z.

1.4.2.2. Data Integrity

This goal signifies that no one other than authorized parties can modify the information. If X sends messages to Y, then these sent messages should be modifiable for X and Y only. These messages should not be modifiable by any unauthorized person Z. Y must be proficient enough to check out messages sent by X that have been modified by an unauthorized person Z.

1.4.2.3. Authentication

This goal solidifies the identification of the source of data and one's identity. For instance, if *X* sends messages to *Y*, then *Y*, after receiving messages from *X*, must be proficient at confirming that messages received from *X* are surely initiated by *X*.

1.4.2.4. Non-Repudiation

It is a tool for ensuring that the information was indeed transmitted by the sender. If *X* sends messages to *Y* and *X* acknowledges that he did so.

1.4.3. Categories of Cryptography

Cryptography is subdivided into symmetric-key cryptography and public-key cryptography.

1.4.3.1. Symmetric-Key Cryptography

The sender and recipient in this category utilise the same key. The sender uses a key *K* to encrypt a meaningful information into a meaningless information, and the receiver uses the same key *K* to decode the meaningless message into a meaningful message. This cryptography approach is symmetric encryption since a single key is utilised at both ends. The distribution of keys is a difficulty in this approach since encryption and decryption are accomplished using a single key. Fig. 1.2 depicts a graphical representation of this category.

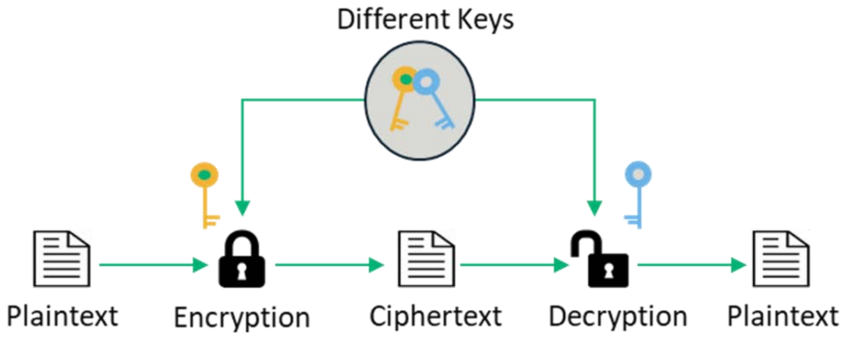


Figure 1.2: Illustration of Symmetric-Key Cryptography

This category is further subdivided into block ciphers and stream ciphers.

1.4.3.1.1. Block Cipher

A fixed-length block of an intelligible message is converted into a nonsensical message of the same length as the intelligible message in block cipher.

1.4.3.1.2. Stream Cipher

The Stream Cipher is also a symmetric-key encryption system. Stream ciphers are projected to be extremely fast, and the work of these ciphers is considerably quicker than block ciphers. These ciphers work on smaller parts of information as compared to block ciphers, which work on big blocks of information.

1.4.3.2. Public-Key Cryptography

Different keys are used at both ends in public-key cryptography. The transmitter uses a key (say K_1) to encrypt an intelligible message into a nonsensical message, while the receiver uses another key (say K_2) to decrypt the received nonsensical message into an intelligible message. This cryptography approach is asymmetric encryption since it employs a pair of keys.

Both participants in this approach utilize a private key as well as a public key (sender and receiver). The private key is kept hidden and not revealed in this case. The public key, on the other hand, is shared with all communicating members. If Bob wants to transmit a secret message to Alice, he will encrypt it with Alice's public key. Alice will use her private key to decipher Bob's encrypted communication after receiving it.

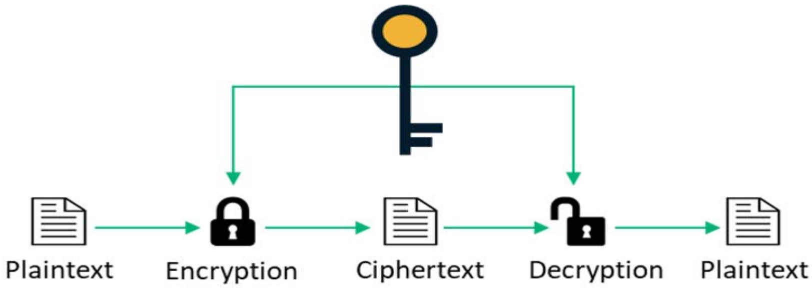


Figure 1.3: Illustration of Public-Key Cryptography

1.5. Boolean Algebra

Boolean functions in algebra are an essential prerequisite for diving deeper into software computing devices. This area of mathematics contracts the real line into two outputs, viz, zero and one. This contraction of the real line resulted in the microprocessor and fast systems inventions. It is also imperative for research to have a better understanding of block ciphers and the S-box. In addition, the transmitted information is converted to bits and bytes, which further processing also needs to have prior knowledge of Boolean algebra. Boolean functions have been studied for a long time, and this section of the dissertation can never do justice to a well-established and broad theory. Our goal is to set a language and notation straight for what follows within the dissertation, specifically regarding the basic cryptographic functions that are described in this dissertation.

Definition 12. Let $GF(2^m)$ is an m-dimensional vector space over the Boolean field $\mathbb{Z}_2$. A **Boolean function** σ is defined as:

$$\sigma : GF(2)^m \to GF(2) \tag{1.1}$$

Here $GF(2^m)$ is the Galois field, comprising 2^m elements in binary form, $u = (u_1, u_2, u_3, \cdots, u_m)$.

The number of elements in domain and codomain sets is 2^m and 2 respectively, the possible distinctive Boolean function is 2^{2^m} that can be built.

Remarks: $GF(2^m) \simeq \mathbb{Z}_2^m$, Since $GF(2)^m$ and $\mathbb{Z}_2^m$ are vector spaces over $\mathbb{Z}_2$.

Throughout this section, σ and σ^* will refer to m-variable Boolean functions.

Definition 13. [4] The collection of binary outcomes of $\sigma(u)$ for each u is the truth table for $\sigma(u)$.

Definition 14. [5] The **polarity** truth table of an m-variable Boolean function σ is given as follows:

$$\hat{\sigma}(u) = (-1)^{\sigma(u)} \tag{1.2}$$

Note that $\hat{\sigma}(u) \in \{1, -1\}$.

Definition 15. Consider a Boolean function $\sigma(u)$ of m-variables, its **hamming weight** is the number of ones (1's) in the truth table (see [5]). It is denoted by $\mathrm{H}(\sigma^*)$ or $\mathrm{H}(\sigma)$.

It is one of the main terms used in explaining many concepts related to the theory of Boolean functions.

Definition 16. Consider two Boolean functions σ, σ^*, then the **hamming distance** is denoted by $d(\sigma, \sigma^*)$, is the number of different truth table positions from each other [6].

$$d(\sigma, \sigma^*) = \#\left\{u \in GF(2)^m \,\middle|\, \sigma(u) \neq \sigma^*(u)\right\} \tag{1.3}$$

It is also known as the Hamming weight of the *XOR* sum of two Boolean functions.

$$d(\sigma,\sigma^*) = \mathrm{H}\left(\sigma \oplus \sigma^*\right) \tag{1.4}$$

The degree of similarity between σ and σ^* is marked by the Hamming distance. These include a parable related to the idea of the correlation of two functions, which is of particular importance for cryptographic analysis. The correlation coefficient of completely uncorrelated and correlated functions is zero and one, respectively.

Definition 17. [6] Consider two Boolean functions σ,σ^* then the **correlation** is denoted by $Corr(\sigma,\sigma^*)$, is defined as follow:

$$\begin{aligned}
Corr(\sigma,\sigma^*) &= 2P\left(\sigma(u) = \sigma^*(u)\right) - 1 \\
Corr(\sigma,\sigma^*) &= 2\left[\frac{2^m - d(\sigma,\sigma^*)}{2^m}\right] - 1 \\
Corr(\sigma,\sigma^*) &= 2\left[1 - \frac{d(\sigma,\sigma^*)}{2^m}\right] - 1 \\
Corr(\sigma,\sigma^*) &= 2 - 2\frac{d(\sigma,\sigma^*)}{2^m} - 1 \\
Corr(\sigma,\sigma^*) &= 1 - \frac{d(\sigma,\sigma^*)}{2^{m-1}}
\end{aligned} \tag{1.5}$$

Using the definition of $d(\sigma,\sigma^*)$:

$$\begin{aligned}
Corr(\sigma,\sigma^*) &= 1 - \frac{d(\sigma,\sigma^*)}{2^{m-1}} \\
Corr(\sigma,\sigma^*) &= 1 - \frac{\sum_u (\sigma(u) \oplus \sigma^*(u))}{2^{m-1}} \\
Corr(\sigma,\sigma^*) &= \frac{2^m - 2\sum_u (\sigma(u) \oplus \sigma^*(u))}{2^m} \\
Corr(\sigma,\sigma^*) &= \frac{\sum_u 1 - 2\sum_u (\sigma(u) \oplus \sigma^*(u))}{2^m} \\
Corr(\sigma,\sigma^*) &= \frac{\sum_u 1 - 2(\sigma(u) \oplus \sigma^*(u))}{2^m} \\
Corr(\sigma,\sigma^*) &= \frac{\sum_u \sigma(u)\sigma^*(u)}{2^m}
\end{aligned} \tag{1.6}$$

The results of $Corr(\sigma,\sigma^*)$ lie down in the interval $[-1,1]$. The $Corr(\sigma,\sigma^*) = 1$ or -1 Whenever $d(\sigma,\sigma^*) = 0$ or 2^m, respectively. This is the main component for determining the imbalance among pairs of functions.

Definition 18. [5] A Boolean function σ is said to be **totally uncorrelated** to a Boolean function σ^* if $Corr(\sigma,\sigma^*)=0$. Total uncorrelation indicates that the assessment of σ is independent of the information of σ^*.

Definition 19. [5] The **algebraic normal form** of σ is stated as:

$$\sigma(u_1,u_2,u_3,\cdots,u_m)=\underset{J\subseteq F}{V}\alpha J\prod_{j\in J}u_j, F=\{0,1,2,\cdots,m\} \tag{1.7}$$

where V represents bitwise exclusive-or operation, the coefficients $\alpha J\in\{0,1\}$, produce the truth table for the *ANF* of $\sigma(u)$.

It is simple to see that each *ANF* representation corresponds to a single Boolean function truth table. The *ANF* represents a Boolean function in the form of a unique *XOR* sum of the input variables and products.

Definition 20. The correlation between function and the set of all linear functions is measured by the **Walsh Hadamard Transform (*WHT*)**. The *WHT* value for different Boolean functions is unique. *WHT* is another way of defining Boolean functions.

1.5.1. Cryptographic Properties of Boolean functions

Definition 21. [7] σ is said to be **balanced** if $W(\sigma)=0$ or $W(\sigma)=2^{m-1}$. Equivalently, if $\#\{u:\sigma(u)=0\}=\#\{u:\sigma(u)=1\}$ and **imbalanced**, otherwise. It follows that:

$$\begin{aligned}
\mathrm{I}(\sigma)&=2^{m-1}(Corr(\sigma(u),0))\\
\mathrm{I}(\sigma)&=\left|W(\sigma)-2^{m-1}\right|\\
\mathrm{I}(\sigma)&=2^{m-1}\left(1-\frac{d(\sigma(u),0)}{2^{m-1}}\right)\\
\mathrm{I}(\sigma)&=2^{m-1}-d(\sigma(u),0)\\
\mathrm{I}(\sigma)&=\left|2^{m-1}-W(\sigma)\right|
\end{aligned} \tag{1.8}$$

where the zero Boolean function is denoted by 0. The scalar value between 0 and the correlation coefficient σ is proportional to $I(\sigma)$. Any function having a zero imbalance is balanced and with the constant function, it does not correlate.

An important and desirable cryptographic property of σ is its non-linearity. This is because each linear system can be easily hacked, utilizing linear cryptanalysis. The degree of nonlinearity $N_L(\sigma)$ can be determined as the Hamming distance between σ and other suitably chosen functions.

Definition 22. [7] The minimal Hamming distance between the set of all m-variable affine functions and an m-variable Boolean function σ determines the **non-linearity** $N_L(\sigma)$ of σ.

$$N_L(\sigma) = 0.5(2^m - WHT_{\max}) \tag{1.9}$$

where WHT is an abbreviation of Walsh–Hadamard Transform and WHT represents the maximum absolute value.

There are other ways to determine nonlinearity of σ. A more efficient way is to use the minimum distance between the affine function and the order of σ. Therefore, non-linearity can be introduced or even increased by reducing the minimum distance to the affine function. As you can see from the formula, a small change to the truth table will make minor changes to the minimum distance.

Definition 23. [5] σ is supposed to validate an **avalanche criterion** if a change in one bit of the input bits changes by half the average value of the output bits.

It also takes care of confusion and diffusion of expected results and guarantees randomness. Such a change in the output signal can be viewed using the derivative of a Boolean function.

Definition 24. [5] The **avalanche effect** $A_{y_j}(\sigma)$ for σ corresponding to a variable y_j is expressed as:

$$A_{y_j} = prob(\sigma(u) \oplus \sigma(u \oplus y_j)),\ \forall u \tag{1.10}$$

Definition 25. [5] A function $\mathbb{Z}_2^m \to \mathbb{Z}_2^S$ is **complete** if

$$\sum_{u \in \mathbb{Z}_2^m} \sigma(u) \oplus \sigma(u \oplus C_j^m) > (0,0,0,\cdots,0), \forall j = 1,2,\cdots,m \tag{1.11}$$

where both the summation and the relation > are applied component-wise.

Definition 26. [5] σ is said to fulfil SAC, if

$$\forall s,\ W(s) = 1, \sum\nolimits_u \sigma(u)\sigma(u \oplus s) = 2^{m-1} \tag{1.12}$$

That is, for one of the inputs, because of the change, one-half of the output bits will probably need to be changed.

Another useful measure is correlation immunity.

Definition 27. σ has i_{th} order **correlation immunity** if it does not depend upon any of the subsets with $i\ (1 \le i \le m)$ input variables. A function is **resilient** if it is balanced and has correlation immunity.

1.6. Substitution Boxes

The substitution box is the sole non-linear component in the block ciphers. Some essential ideas for describing the S-box theory are provided to support the study. In addition, some of the cryptographic key characteristics of S-boxes are given here.

The S-box addresses the conventional development of the notion of one input to multiple outputs.

Definition 28. An **S-box** of dimension $n \times m$ is a nonlinear mapping $S : \mathbb{Z}_2^n \to \mathbb{Z}_2^m$ working on n input bits and generating m output bits

For $n = m$, there are two different S-box formats. In one case, each input has its output, while in the second-several inputs to the same one, all possible outputs do not exist in an S-box. It is referred to be a bijective S-box if it is one-to-one and onto. That is, each input is assigned a unique output, and all outputs are included in the S-box. For reversible S-boxes, it may be the case that $n = m$. Reversible S-boxes play a very important role in symmetric-key cryptosystems.

1.6.1. Cryptographic Properties of Substitution Box

In this subsection, the standard measures for evaluating the cryptographic properties of S-boxes are given. To resist linear attacks on the approximation of the S-box, the degree of nonlinearity is also of great importance. Higher values of nonlinearity indicate strength and rigidity, against linear attacks.

Definition 29. **Nonlinearity** computes the base separation concerning the arrangement of all n-variable Affine functions and an n-variable Boolean function. It is computed by:

$$NL(g) = 0.5(2^n - WHT_{\max}) \tag{1.13}$$

where WHT is an abbreviation of Walsh–Hadamard Transform and $WHT_{\max}$ represents the maximum absolute value.

In other words, nonlinearity is the smallest Hamming distance of a Boolean function to the collection of affine functions [8].

In any substitution-permutation network, the Avalanche effect is observable whenever a chain of deviations is produced due to the consequence of a solitary input disparity [6].

Definition 30. A mapping $S:\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ is said to satisfy the **Strict Avalanche Criterion** (SAC) if the following relation holds:

$$\sum_{u \in \mathbb{Z}_2^n} S(u) \oplus S(u \oplus C_j^n) = (2^{n-1}, 2^{n-1}, 2^{n-1}, \cdots, 2^{n-1}), \ (1 \leq j \leq n) \tag{1.14}$$

This criterion was met for each of the strong S-boxes together with the completeness property. It quantifies the extent to which the output bits are changed by a single input bit alteration. One bit in the input, which changes about half of the output bits, is a very interesting observation indeed. For any S-box to satisfy this measure, it must change 50% of the output bits by one-bit alteration in the input bits. This measure indicates the powerful resistance throughout plaintext attacks.

The bit independence criterion (BIC) investigates the information bits which remain unchanged. The symmetric cryptosystem has this compelling property. By increasing freedom among bits, it is almost difficult to foresee and perceive the indications of the framework.

Definition 31. A mapping $S:\mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^n$ is said to satisfy the **Bit Independence Criterion** if $\forall x, y, z \in \{1, 2, 3, \cdots, m\}$ with $y \neq z$, changing x input bit make y and z output bits to vary independently.

The BIC is to investigate the effect of integration from a single input bit to total output bits. Therefore, the independent behaviour of two avalanche vectors in pairs and the variation of input bits are imperative factors for BIC. The range values for BIC are in $[0,1]$, where the minimum and maximum values of this interval indicate the ideal and the worst cases respectively.

It computes the imbalance of the occurrence. This investigation helps to count the supreme estimation of the inconsistency of an occasion between input and output.

Definition 32. The maximum amount of imbalance of an event is measured in the **linear approximation probability** (LAP) [9]. It is computed as:

$$LP = \max_{\Gamma_u \Gamma_v \neq 0} \left[\frac{\#\{u : u \cdot \Gamma_u = S(u) \cdot \Gamma_v\}}{2^n} - 0.5 \right] \tag{1.14}$$

where Γ_u and Γ_v are two covers, u and v are all possible inputs, and 2^n is the quantity of the information component.

Definition 33. Differential approximation probability (DP) ensured uniform mapping. For each alteration in the input, there must be a unique change in the yield. This climax of differential estimate likelihood guarantees uniform mapping likelihood for each information bit *i*.

$$DP = (\Delta u \to \Delta v) = \left[\frac{\#\{u \in X : S(u) \oplus S(u \oplus \Delta u) = \Delta v\}}{2^n} \right] \tag{1.15}$$

1.6.1.1. Majority Logic Criterion

An image encrypted with an S-box must pass the majority logic requirement in this criterion. It includes analyses such as homogeneity, energy, contrast, correlation, and entropy [10]. These analyses are used to measure the alterations made to an encrypted image. To put it another way, they are used to examine the strength of an S-box for image encryption.

1.6.1.2. Randomness Test (NIST SP-800 22)

The NIST-authenticated randomness test, also known as NIST SP 800-22 [11], is used to verify the statistical randomness and unpredictability of pseudorandom number generators for cryptographic purposes. This contains fifteen tests, including frequency (mono-bit) tests, block frequencies, long runs of ones, overlapping templates, approximate entropy, and random excursions, etc. The frequency test, which counts the number of ones and zeroes in a sequence, is the most fundamental of these. The passing of this test determines the outcome of the next fourteen tests. If it fails, the probability of other failures increases. After that, the test suit software analyzes the remaining tests to proclaim the randomness of the input data.

1.7. Chaos and Chaotic Systems

Typically, each of the physical systems governed by a series of mathematical equations that create dynamics that are impossible to predict over time is known to be one of the most chaotic systems. Chaos is also known as confusion or disorder. Some systems and changes are observed over time, occasionally providing chaotic motion. Thus, now time and change are two foundations of the chaos theory. A system’s chaotic behavior is identified by a graphical estimate of the system's time series. These systems are unpredictable because they do not follow any trends. There are many natural and laboratory studies of dynamic system design in the fields of engineering, electronic engineering, physics, economics, ecology, and many, many others) that have been found useful. You do not have to accept chaotic behavior resulting from a complex system of equations before we can see the disorderly motion of a simple equation, as in [12]–[14]. The only variable that can appear in the equation generates chaos, i.e., it has no restrictions on the number of variables and parameters. Also, several systems are deterministic, meaning they represent a large set of line equations to predict the next term or region, but still, if they were random, such a system should generate deterministic chaos. In addition, self-movement leads to the chaotic movement of the system, which means that there is no need for external participation-necessary to produce chaos, which is an option. All this will lead to a difficult situation-determining the level of chaos in real cases. Although they can be seen in the fields of mathematics and computer science, thanks to the graphical representation of control equations in problems.

The scientists' first and most important attraction to chaos theory is the visualization of the complex and disordered behavior of a system that results from a simple deterministic equation. Secondly, the system being considered is comprehendible at the same time, impossible to decipher and recognize from the solution trajectory. The third attraction is the minimum amount of knowledge of higher mathematics that can be understood by the game, along with basic knowledge of algebra, geometry, and data analysis. After all, chaos can be analyzed without going too deep into the underlying mathematical equations. All these revelations came as a surprise to cryptographers and forcing them to use such systems means creating strong cryptosystems that are difficult to decipher.

1.7.1. Chaotic Dynamical Systems

In chaos, perhaps, sometimes, as in a system, changes are detected over time. Temporal chaos and spatial chaos arise when time has been replaced by space and distance, respectively. Unlike linear systems, nonlinear equations that appear in algebra or differential equations are difficult to solve. The dynamics of such systems can be very complex. Also, each of the nonlinear systems does not have to be chaotic. Many experts believe that nonlinear dynamics, the theory of dynamical systems, is in the field of chaotic dynamical systems.

There are two types of dynamical systems, depending on energy conservation. In a conservative dynamical system, there is no energy loss. That is, the system is friction-free. At the same time, a dissipative system is charged by friction and loses energy in the process. A dissipative dynamical system, after the loss of energy, a limiting factor is realized. Under the influence of these restrictions, chaotic solutions are born. In this thesis, we will focus on chaotic dynamical systems, and hence on dissipative dynamical systems.

Changes in the dynamical system can be observed at discrete time intervals. These intervals can be uniform or nonuniform. Examples of such systems are storms, earthquakes, and volcanic eruptions. Discrete-time systems are controlled by differential equations that are iteratively solved. Variations in dynamical systems should also be observed over a continuous period. There is continuity in the measurement of such phenomena, in contrast to discrete time intervals. Differential equations are used to calculate continuous changes in a dynamical system. Examples of such systems are temperature, heat, and water flow in rivers and streams.

Differential equations are a large and developed branch of mathematics that is found in almost all areas where a physical system is subject to modelling. Thanks to the active work of mathematicians in this field, it can predict phenomena in acoustics, astrophysics, weather forecasting, and many other areas of life sciences. The idea is to implement differential equations in cybersecurity when designing secure and stable systems. The only non-linear component of a block cipher is designed using a system of non-linear differential equations that must be solved, and which can become an obstacle to cryptanalysis.

1.7.1.1. Causes of a chaotic system

Chaos theory is a multidiscipline topic. The importance of chaos in recent decades has been recognized by many scientists by considering such systems for their proper evaluation and examination. The factors causing chaos in real-world phenomena are still unknown. To some extent, one can say that the factors causing chaos are variations in control parameters, deviations from initial conditions, nonlinear interaction of two or more progressions, involvement of nonlinear terms in the equations, and noise/resistance.

1.7.1.2. Characteristics of a chaotic system

The peculiar nature of a chaotic dynamical system is still a well-known problem for scientists. With the advancement of computing devices, the bifurcation pattern of chaotic systems can be visualized by using different software, but still, getting the proper grip on this subject is an objective for many. The unusual behaviour is observed by all in analysing these systems. The specific attributes of a chaotic system are as followed.

1.7.1.2.1. Sensitivity to initial conditions

The most important property of a chaotic system is its sensitive behaviour towards initial conditions and parameters. Sometimes, slight variations in initial input result in different bifurcation patterns of that system. Cryptographically speaking, this property is the most attractive for the design of a cryptosystem. It assures the sender that any slightly wrong guess will generate a different solution space, hence the predictability of data is minimized.

1.7.1.2.2. Entropy

The amount of disorder is usually evaluated in entropy analysis. Since a chaotic system bears the most disorderly behaviour. That's why entropy is linked with these systems.

1.7.1.2.3. Lyapunov exponent

The Lyapunov exponent is used to decide whether the mathematical system used is chaotic or not. The value of this exponent greater than zero implies the chaotic nature of a system.

1.7.1.2.4. Long term unpredictability

This characteristic of a chaotic system is very interesting and irrational. The bifurcation pattern and trajectory of such a system are unpredictable for a very long interval. This is very useful for the utilization of such systems in cyber security.

1.7.1.3. One-dimensional discrete chaotic system

The chaotic system used in cryptography is reviewed hereafter based on dimensions initially. Mostly, simple chaotic systems having one dimension are used in cryptography because they are easy to understand and evaluate as compared to higher dimension systems. The shortcoming lies in these small solution spaces, can be predicted using advanced technology, the fewer number of controlled parameters and conditions, and smaller key spaces. Due to all these, the recapture of such a system using different software is comparatively an easy task [15].

1.7.1.3.1. The logistic equation

The population model in terms of an equation known as the logistic equation was proposed by biologist Robert May in 1976 [13]. This is the simplest discrete time intervals based chaotic system. It explains various key features of a chaotic system. Moreover, many researchers have used this map because of its simplicity in cryptography [16], [17]. Mathematically, its map is represented as:

$$\chi_{m+1} = \gamma\chi_m\left(1-\chi_m\right) \tag{1.16}$$

1.7.1.3.2. Tent map

The Tent map is an iterative map-generating deterministic chaos under a certain selection of the parameter χ, which is considered responsible for controlling chaos. The range of χ for this map is in $\left[1,2\right]$ for chaotic behaviour.

$$\begin{aligned} \chi_{m+1} &= 2\chi_m \text{ if } 0 \le \chi \le 0.5 \\ \chi_{m+1} &= 2-2\chi_m \text{ if } 0.5 \le \chi \le 1 \end{aligned} \tag{1.17}$$

This map with a slight extension in it has been utilized by [16] in the field of chaotic cryptography.

1.7.1.3.3. Quadratic map

The term quadratic refers to the polynomial of degree 2. The standard quadratic equation is

$$a\chi^2 + b\chi + c = 0 \tag{1.18}$$

The constants *a*, *b* and *c* define the chaotic behaviour of this quadratic map. For example,

$$\chi_{m+1} = c + \chi_m^2 \tag{1.19}$$

Where *c* is a constant. The above equation is a special case of the standard quadratic equation for the case $a=1$ and $b=1$. A similar quadratic equation generating chaos is of the type

$$\chi_{m+1} = \left(\chi_m - 2\right)^2 \tag{1.20}$$

1.7.1.3.4. Henon Map

This is an example of a discrete time dynamical system proposed by Michel Henon [19] to explain the Poincare section of the Lorenz model. It involves two parameters *a* and *b* that control the chaos. Mathematically,

$$\begin{aligned} \chi_{m+1} &= 1 - y_{m+1} + a\chi_m^2 \\ y_{m+1} &= b\chi_m \end{aligned} \tag{1.21}$$

[1] Utilized this map for the construction of the S-box.

Chapter 2

Design of Nonlinear Component of Block Cipher using 3*D* Chaotic map

Three-dimensional chaotic systems with rich chaotic and complicated dynamics are used in data security in this chapter. These systems will first be used to produce random numbers, which will be permuted to create a highly nonlinear chaotic S-box. The suggested design's key advantage is the ability to create a large number of cryptographically strong S-boxes by modifying the system's parameters and initial states slightly. The algebraic and statistical analyses that are easily available in the literature are used to evaluate the S-boxes created in this chapter. The study's findings are encouraging, demonstrating the study's relevance to secure communications implementation.

2.1. Introduction

Humanity's desire for global communication via diverse technologies is rising quickly. It includes sensitive material from fields such as biology, engineering, foreign ministries, and the military. Data loss or modification is always a possibility while chatting online. Many companies pay huge sums of money to ensure safe data transfer. These cryptanalysts foresee the illicit interception, alteration, and use of secret information that must be secured. Researchers employ cryptographic methods to secure sensitive data transmission.

Cryptography is the art of hiding data from beginning to finish using cryptographic methods, such that no one in the communication channel can obtain the important data communicated. If the sender supplies a proper algorithm and keys, only authorised persons will have access to the generated data. There are two types of cryptosystems: symmetric and asymmetric. Asymmetric cryptography does not utilise the same key for encryption and decryption. Symmetric cryptography does. Symmetric cryptography is divided into two types: stream ciphers and block ciphers [5]. The block cryptosystem served as the motivation for this chapter. To allow the cryptographic technique to be employed in a step-by-step way, the plaintext is divided into blocks.

The two basic concepts of block cryptosystems, confusion and diffusion, were proposed by Shannon [1]. Substitution, permutation, mixing, and adding keys are the four processes of the block cryptosystem [8], [20]–[23]. The algorithms of the block cryptosystem first divide the primary data into blocks of equivalent size, then encrypt the entire block. Diffusion is the process of modifying and obscuring the plaintext containing the sender's original message by distributing the original text bits to the cipher text bits. Confusion refers to the process of changing plain text to modify encrypted text. To accomplish these two properties, round recurrence is often employed.

When certain parameters are constrained, specific systems cause chaos. Such chaotic dynamical systems are extremely sensitive to initial conditions and exhibit unpredictable behaviour, resulting in a variety of paths given varying initial conditions. Because of its unpredictability, chaotic dynamical systems are employed in cryptosystems to generate confusion and diffusion. Chaotic systems and block cryptosystem characteristics like as confusion and diffusion have a strong connection. The system's sensitivity to initial conditions/parameters, unpredictability, and chaos all contribute to this link's existence. A wider solution area also permits many reliable and secure S-box approaches from a single system to coexist.

In contrast to previous systems such as logistic, tent, and Chebyshev maps, this methodology use a three-dimensional system. In the suggested approach, this three-dimensional system is responsible for complex and chaotic dynamics, making it ideal for the creation of an S-box.

2.2. 3*D* Chaotic Map

Since color images has three layers, Red, Green, and Blue (RGB). In order to encrypt each layer of color image with high security level, we designed 3*D* chaotic map which is very sensitive to initial conditions and highly chaotic (Randomness). This designed 3D map is analyzed by chaotic attractors as shown in section 2.2.

This map is used to generate three nonlinear chaotic sequences which are used for image encryption. These three random sequences are extracted and used for pixels rows and columns permutations. Finally, these sequences are further used to construct chaotic Substitution boxes. Then, the pixels are substituted with the entries of newly designed Substitution boxes to enhance the confusion in the encrypted image.

This section suggests a chaotic map for a more efficient multi-image encryption scheme. The suggested 3*D* chaotic map is defined as:

$$x_{(u+1)} = \mu^{m} \cdot \sin(x_u) + y_u - \lambda^{m} \cdot \cos(z_u) \tag{2.1}$$

$$y_{(u+1)} = \sin(x_u) \cdot \cos(y_u + x_u + \tan(z_u)) \tag{2.2}$$

$$z_{(u+1)} = y_u \cdot \cos\left(x_u\right) + x_u \cdot \sin\left(y_u\right) - \psi^{m} \cdot \tan^{-1}(y_u) - \sigma \tag{2.3}$$

ψ, μ, λ and σ are the control parameters, *x, y, z* are the variables, and *u, m* are nonnegative integers as *m* represents the exponent.

Every chaotic system exhibits chaotic behavior for a specific interval of control parameters and initial values. The interval for control parameters for suggested system in Eq. (2.1) to Eq. (2.3) is:

$$0 \le \lambda, \psi \le 2, \; 0 \le \mu, \sigma \le 1,$$

Further, *x, y, z* are the obtained pseudo-random sequences, where:

$$-8 \le x \le 8, \; -1 \le y \le 1, -8 \le z \le 8, \text{ and } 0 \le m \le 10,$$

As an example, the chaotic behavior of the suggested map for the initial values:

$$x_1 = 0.20005, \; y_1 = 0.00001, z_1 = 0.10038,$$

$$\psi = 1.113, \mu = 0.6888, \lambda = 1.43332 \text{ and } \sigma = 0.11.$$

is presented in Fig. 2.1. The non-uniform histograms of the suggested chaotic sequences are made uniform by the histogram equalization approach [24]. The histograms of the proposed sequences are shown in Fig. 2.2. Fig. 2.3 illustrates the 2*D* and 3*D* chaotic trajectories of the suggested dynamic system. The chaotic sequences and trajectories obtained by the 3*D* chaotic map are distributed uniformly and have complex chaotic behavior, which is suitable for image encryption.

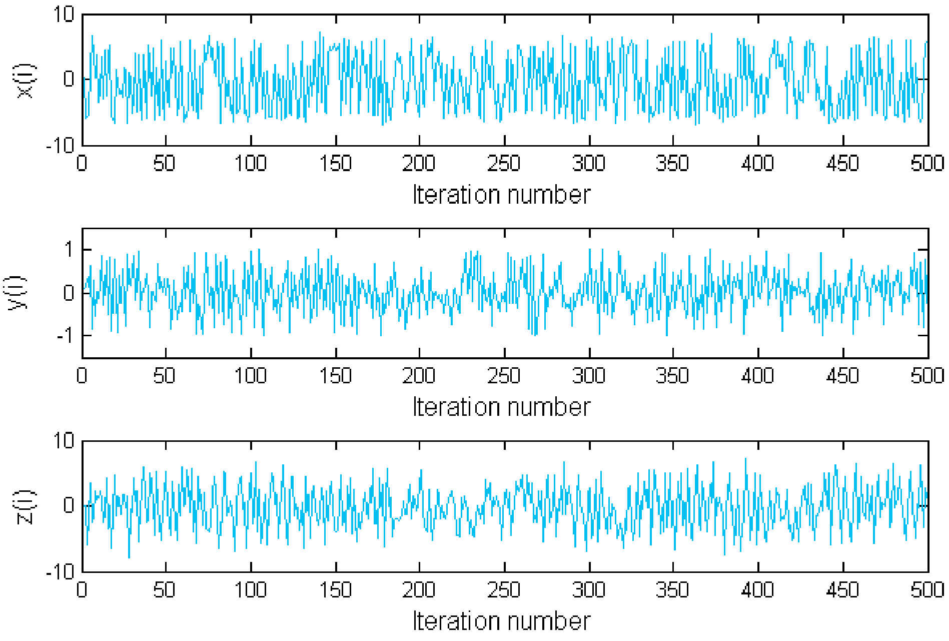
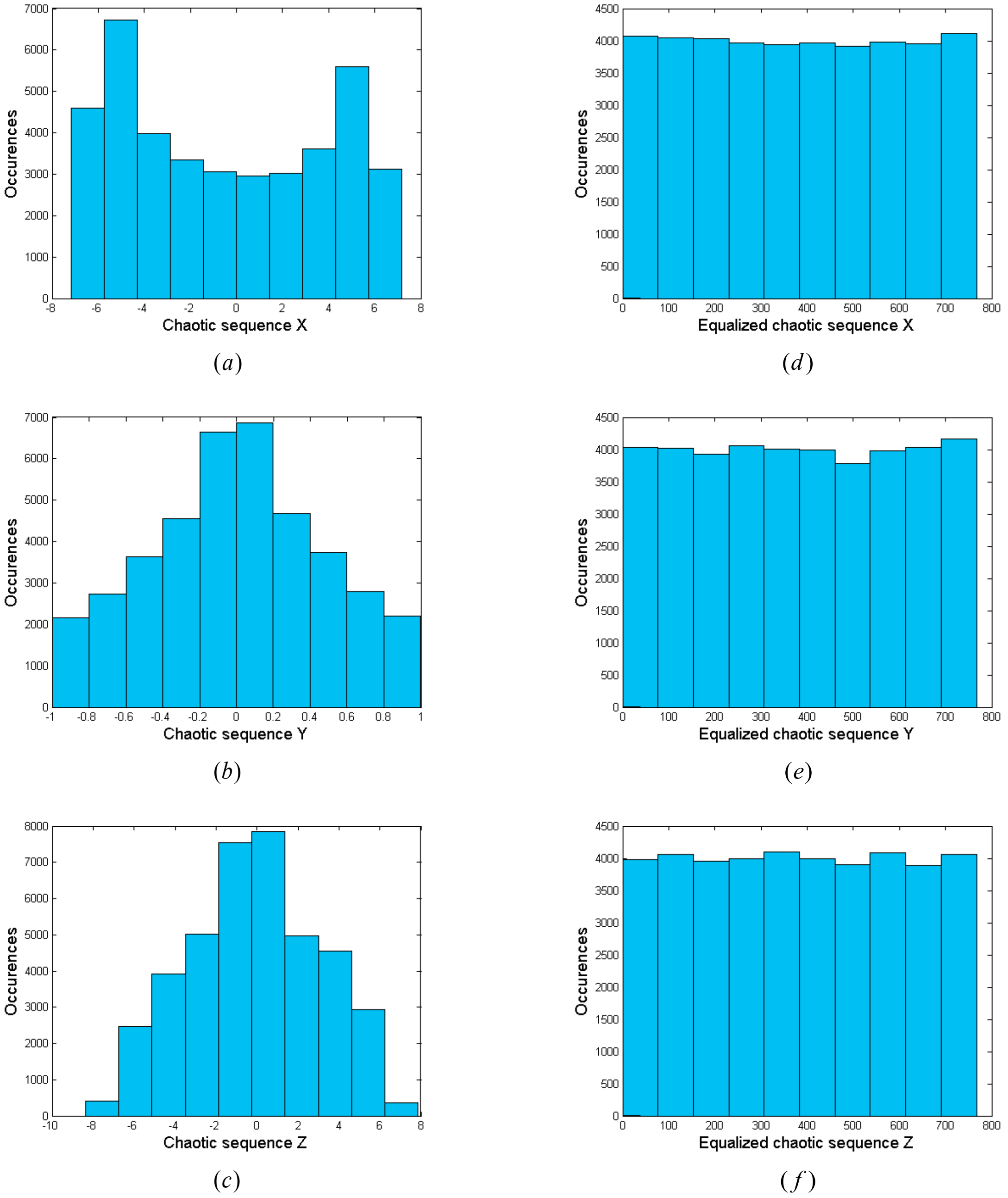


Figure 2.1: Chaotic performance of the suggested chaotic X, Y, and Z sequences

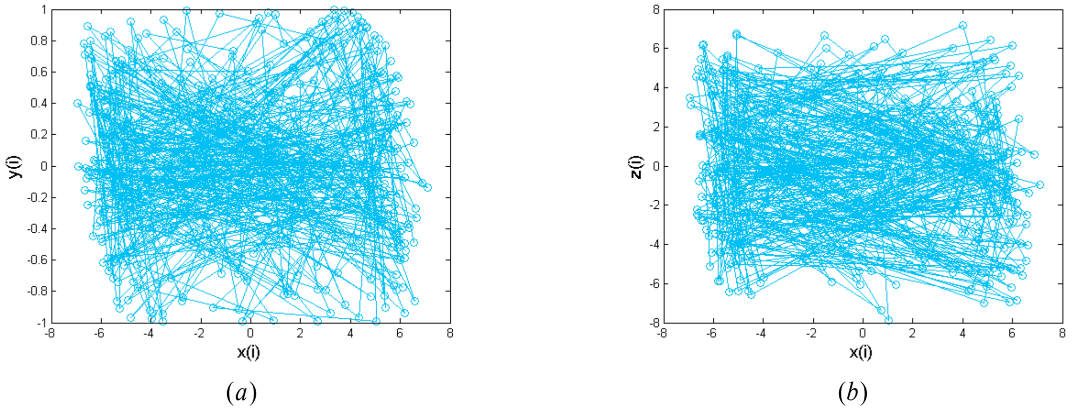


(*a*) (*d*)

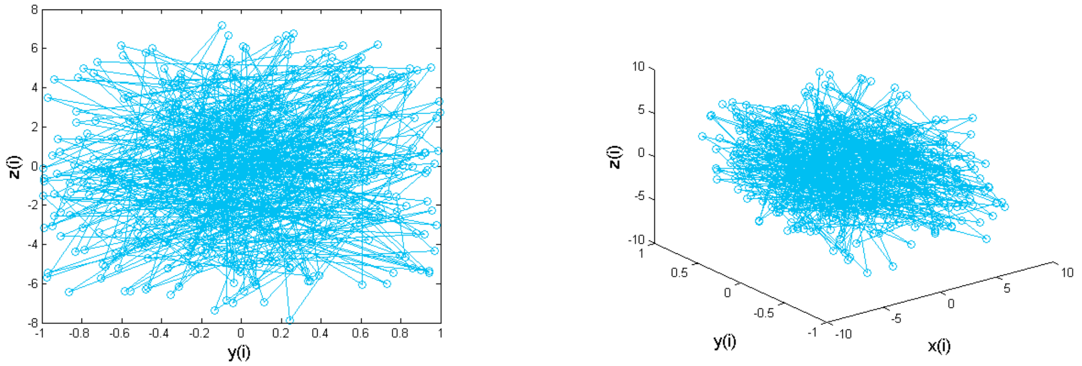
(*b*) (*e*)

(*c*) (*f*)

Figure 2.2: Histograms of suggested sequences.
2.2(*a-c*): Histograms before equalization, 2.2(*d-f*): Histograms after equalization



(*a*) (*b*)



(c) (d)

Figure 2.3: $2D$ and $3D$ chaotic trajectories of a suggested chaotic map.
3(a): the trajectory of (x_i, y_i); 3(b): the trajectory of (x_i, z_i); 3(c): the trajectory of (y_i, z_i); 3(d): the trajectory of (x_i, y_i, z_i)

2.2.1. Construction of Substitution boxes (1st Construction)

The system of equations used here is far superior that generates significant complex and chaotic dynamics. Subsection 2.2 describes the range of parameters for the chaotic bifurcation pattern seen on MATLAB.

The following are the steps involved in the creation of a substitute box:

- Initial condition used in Eq. (2.1) to Eq. (2.3) are:

$$x_1 = 0.20005,\ y_1 = 0.00001,\ z_1 = 0.10038,$$

$$\psi = 1.113, \mu = 0.6888, \lambda = 1.43332 \text{ and } \sigma = 0.11.$$

- In this step extract y_i from the sequence $[x_i, y_i, z_i]$. We can extract anyone among from the sequence $[x_i, y_i, z_i]$.
- Multiplying y_i with 100000 to get a new sequence of numbers L in integer representation.

$$L = y_i \times 100000,$$

- The sequence of numbers M is obtained using $ceil(\text{mod}(L \times 256, 256))$.

$$M = ceil(\text{mod}(L \times 256, 256)).$$

- In the final step, the above-mentioned sequence is permuted in MATLAB to produce an S-box with appropriate cryptographic characteristics.

The flowchart below explains all the steps.

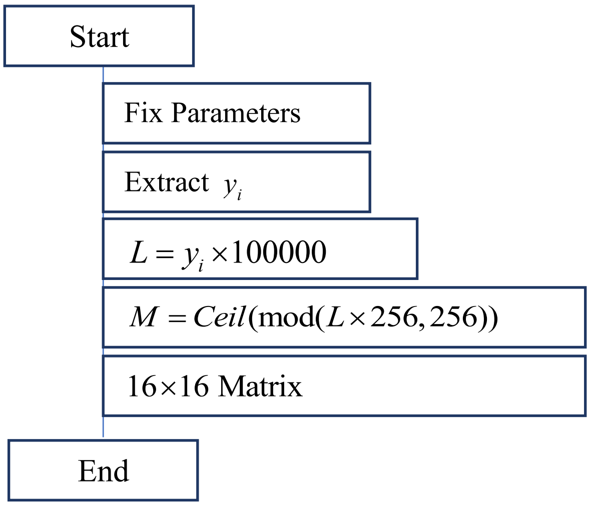


Figure 2.4: Flow chart for S-box design

Table 2.1: Suggested S-box

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

2.2.2. Algebraic analyses for substitution boxes

This section examines the effectiveness of the block cipher's nonlinear component. The measurements that determine its efficacy include nonlinearity analysis, bit independence criteria (BIC), strict avalanche criterion (SAC), and linear and differential approximation probabilities. The details of these analyses are presented below.

2.2.2.1. Nonlinearity

It is the most important among all the cryptographic characteristics. Nonlinearity must be higher to have a robust cryptographic system. If we express nonlinearity mathematically as *NL*, then it is defined as:

$$NL(g) = 0.5(2^n - WHT_{\max}) \tag{2.4}$$

where WHT is an abbreviation of Walsh-Hadamard Transform and $WHT_{\max}$ represents the maximum absolute value which validates resistance to linear cryptanalysis by calculating the resistance of a system described as a set of linear equations.

Table 2.2: The nonlinearity analysis and comparison

S-boxes	**Proposed**	**Ref.** [28]	**Ref.** [33]	**Ref.** [34]	**Ref.** [35]	**Ref.** [36]
Average	103.5	103.2	103.3	103	105.25	104.7
Minimum	100	98	99	100	102	102
Maximum	108	108	106	106	108	108

Table 2.2 clearly indicates that the average value achieved from the suggested strategy for creating S-boxes is significantly higher than that obtained from other approaches previously found in the literature.

2.2.2.2. Bit Independence Criterion

This concept is employed in substitution boxes to increase the efficiency of the confusion function. Webster and Tavares [25] were the first to develop this statistical criterion, which states for a given set of avalanche vectors, avalanche variables must be pairwise independent.

Table 2.3: The BIC analysis and comparison

S-Boxes	**Average**	**Minimum Value**	**Square Deviation**
Proposed	103.214	100	1.9522
Ref. [26]	106	102	2.1380
Ref. [27]	103.24	98	2.6098
Ref. [28]	103.78	100	1.8776

Table 2.3 displays the results of the BIC analysis, as well as a comparison to other existing methods. The suggested S-box has a minimum value of 100, an average of 103.214, and a square deviation of 1.9522. These findings outperform those seen in [26], [27]and [28].

2.2.2.3. Strict Avalanche Criterion

It quantifies the extent to which a single input bit change affects the output bits [29]. It is computed by:

$$HW(t) = 1\sum_{x} g(x)g(x \oplus t) = 2^{n-1}, \tag{2.5}$$

where $g(x)$ is the Boolean function satisfies Eq. (2.5) for every t.

For any S-box to satisfy this measure, it must change 50% of the output bits by one-bit alteration in the input bits. Table 2.4 displays the results of the SAC analysis, as well as a comparison to other existing methods. The suggested S-box has a minimum value of 0.406250, an average of 0.498047, and a maximum of 0.593750. The comparison also confirms the usefulness of the proposed S-box.

Table 2.4: The SAC analysis and comparison

S-boxes	**Proposed**	**Ref.** [28]	**Ref.** [16]	**Ref.** [33]	**Ref.** [34]	**Ref.** [35]	**Ref.** [36]
Minimum	0.406250	0.3671	0.4219	0.4140	0.4218	0.4297	0.3906
Average	0.498047	0.506	0.4939	0.499	0.500	0.496	0.506
Maximum	0.593750	0.5975	0.5625	0.6015	0.6093	0.5313	0.5937

2.2.2.4. Linear Approximation Probability

The linear approximation probability (LAP) measures the highest level of imbalance in an event [29]. It is computed as:

$$LP = \max_{\Gamma_u \Gamma_v \neq 0} \left[\frac{\#\{u : u \cdot \Gamma_u = S(u) \cdot \Gamma_v\}}{2^n} - 0.5 \right] \tag{2.6}$$

where Γ_u and Γ_v are two covers, u are all possible inputs, and 2^n is the quantity of the information component.

In other words, it is the greatest value of an event's disparity. Table 2.5 displays the LP analysis findings, which are compared to various S-boxes. These findings show that the suggested S-box provides significant resistance against linear attacks.

Table 2.5: The LAP analysis and comparison

S-boxes	**Proposed**	**Ref.** [28]	**Ref.** [16]	**Ref.** [33]	**Ref.** [34]	**Ref.** [35]	**Ref.** [36]
Max. LP	0.14062	0.1289	0.1250	0.1328	0.1289	0.1562	0.1250
Max. Value	160	162	160	164	162	168	160

2.2.2.5. Differential Approximation Probability

Uniform mapping is accomplished via differential approximation probability (DP). There must be a distinct change in the yield for each change in the input. This climax of differential estimate likelihood guarantees uniform mapping likelihood for each information bit *i*.

$$DP = (\Delta u \rightarrow \Delta v) = \left[\frac{\#\left\{ u \in X : S\left(u\right) \oplus S\left(u \oplus \Delta u\right) = \Delta v \right\}}{2^{n}} \right] \tag{2.7}$$

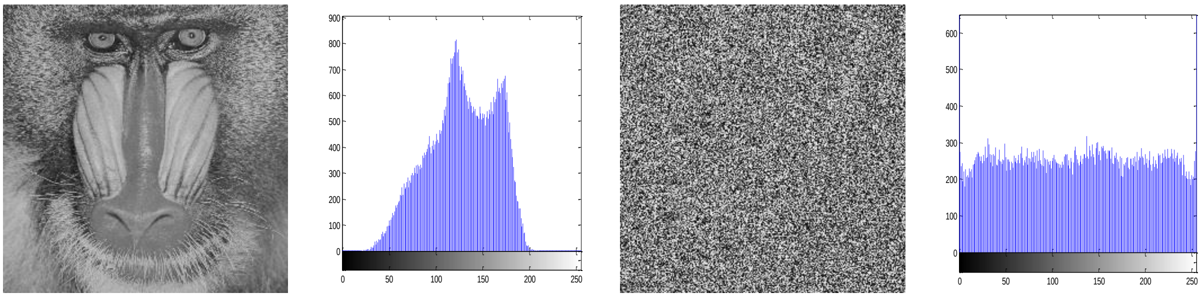
Table 2.6 shows the result and comparison of DP for the suggested S-box. Because the suggested S-box has a DP of 0.046875, it is effective against differential attacks. These results collectively show that the new S-box will outperform many others.

Table 2.6: The DP analysis and comparison

S-boxes	**Proposed**	**Ref.** [28]	**Ref.** [16]	**Ref.** [33]	**Ref.** [34]	**Ref.** [35]	**Ref.** [36]
Max. DP	0.046875	0.04688	0.0625	0.03906	0.05469	0.03906	0.04688

2.2.2.6. Majority Logic Criteria

An image encrypted by an S-box must pass the majority logic criterion (MLC). It includes analyses such as homogeneity, energy, contrast, correlation, and entropy [29]. These analyses are used to measure the alterations made to an encrypted image. The graphical representations of these analyses are shown in Fig. 2.5, and the comparison for the proposed S-box is shown in Table 2.7.



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

Figure 2.5: Histogram of original and encrypted images using the proposed S-box

Fig. 2.5(*a*) and Fig. 2.5(*c*) illustrate the host and the encrypted images. Fig. 2.5(*b*) and Fig. 2.5(*d*) shows their respective histograms.

Table 2.7: The MLC analysis and comparison

Pictures	**Entropy**	**Correlation**	**Energy**	**Homogeneity**	**Contrast**
Original	7.2187	0.6947	0.0887	0.7549	0.8657
Proposed	7.9657	0.0035	0.0257	0.4035	10.4572
Ref. [20]	7.9591	-0.0441	0.0202	0.4151	8.2314
Ref. [22]	7.9561	0.0554	0.0202	0.4662	8.3124
Ref. [30]	7.9431	0.0155	0.0219	0.4248	8.2113

The MLC results are similarly encouraging, indicating that the suggested S-box is suitable for the construction of cryptographic algorithms for data encryption.

2.3. 3*D* mixed Chaotic Map

The 3*D* mixed chaotic map is defined by the following equations:

$$\alpha_i = sin\left(n_1 sin^{-1}\left(\sqrt{\alpha_{i-1}}\right)\right)^2 , \tag{2.8}$$

$$\beta_i = sin\left(n_2 sin^{-1}\left(\sqrt{\beta_{i-1}}\right)\right)^2 , \tag{2.9}$$

$$\gamma_i = sin\left(n_3 sin^{-1}\left(\sqrt{\gamma_{i-1}}\right)\right)^2 . \tag{2.10}$$

This system has chaotic behaviour for the initial values $\alpha_1 = \sin\left(\theta_1 \pi n_1\right)^2 , \beta_1 = \sin\left(\theta_2 \pi n_2\right)^2$, $\gamma_1 = \sin\left(\theta_3 \pi n_3\right)^2$, here $n_1, n_2, n_3 = n_1 \times n_2$ are parameters which are non-zero real numbers. Further, $i \geq 2,\ i \in \mathbb{Z}^+, \theta_j \in \left(0, 2\pi\right], j = 1,2,3$ and $\pi \approx 3.14$. We used $\theta_j = 45^\circ, j = 1,2,3$ in initial conditions. The equations (2.8) - (2.10) are used to cause N term chaotic sequence.

2.3.1. Construction of Substitution boxes (2nd Construction)

We utilized the following expressions and changed them into integers in the range of $[0-255]$.

$$\alpha_i' = round\left(\alpha_i \times 10^{15} \bmod 256\right), \tag{2.11}$$

$$\beta_i' = round\left(\beta_i \times 10^{15} \bmod 256\right), \tag{2.12}$$

$$\gamma_i' = round\left(\gamma_i \times 10^{15} \bmod 256\right). \tag{2.13}$$

Using Eq. (2.11) with the initial condition $\alpha_1 = \sin\left(\theta_1 \pi n_1\right)^2$, the first suggested S-box is given in Table 2.8.

Table 2.8: Substitution box 1 (S-box 1)

215	57	147	179	7	192	76	114	61	250	128	101	87	201	176	198
15	213	253	96	178	36	227	142	0	13	173	74	42	241	211	139
161	109	132	32	233	148	228	40	144	162	11	138	151	50	24	129
152	124	62	207	247	107	205	33	97	67	149	37	174	231	43	242
26	156	83	193	70	118	59	46	79	68	181	137	254	112	125	243
216	208	5	167	225	115	200	222	195	80	45	196	140	219	163	18
72	119	86	47	123	164	223	10	226	120	39	82	73	238	155	55
169	232	191	64	103	54	126	116	186	52	92	246	3	190	199	12
157	9	170	53	30	183	69	65	1	113	63	105	175	212	136	88
236	249	188	110	166	182	34	160	220	75	172	168	19	204	158	165

17	133	127	27	150	221	180	14	141	90	23	187	20	251	171	66
229	185	230	2	203	77	44	121	91	6	99	89	48	78	245	106
237	35	145	217	135	214	240	31	248	189	25	224	93	104	102	202
153	194	21	108	210	252	134	234	38	111	255	51	235	8	197	154
94	146	100	218	130	16	58	22	131	60	209	81	84	184	29	95
239	41	143	206	98	28	122	244	177	4	159	117	56	49	71	85

Using Eq. (2.12) with the initial condition $\beta_1 = \sin\left(\theta_2 \pi n_2\right)^2$, the second suggested S-box is given in Table 2.9.

Table 2.9: Substitution box 2 (S-box 2)

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

Using Eq. (2.13) with the initial condition $\gamma_1 = \sin\left(\theta_3 \pi n_3\right)^2$, the third suggested S-box is given in Table 2.10.

Table 2.10: Substitution box 3 (S-box 3)

213	156	109	233	234	216	125	129	243	2	128	68	204	166	39	103
215	250	127	96	119	15	242	225	147	105	239	77	135	248	199	19
90	49	227	93	136	64	247	13	153	88	187	143	6	202	24	252
126	70	11	85	78	50	198	218	168	1	40	53	21	161	97	55

110	174	163	132	26	240	66	57	144	154	230	92	80	4	130	32
177	121	46	18	245	180	108	208	72	14	33	52	16	22	160	176
59	229	0	3	134	236	131	27	206	222	12	169	167	114	122	188
133	111	83	107	98	155	23	113	45	123	226	165	5	224	235	87
47	94	10	17	137	7	9	181	118	223	44	214	217	62	116	42
115	145	141	35	175	212	173	164	71	30	102	67	162	43	151	228
193	8	179	41	171	159	253	36	157	140	186	192	201	158	74	106
205	178	231	54	95	237	58	210	37	76	189	84	190	207	209	81
65	34	142	75	244	61	79	183	246	28	232	221	195	146	91	196
182	29	194	139	120	219	238	101	249	148	100	31	86	241	197	254
255	89	220	138	60	63	56	104	82	20	251	149	51	25	150	112
48	124	184	99	211	203	117	38	73	152	185	69	191	172	170	200

2.3.2. Algebraic and Statistical Analyses of S-box

Several statistical and theoretical approaches are used to investigate the interesting characteristics of S-boxes. This evaluation of the strength of S-box impacts its suitability for usage in various cryptographic methods and for security requirements. [25] provides a concise discussion of a technique that employs differential block cipher features. This cryptanalysis technique is easily applicable to the DES algorithm, many cyphers, and S-boxes [25].

A technique based on information theory can also be used to evaluate the strength of a cipher [29]. This technique uses a variety of criteria to determine the features and connections of input and output bits, including nonlinearity, bit independence criterion and strict avalanche criterion [29]. In addition, approximation probability offers event probability as well as differential uniformity, allowing an iterative approach to be developed.

Tables 2.8 – 2.10 show the tabular form of S-boxes generated with the help of $3D$ mixed chaotic map. Table 2.11 shows the nonlinearity outcomes of the suggested S-boxes in contrast to a variety of well-known S-boxes. The average nonlinearity values for the generated S-boxes can be seen to be better than all other S-boxes, as shown in this table. Furthermore, because the suggested S-boxes' entries are unique and lie in the integral range of 0 to 255, they have the bijection property. Table 2.12 also includes the strict avalanche criterion, bit independence criterion, and linear and differential approximation probabilities. The graphical demonstration of Table 2.12 is provided in Fig. 2.6 to Fig. 2.10.

Table 2.11: Comparison of nonlinearity values

S-boxes	S-box 1	S-box 2	S-box 3	Ref. [28]	Ref. [33]	Ref. [34]	Ref. [35]	Ref. [36]
Average	103.75	104.25	103.75	103.2	103.3	103	105.25	104.7
Minimum	98	102	102	98	99	100	102	102
Maximum	108	106	106	108	106	106	108	108

Table 2.12: Results of standard measures of proposed S-boxes

Substitution boxes	Nonlinearity	SAC	DP	LP	BIC
S-box 1	103.75	0.508	0.0390	0.1562	103.6
S-box 2	105.75	0.498	0.0546	0.1328	103.2
S-box 3	104.25	0.491	0.0468	0.1327	103.6
Ref. [31]	104.7	0.506	0.0469	0.1250	104.1
Ref. [21]	103.2	0.506	0.0469	0.1289	104.2
Ref. [32]	103.3	0.499	0.0391	0.1328	103.3
Ref. [33]	103.2	0.505	0.0391	0.1289	103.7
Ref. [34]	103	0.500	0.0547	0.1289	103.1
Ref. [35]	105.25	0.496	0.0391	0.1562	103.8

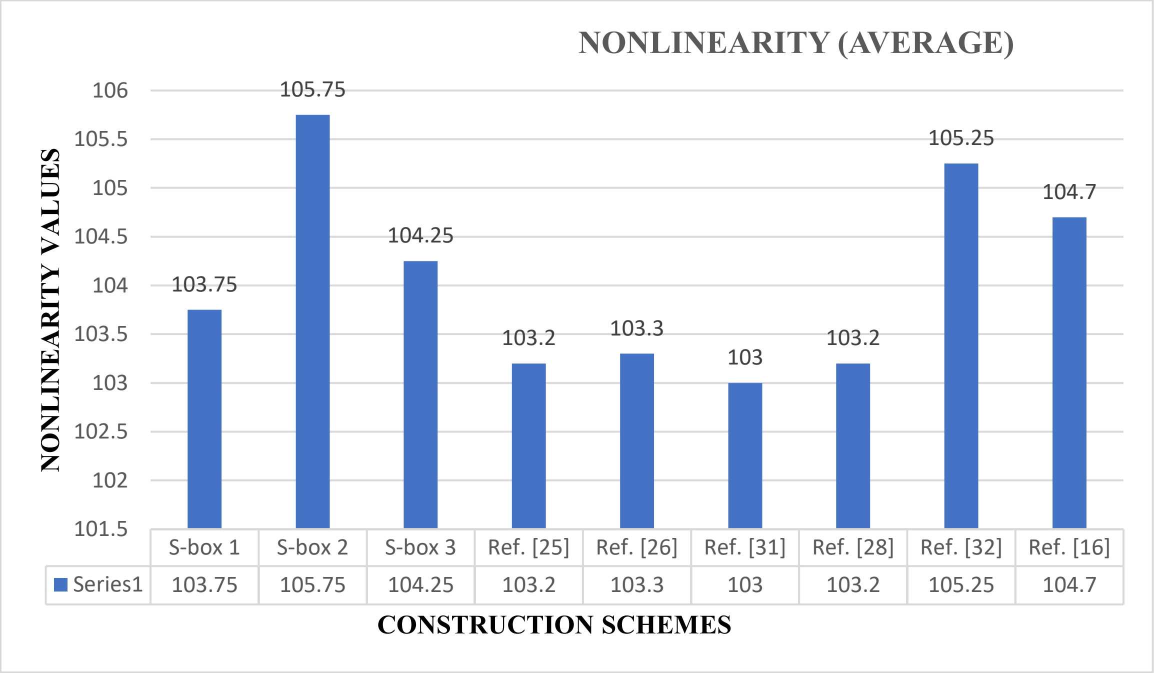


Figure 2.6: Graphic display of Nonlinearities and comparison

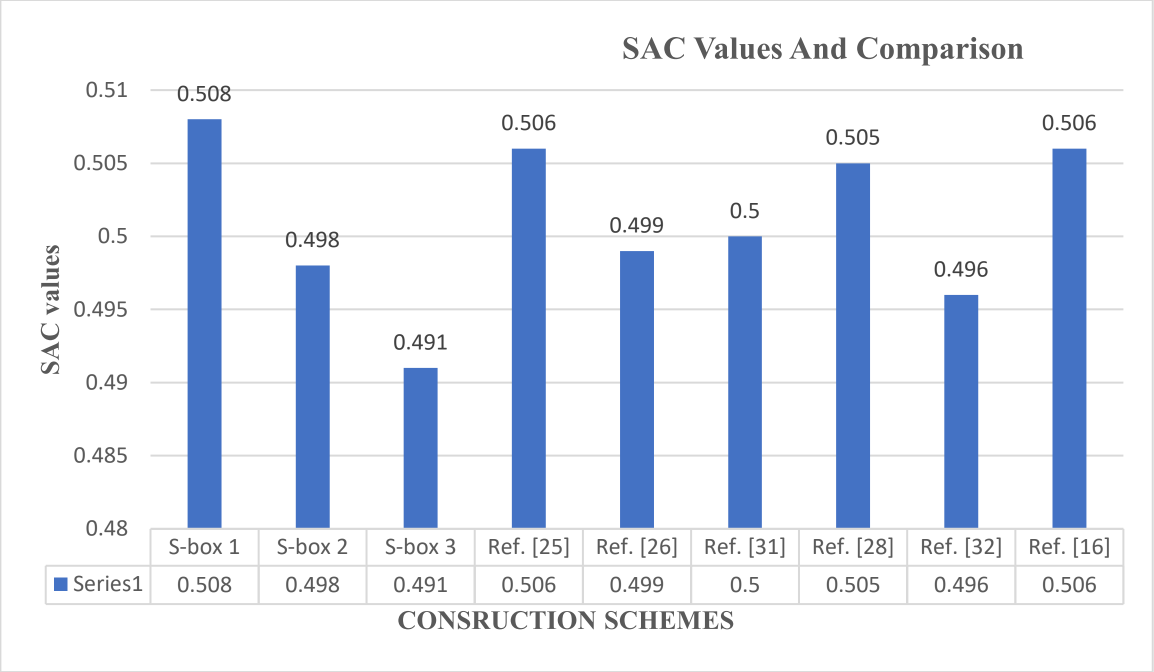


Figure 2.7: Graphic display of SAC values and comparison

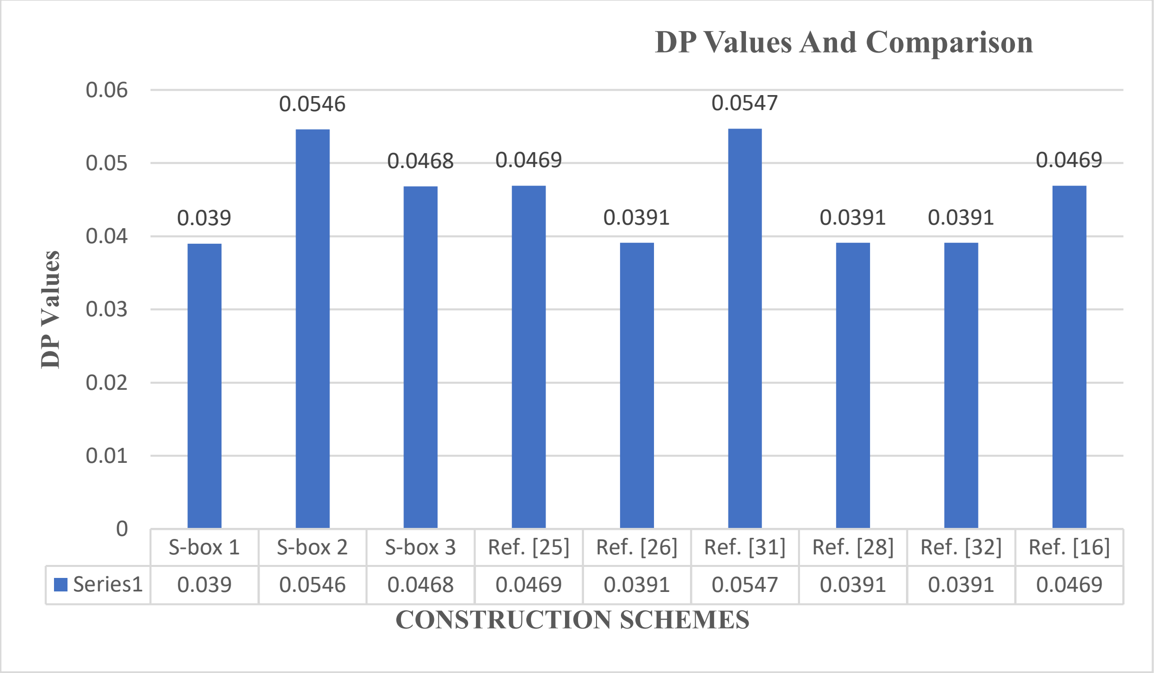


Figure 2.8: Graphic display of DP values and comparison

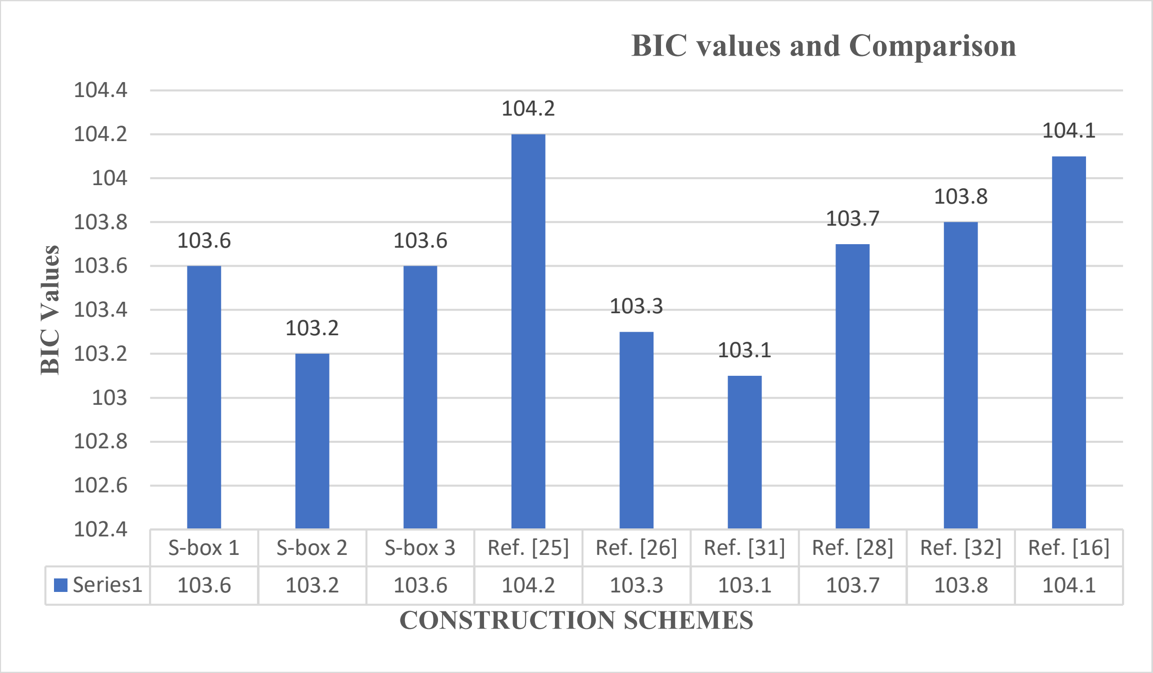


Figure 2.9: Graphic display of BIC values and comparison

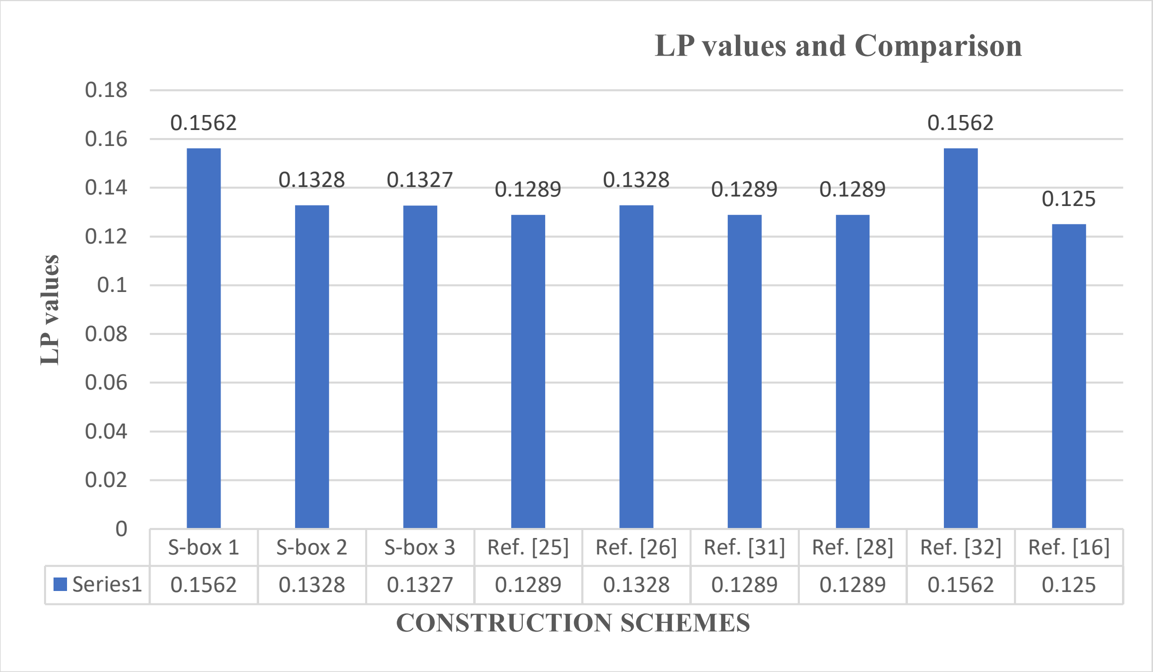


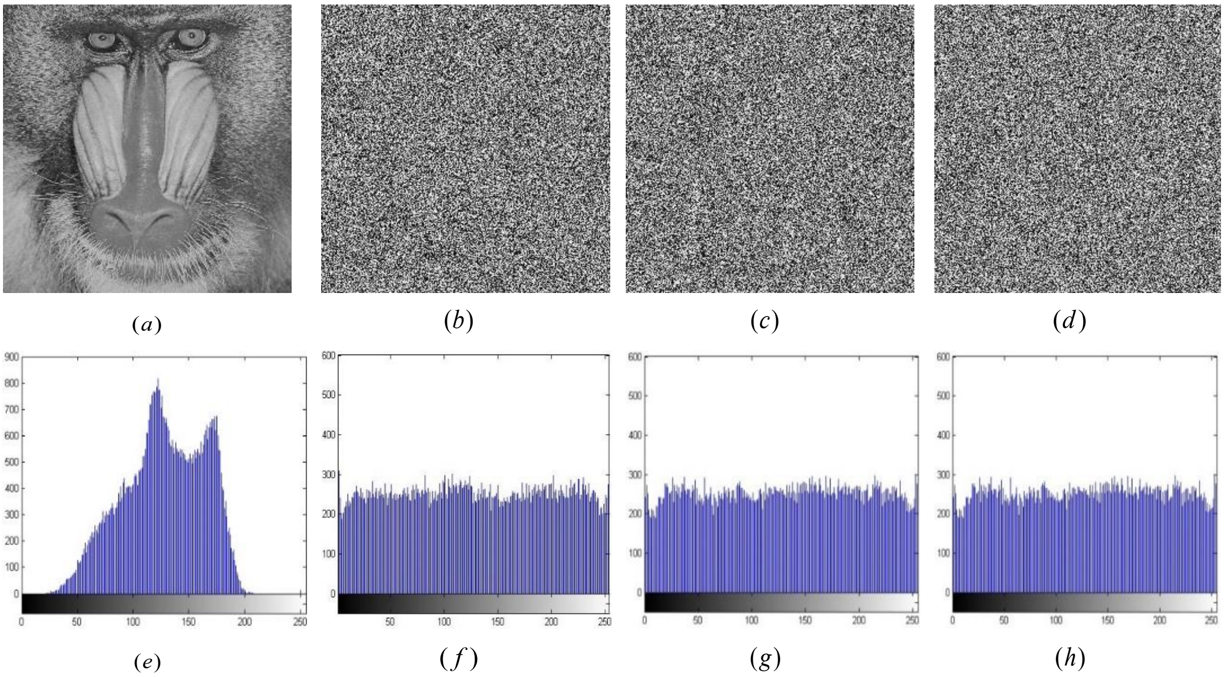
Figure 2.10: Graphic display of LP values and comparison

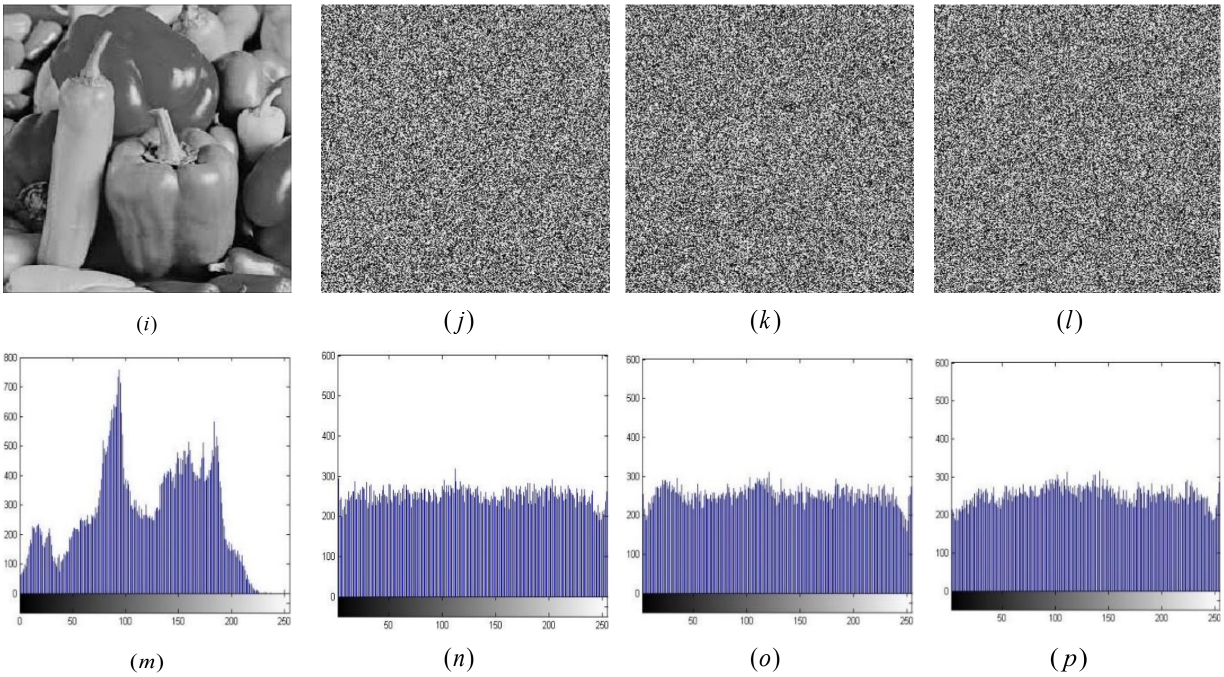
From Table 2.12, it can be noted that the average nonlinearity of newly constructed S-boxes is approximately 105 and the strict avalanche criterion for newly constructed S-boxes is as high as 0.59375. Furthermore, the BIC investigation of the proposed S-boxes has a value of 104. Also, the most serious estimate of the linear approximation of the proposed S-boxes is 168, which proves that the proposed S-boxes have solid counter-capability against direct attacks. The proposed S boxes have a very high probability of variance of 0.01562.

Performance analyses and comparisons show that the proposed S-boxes have almost optimal results when it comes to randomness, and resistance to various linear and different attacks.

2.3.2.1. Majority Logic Criterion

The majority logic criteria (MLC) are discussed briefly in Ref. [36]. This analysis examines the S-box's strength in image encryption applications. Encryption distorts images, which indicate the algorithm's strength. The correlation analysis is the most important method used to compare two images. The higher correlation value enhances the chances of actual information being deciphered by cryptanalysis. Contrast helps identify objects in images. After scrambling the data, the increase in unpredictability leads in a large increase in contrast level. The higher contrast in the encrypted images indicates good encryption. Entropy measures a cryptosystem's randomness. The value of entropy relates to the arrangement of components in a digital image. The homogeneity of entries in the grey level co-occurrence matrix (GLCM) is computed. Energy analysis evaluates the dispersion of energy before and after encryption by computing the sum of square elements in GLCM. Fig. 2.5(*a*) and Fig. 2.5(*c*) illustrate the host and the encrypted images. Fig. 2.5(*b*) and Fig. 2.5(*d*) shows their respective histograms.




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

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

Figure 2.11: Histogram of original and encrypted images using the proposed S-box
2.11(*a-d*): Original and encrypted images of Baboon; 2.11(*e-h*): Histogram of Original and encrypted images of Baboon; 2.11(*i-l*): Original and encrypted images of Pepper; 2.11(*m-p*): Histogram of Original and encrypted images of Pepper.

Table 2.13: Comparison of MLC analysis

Images	Entropy	Contrast	Correlation	Energy	Homogeneity
			Baboon image		
Plain Text	7.5817	0.2752	0.9395	0.1378	0.9132
Proposed 1	7.9723	8.6727	-0.0041	0.0175	0.4065
Proposed 2	7.9823	8.5814	-0.0046	0.0176	0.4089
Proposed 3	7.9829	8.3123	0.0012	0.0181	0.4125
Ref. [20]	7.9562	8.3129	0.0103	0.0180	0.4219
AES [22]	7.9211	7.5509	0.0554	0.0202	0.4662
Belazi [30]	7.9233	8.1423	-0.0112	0.0286	0.4648
Skipjack [37]	7.7561	7.7058	0.1205	0.0239	0.4708

Table 2.13 shows that the MLC findings are also good, showing that the proposed S-box is suitable for the development of cryptographic algorithms for data encryption.

Chapter 3

Image Encryption Application of Block Cipher Improved by 3*D* Chaotic map

This chapter introduces a new hybrid permutation-substitution-based color image encryption system. The permutation and substitution processes are being applied by using an S-box that makes the system extremely diffusing and confusing. To enhance the diffusion and confusion in the algorithm, a 3*D* chaotic map has been used. The permutation box, substitution box, and initial conditions of the 3*D* mixed chaotic map are being used as a key. The stability of the proposed scheme for statistical purposes and differential attacks is also analyzed.

3.1. Introduction

The protection of digital content is increasingly becoming a significant issue for researchers and engineers as millions of digital images are transmitted every second to all corners of the world. Different encryption techniques are thus applied to prevent unauthorized access to such information. These techniques provide considerable convenience for secure transmission over Internet channels.

Research in image encryption has rapidly developed in the last decade, where researchers have produced some ground-breaking work. Some of the relevant research is presented as follows: Wang et al. [38] used Deoxyribonucleic Acid, and Babaei et al. [39] used Recursive Cellular Automata for their effective image masking techniques; a high-speed modified El Gamal encryption algorithm was proposed in [40]. In a later study [41], a controlled alternate quantum walk was used to generate random numbers for a quantum-color image masking technique. Similarly, an image masking technique was developed based on an aperture nonlinear fractional Mellin transform with extreme resistance to known-plaintext and chosen-plaintext attacks [42]. [43] effectively applied the fractional domain, Arnold transforms, DWT, and MSVD to design an image-masking algorithm.

It is vital to scientifically study the fundamental core of the critical problems in image encryption algorithms and then strategize new algorithms. Chaos-based encryption processes are more efficient as compared to other practical techniques. Lorenz was the first to introduce the "Butterfly effect" in 1963. He suggested the Lorenz system used in [38], [44]. Li and Yorke discovered the development from order to chaos precisely in Ref. [45].

Researchers have recently developed several algorithms based on neural networks [46]. In particularly, the pseudo-random number sequences are efficiently generated by employing a composite chaotic map in [46] and a chaotic Hopfield neural network for the permutation and diffusion by bit XOR operation in [47]. The proposed scheme has achieved a high degree of security, but the diffusion portion is not secure enough to withstand plaintext attacks, so the scheme's security has some question marks. The Boltzmann machine is more effective for encryption than neural networks [48], the restricted Boltzmann device is utilized to generate pseudo-random numbers that continuously adjust the weight matrix between the hidden and visible layers. Similarly, the ultimate weight matrix is used as a pseudo-random number matrix [46]. Finally, the XORing bit operation with the plain image accomplishes the encryption. The developed scheme has some faults, like lack of permutation, which weakens the diffusion segment and has a small key space.

Modified fuzzy cellular neural networks were introduced in [49]. Chaotic fuzzy cellular neural networks with high sensitivity efficiently provide plaintext sensitivity and key sensitivity. The major drawbacks of this algorithm are the absence of a permutation process and the slow rate of encryption/decryption [46]. The image encryption scheme in [50] is known as the Chaotic Neural Network (CNN), has two phases (3-layer neurons). These phases are named the chaotic neuron layer and the permutation neuron layer and are used in the diffusion part and the permutation part of image pixel values, respectively. Lusystems, Chua, and Lorenz bring in the bias vector of the chaotic neuron layer and weight matrix, and a tent map is used as the activation function. In the permutation of the neuron layer, a cat map is utilized for scrambling the pixel position. This is applicable to limited image types and the tent map has a low degree of nonlinearity. Further, the diffusion phase weakens the security of the overall algorithm.

In Ref. [51], [52], Huang et al., and Lidong et al., proposed double-image encryption and triple-image compression encryption algorithms based on chaotic systems, S-boxes, compression, and interpolation. In Ref. [53], Patro et al. presented a multi-color image encryption scheme through a multi-level scrambling operation. Moreover, the hash value of the image has been linked with the integrated PWLCM system to improve the security of the encryption scheme. Although Patro's scheme improves encryption efficiency to some extent, it does not consider compressing more vivid images to reduce storage space and transfer costs.

The encryption schemes in these articles focus on one aspect out of two (confusion & diffusion). Confusion is obtained by a substitution process, while for diffusion, chaotic maps and permutations are used. A highly secure scheme has a balance of confusion and diffusion.

3.2. Proposed Encryption Scheme-I (PES-I)

The proposed multi-image encryption scheme is explored in this section. The scheme is based on the chaotic map and is described by four modules.

3.2.1. Combine images and RGB channels

3.2.2. Permutation of the combined RGB channels

3.2.3. Construction of substitution boxes

3.2.4. Substitution of permuted RGB channels

Now we discuss these modules one by one hereunder:

3.2.1. Combine Images and RGB Channels

Let $I_1, I_2, I_3,$ and I_4 be the RGB images of dimension $M \times N \times 3$. Initially, the scheme merges each color component of the images I_i for $1 \le i \le 4$ into a single matrix. Then combine the Color components to produce a single image I_m of dimension $2M \times 2N \times 3$. Once obtained, this matrix is processed through the following modules to encrypt the image I_m.

3.2.2. Permutation of RGB Channels

In digital images, up to fifteen neighbouring pixels are highly correlated; therefore, a well-organized pattern should destroy the pixel intra-correlation. This module permutes the pixel's position of the combined image (single image) using the map given in Eq. (2.1) to Eq. (2.3) in chapter 2. To mix the data of each image in a nonlinear manner, the chaos generated by the suggested nonlinear map is used in the permutation process. The mathematical representation of the permutation process is given in four cases as follows.

2.3.2.1. Row-Wise Permutation

Case I

$$I_p(u,v) = I(u - x_u, v) \tag{3.1}$$

if $u - x_u \ge 1$ and $x_u = 2q$ for some $q \in \mathbb{Z}$

Case II

$$I_p(u,v) = I(u + M - x_u, v), \tag{3.2}$$

if $u - x_u < 1$ and $x_u = 2q$ for some $q \in \mathbb{Z}$

Case III

$$I_p(u,v) = I(u - x_u, v), \tag{3.3}$$

if $u - x_u \le M$ and $x_u = 2q + 1$ for some $q \in \mathbb{Z}$

Case IV

$$I_p(u,v) = I(u + x_u - M, v) \tag{3.4}$$

if $u - x_u > M$ and $x_u = 2q + 1$ for some $q \in \mathbb{Z}$

2.3.2.2. Column-Wise Permutation

Case I

$$I_p(u,v) = I(u - x_u, v) \tag{3.5}$$

if $u - x_u \ge 1$ and $x_u = 2q$ for some $q \in \mathbb{Z}$

Case II

$$I_p(u,v) = I(u + M - x_u, v), \tag{3.6}$$

if $u - x_u < 1$ and $x_u = 2q$ for some $q \in \mathbb{Z}$

Case III

$$I_p(u,v) = I(u - x_u, v), \tag{3.7}$$

if $u - x_u \le M$ and $x_u = 2q + 1$ for some $q \in \mathbb{Z}$

Case IV

$$I_p(u,v) = I(u + x_u - M, v) \tag{3.8}$$

if $u - x_u > M$ and $x_u = 2q + 1$ for some $q \in \mathbb{Z}$

$I(u,v)$ and $I_p(u,v)$ denotes the pixel values of the original and the permuted image, respectively.

All pixel values in the original image are row-wise permuted, followed by a column-wise permutation, depending on the value of the chaotic sequence. The consequent matrix is represented by I_p. In this scheme, the column-wise permutation process is the same as the row-wise permutation. However, a different approach for the two permutations can be used to induce further complexity.

3.2.3. Construction of Substitution Boxes

The substitution box is an essential part of any symmetric key cryptographic scheme. Therefore, this module generates an S-box and then uses it for the substitution. The S-box construction procedure is given as.

$$y_i^{''} \equiv y_i \bmod 256 \tag{3.9}$$

Defined a map:

$$S : y_i^{''} \rightarrow \mathbb{Z}_{256}$$

$$S(y_i^{''}) = \begin{cases} y_i^{''} & \text{if } y_i^{''} \neq S, \ \forall \ 1 \leq j \leq i\text{-}1 \\ 0 & \text{if } y_i^{''} = S, \exists \ 1 \leq j \leq i\text{-}1 \end{cases} \tag{3.10}$$

The map *S* is an onto map that contains random numbers from 0 to 255. For a different value of the initial condition and the parameter, the scheme generates different S-boxes which preserve all the cryptographic properties.

3.2.4. Substitution of Permuted RGB Channels

In the last module, the substitution is performed through the S-boxes generated in module III via the AES substitution method. The resultant image is encrypted I_e.

The flowchart of the scheme, the results of the combined and individual encrypted images are demonstrated in Fig. 3.1 to Fig. 3.3, respectively.

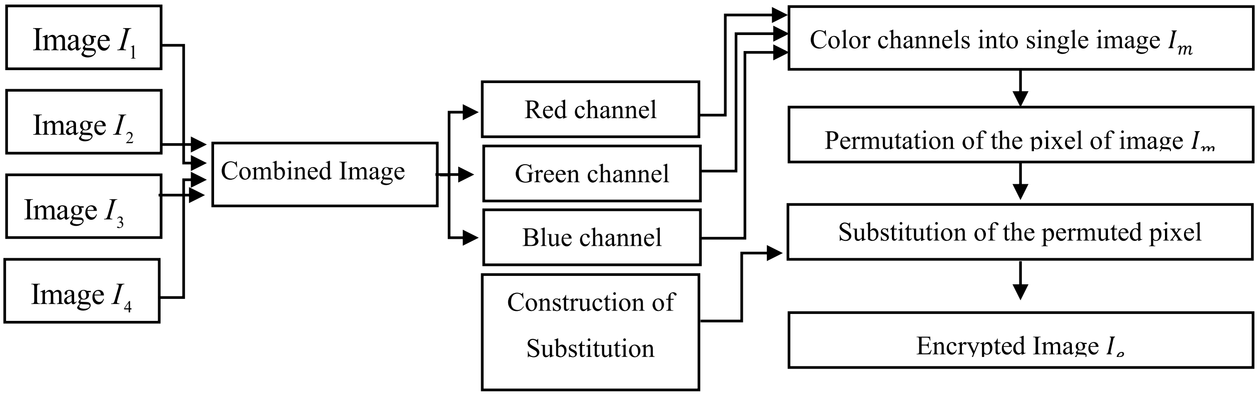


Image I_1
Image I_2
Image I_3
Image I_4
Combined Image
Red channel
Green channel
Blue channel
Construction of Substitution
Color channels into single image I_m
Permutation of the pixel of image I_m
Substitution of the permuted pixel
Encrypted Image I_e

Figure 3.1: Flow chart of the encryption process

Fig. 3.2 shows that the ciphered and original images have no relationship, but later the decryption gives the original image. In Fig. 3.3, the original, permuted, and ciphered images of Lena, Mandrill, Peppers, and Deblur are provided. Both figures demonstrate that the scheme has exceptional encryption and decryption properties.

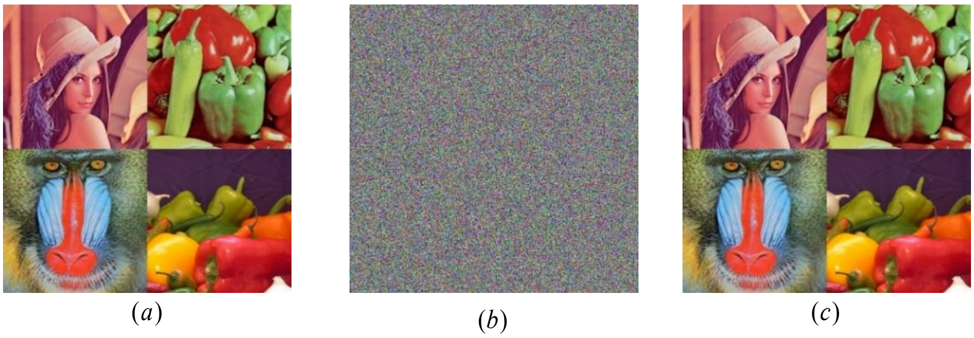


Figure 3.2: Encryption outcomes, 3.2(*a*): Plain image; 3.2(*b*): Encrypted image; 3.2(*c*): Decrypted image

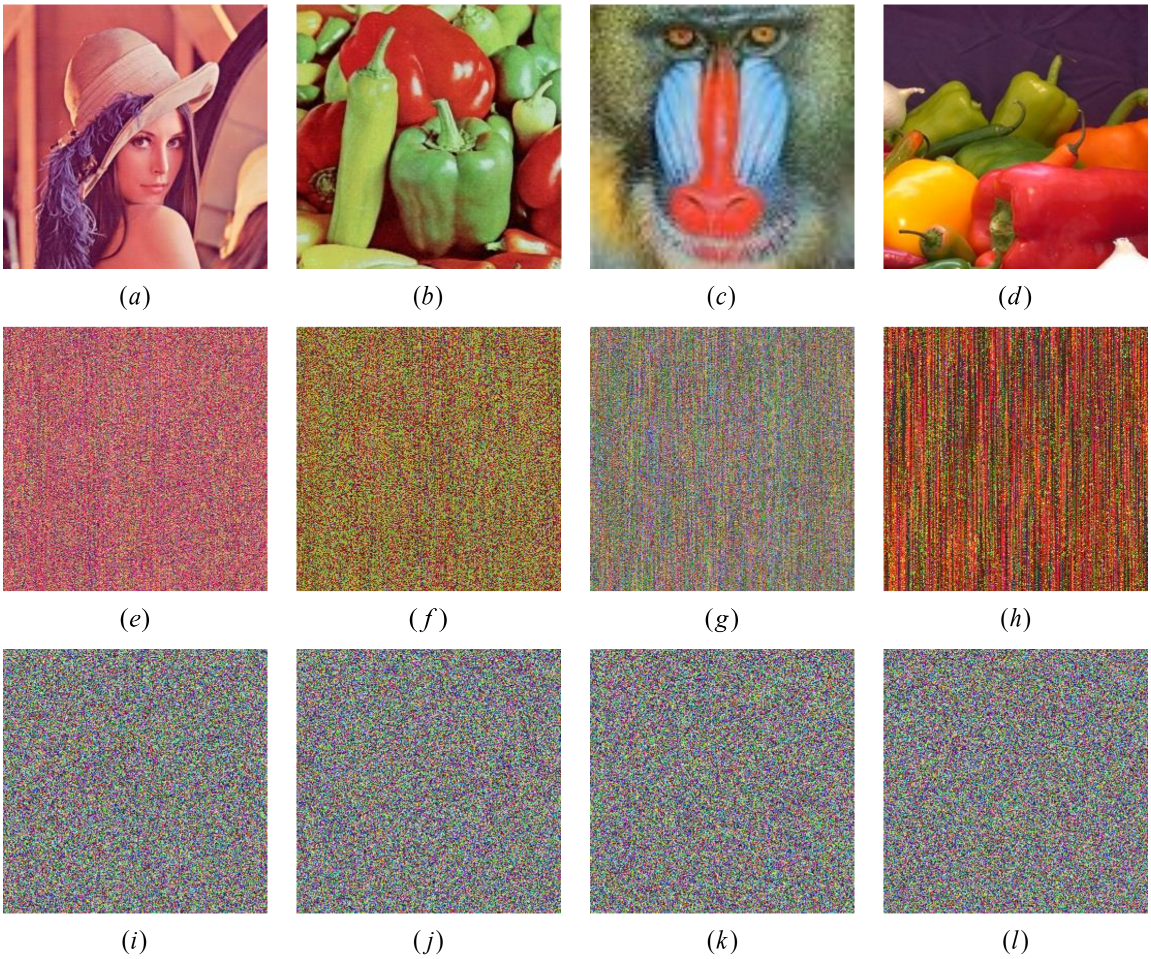


Figure 3.3: Experimental outcomes.
3.3(*a-d*): Plain images; 3.3(*e-h*): permuted images; 3.3(*i-l*): encrypted images

3.3. Simulation Results and Analyses

In this work, standard Color images of "Lena", "Peppers", "Mandrill", and "Deblur" have been used as test images.

The combined multi-image, its ciphered and deciphered images are provided in Fig. 3.2(*a*), Fig. 3.2(*b*), and Fig. 3.2(*c*), respectively. Furthermore, individual plain images, their permuted and ciphered images are displayed in Fig. 3.3(*a-d*), Fig. 3.3(*e-h*) and Fig. 3.3(*i-l*), respectively. For the execution of both the encryption and decryption process, the computerized simulations are conducted in MATLAB R2013a (8.1.0.604).

3.3.1. Security Analyses

To examine the security strength of the proposed scheme, we performed different analyses on it. The detail of these analyses on the proposed scheme is discussed critically.

3.3.1.1. Histogram Analysis

The histogram analysis is presented to evaluate the uniform distribution of ciphered [54]. A cryptosystem has a high resistance to statistical attacks if the probability of each gray value in the uniform histogram is the same [54].

In Fig. 3.4, the original, the ciphered, and their corresponding histograms of the multi-image and single images are displayed. These histograms demonstrate that the pixels of the ciphered images are more evenly spread than the original images. This aspect ensures that the proposed scheme has high resistive capability against differential, plaintext, and statistical attacks.

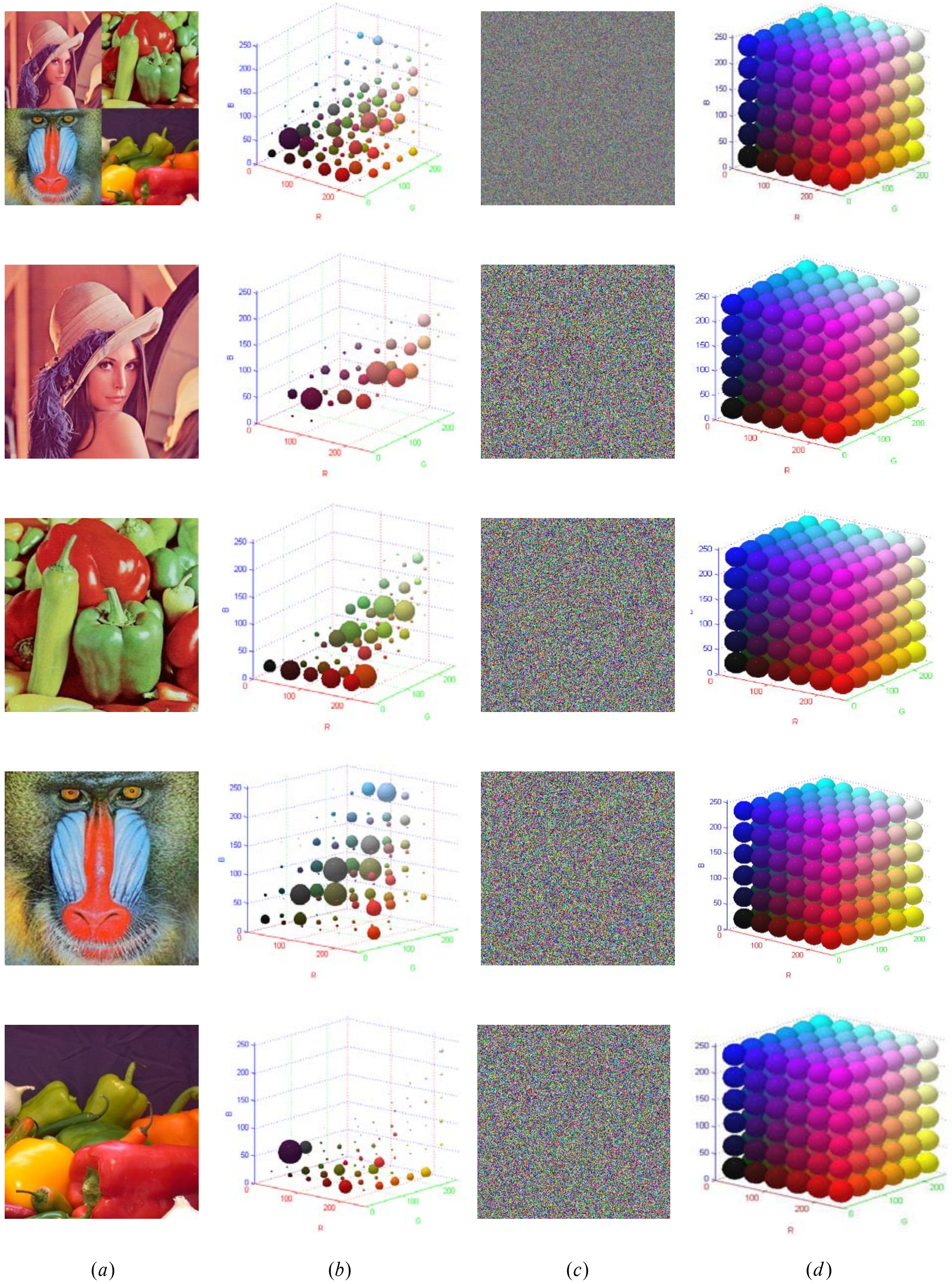


Figure 3.4: Histogram of original and encrypted images.
3.4(*a*): plain images; 3.4(*b*): corresponding histograms; 3.4(*c*): encrypted images; 3.4(*d*): corresponding histograms

3.3.1.2. Key Sensitive Analysis

The key plays a vital role in testing the strength of the encryption scheme [55]. A cryptosystem has a high key sensitivity if the decryption with slightly different key outputs different images instead of plain images [56].

To appraise the key sensitivity of the suggested scheme, two keys K_1 and K_2 which are slightly different from each other are compared. The Lena test image is encrypted using K_1 and K_2. The demonstration is provided in Fig. 3.5. The plain image is given in Fig. 3.5(*a*). The encryption of plain images with K_1 and K_2 are given in Fig. 3.5(*b*) and Fig. 3.5(*c*) respectively. The difference between encrypted images is given in Fig. 3.5(*d*). During the decryption of Fig. 3.5(*b*) with key K_1, the original image is obtained, but this is not the case with key K_2, where the obtained image is shown in Fig. 3.5(*f*). Likewise, during the decryption of Fig. 3.5(*c*) with key K_1, the obtained image is shown in Fig. 3.5(*g*) which is not same as the original image, at the same time we obtain the original image with key K_2. This analysis ensures the capability of the scheme to yield different ciphered images when encryption is performed with slightly different keys.

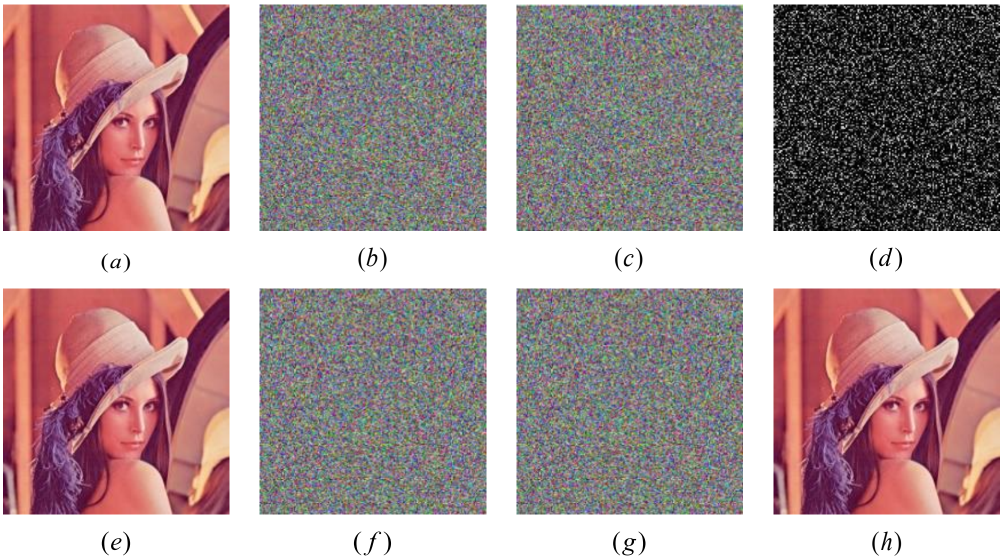


Figure 3.5: Key sensitive analysis

3.2.1.3. Keyspace Analysis

It is important to test the brute force attack to test the security strength of the cryptosystem [57]. A cryptosystem can withstand a brute force attack if its key space is greater than $110^{30} \approx 2^{100}0^{30} \approx 2^{100}$. Assume that the precision of the computer is 10^{15}. The keys of the $3D$

chaotic map given in Eq. (2.1) to Eq. (2.3) are $x_1, y_1, z_1, \psi, \mu, \lambda$ and σ. Thus, the key space has a total of $10^{105} \approx 2^{348}$ possibilities. It shows that the key space of the proposed scheme is enormous in its ability to withstand the brute force attack.

3.2.1.4. Time Execution Analysis

The time required for algorithm execution is also of critical importance to test the value of a cryptosystem [58]. The proposed algorithm is tested on a machine with the following specs: Intel(R) Core (TM) i3-4010U processor @ 1.70GHz; 4.00 GB RAM; and Windows 10 Enterprise. For the execution of both the encryption and decryption process, the computerized simulations are conducted in MATLAB R2013a (8.1.0.604). The time taken to encrypt the RGB Test image is 19.922 seconds.

3.3.2. Statistical Analyses

The key point of the proposed work is to transmute visually meaningful images into noise-like encrypted images. Several statistical analyses are used to evaluate the noise-like encrypted images. The noise analysis, information entropy, correlation analysis, and differential attacks are presented hereunder.

3.3.2.1. Noise Analysis

When exposed to some noise in the transmission, the behaviour of the cipher scheme is of critical importance. Rarely, there is some noise in the broadcast channel. As a result, the encrypted image gets affected severely, and the cryptosystem failed to recover the image [59]. Hence, a cryptosystem is strong if it has image retrieval property even if there is noise. Here, the effectiveness of the proposed scheme is analyzed.

Consider the analysis of fat-tail distribution, also known as salt and pepper noise [59]. There are bright pixels in the dark and dark pixels in the bright in this type of noise. In Fig. 3.6, encrypted and decrypted images of Lena, Baboon, Fruits, and Airplane with increment in noise are given. The proposed scheme can recover the original image in each case of noise. The encrypted and decrypted images with minimum, default, and maximum noise are given in Fig. 3.6 (*a-c*) and Fig. 3.6 (*d-f*) respectively.

3.3.2.2. Randomness Test

The security level of a cryptosystem can be determined by finding its distribution, complexity, period, and output data. A cryptosystem is safe if the data is evenly distributed, so it exhibits high complexity and durability [60]. In this chapter, NIST SP 800–22 test is performed on a multi-image. There are also some subcategories in this test. Test results show that the encrypted test image using the proposed scheme passes all the security threats. The NIST test results are presented in Table 3.1.

Table 3.1: NIST test results

Test		**P – values (Encrypted Image)**			**Result**	
		Red	**Green**	**Blue**	**Random**	**Non-random**
Frequency		0.49672	0.81027	0.24957	☑	
Block Frequency		0.2314	0.03474	0.79895	☑	
Rank		0.28911	0.29892	0.29781	☑	
Runs (M=10,000)		0.81517	0.96785	0.74577	☑	
Long Runs of ones		0.7126	0.7126	0.7126	☑	
Overlapping Templates		0.86598	0.82166	0.85789	☑	
No Overlapping Templates		0.99326	0.99819	0.99628	☑	
Spectral DFT		0.25474	1	0.47686	☑	
Approximate Entropy		0.052736	0.70132	0.6312	☑	
Universal		0.98108	0.99878	0.99115	☑	
Serial	p values 1	0.029565	0.19870	0.13674	☑	
Serial	p values 2	0.003765	0.03782	0.15076	☑	
Cumulative Sums Forward		0.093897	0.23879	0.10914	☑	
Cumulative Sums Reverse		1.1715	0.61785	0.91678	☑	
Random Excursions	$X = -4$	3.45E-15	0.23178	0.62765	☑	
	$X = -3$	0.59549	0.00343	0.61652	☑	
	$X = -2$	0.01279	0.5343	0.93581	☑	
	$X = -1$	0.7138	0.81799	0.93472	☑	
	$X = 1$	0.91818	0.9402	0.01759	☑	
	$X = 2$	0.97863	0.89732	0.87874	☑	
	$X = 3$	0.99435	0.034587	0.56754	☑	
	$X = 4$	0.9895	0.031562	0.63204	☑	
Random excursions variants	$X = -5$	0.13454	0.32821	0.30243	☑	
	$X = -4$	0.70664	0.28653	0.62678	☑	
	$X = -3$	1	0.19349	1	☑	
	$X = -2$	0.78392	0.17659	0.83415	☑	

	$X=-1$	0.62617	0.19947	0.89837	☑
	$X=1$	0.31843	0.34674	0.30262	☑
	$X=2$	0.5726	0.48946	0.37325	☑
	$X=3$	0.66354	0.74845	0.19643	☑
	$X=4$	0.71657	0.83143	0.05465	☑

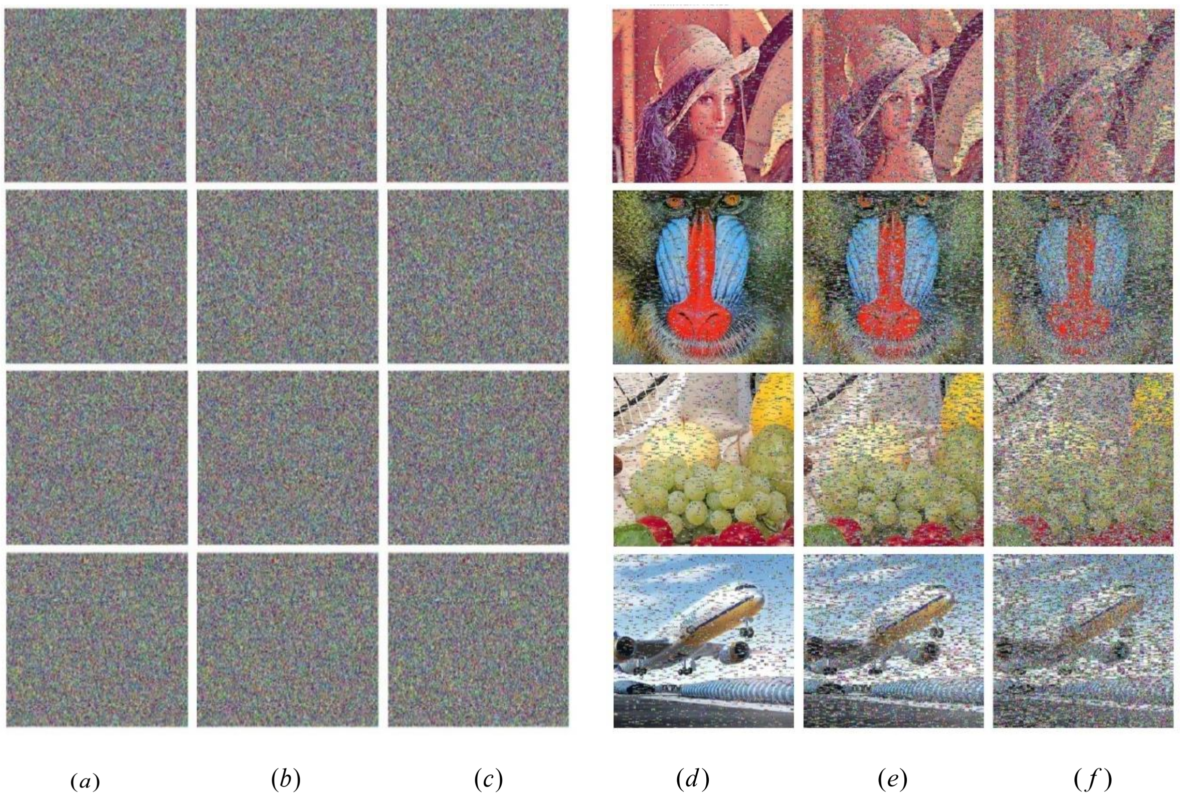


Figure 3.6: Noise Analysis

3.3.2.3. Information Entropy Analysis

Entropy estimates the strength of a cryptographic scheme in terms of how much it can disorganize the encrypted image [54], [61]. It measures the degree of randomness of an encryption scheme [62]. The expression to compute the degree of randomness is given as [54].

$$H(m) = -\sum_{u=0}^{255} p(m_u)\log_2 p(m_u) \tag{3.11}$$

m and $p(m_u)$ are the unique random variable and probability of m_u.

A cryptosystem has a high degree of randomness if its entropy estimation is 8. The entropy analysis of the original and the ciphered image is presented in Table 3.2. Note that the randomness of the ciphered image is in proximity to the optimum value. Consequently, the suggested scheme can randomize the pixels to their optimum level.

Table 3.2: Information entropy analysis

Test Image	Information entropy (Original)			Information entropy (Encrypted)		
	Red	Green	Blue	Red	Green	Blue
Combine	7.7599	7.6978	7.6571	7.9991	7.9954	7.9963
Lena	7.3277	7.6048	7.1326	7.9977	7.9945	7.9943
Peppers	7.3920	7.3920	7.1738	7.9965	7.9969	7.9932
Deblur	7.6646	7.1724	6.4954	7.9971	7.9957	7.9949
Mandrill	7.6634	7.3871	7.6646	7.9967	7.9931	7.9939

3.3.2.4. Correlation Analysis

It examines the strength of the encryption scheme to determine how much it can break the relationship of neighbouring pixels [63]. In the plain image, the adjacent pixels are highly correlated. A good encryption scheme can break this relationship [61]. Two thousand pairs are randomly chosen to analyze adjacent correlation coefficients. The following expressions are used to calculate the correlation coefficient.

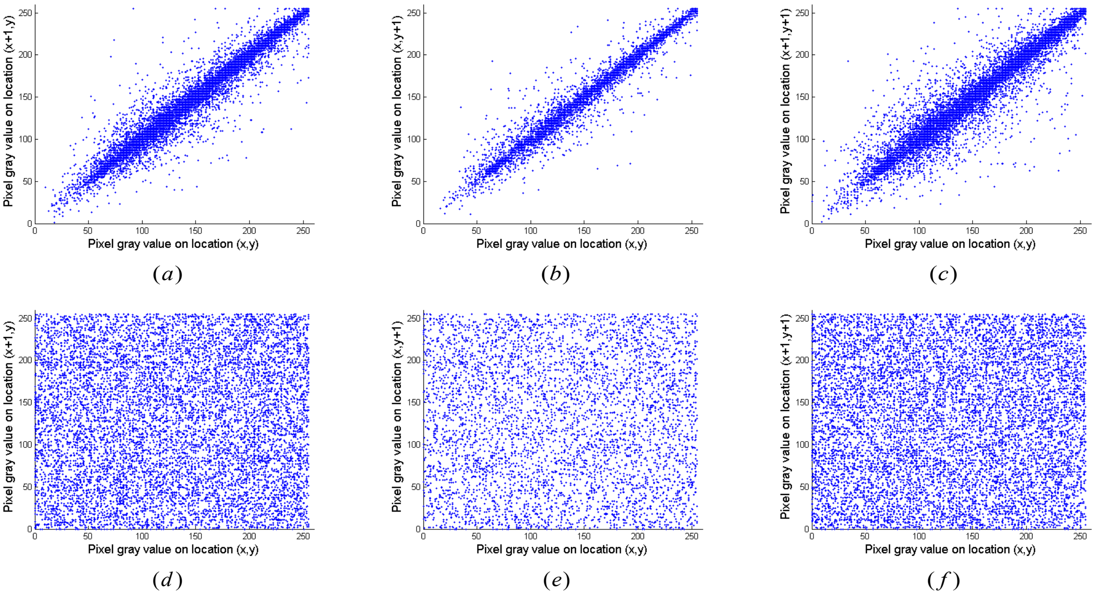
$$r_{u,v} = \frac{E((u-E(u))(v-E(v)))}{\sqrt{D(u)D(v)}}, \tag{3.12}$$

$$E(u) = \frac{1}{N}\sum_{i=1}^{N} u_i, \tag{3.13}$$

$$D(u) = \frac{1}{N}\sum_{i=1}^{N} (u_i - E(u))^2, \tag{3.14}$$

$E(u)$ and $D(u)$ are the mathematical expectation and covariance [54].

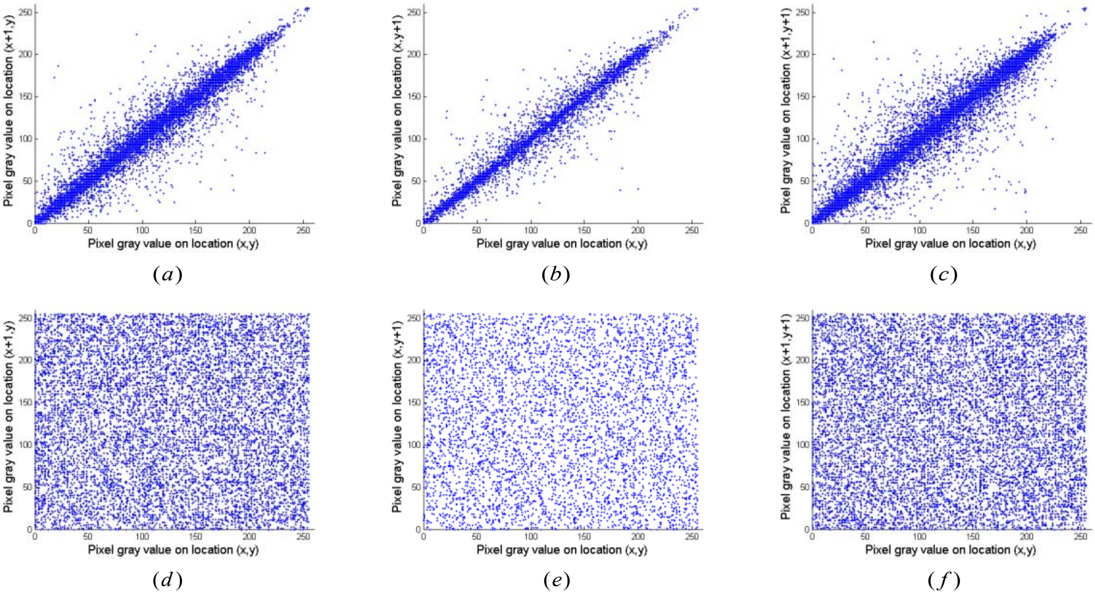
A cryptosystem has more strength if its correlation estimation is 0. The original image correlates close to 1 and the correlation of our test images is close to 0. This suggests that the proposed scheme is capable to break the relationship of adjacent pixels. The results of the correlation analysis of the original and the ciphered images are provided in Fig. 3.7(A) to Fig. 3.7(C), and Table 3.3. In Fig. 3.7(A) to Fig. 3.7(C), (*a-c*) and (*d-f*) represent the horizontal, vertical, and diagonal correlation of original and encrypted images, respectively.



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

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

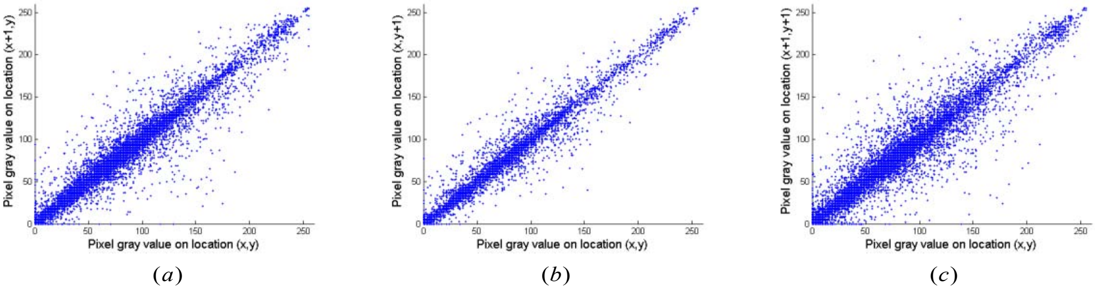
Figure 3.7(A): The correlation coefficient (red channel)



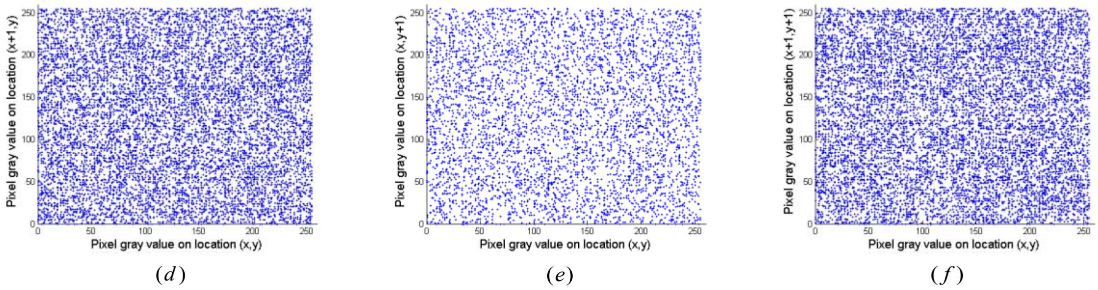
(*a*) (*b*) (*c*)

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

Figure 3.7(B): The correlation coefficient (green channel)



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



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

Figure 3.7(C): The correlation coefficient (blue channel)

Table 3.3: Correlation analysis

Test Image	Correlation (Original)			Correlation (Encrypted)		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Combine	0.9724	0.9718	0.9386	0.0016	-0.0056	0.0015
Lena	0.9452	0.9438	0.9048	-0.00243	-0.00187	-0.00254
Peppers	0.9369	0.9272	0.9637	-0.0174	-0.0105	-0.0241
Deblur	0.9848	0.9903	0.9825	-0.0291	-0.0014	-0.0149
Mandrill	0.9419	0.9656	0.9114	0.0065	-0.0187	-0.0054

3.3.2.5. Differential Attacks

The association between the pixels of the plain image and the ciphered image is evaluated by the NPCR and UACI analyses [54].

A cryptosystem is secure if it is highly sensitive to minor changes in input. Suppose C_1 and C_2 are two ciphers of plain images. The following expressions are used to calculate NPCR and UACI.

$$NPCR = \frac{1}{W \times H}\left[\sum_{u,v} D(u,v)\right] \times 100\%, \tag{3.15}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{u,v} \frac{C_1(u,v) - C_2(u,v)}{255}\right] \times 100\%, \tag{3.16}$$

$C_1(u,v)$ is the gray pixel value of the cipher image [54].

$$D(u,v) = \begin{cases} 1 & C_1(m,n) \neq C_2(m,n) \\ 0 & otherwise \end{cases}, \tag{3.17}$$

These analyses are evaluated, and the findings are presented in Table 3.4. These findings indicate the suggested scheme's high resistance to differential attacks.

Table 3.4: NPCR and UACI results

Schemes	NPCR			UACI		
	Blue (%)	Green (%)	Red (%)	Blue (%)	Green (%)	Red (%)
Combine	99.6063	99.6017	99.5997	33.3846	33.4102	33.2960
Lena	99.5925	99.5921	99.5917	33.0371	33.3102	33.0319
Peppers	99.6014	99.6174	99.6275	33.1504	33.0761	33.2046
Deblur	99.6032	99.6051	99.5961	33.5202	33.2466	33.2779
Mandrill	99.5809	99.5992	99.5975	33.4076	33.1655	33.2769

3.3.2.6. Comparisons

The experimental findings of Entropy, Correlation coefficient, NPCR, and UACI of the suggested scheme are compared with some existing schemes in Table 3.5. Note that the entropy of the ciphered image is too close to the optimum value. Consequently, the suggested scheme is considerably more secure and has more strength. The results of NPCR and UACI of the ciphered image are 99.61% and 33.40%, respectively. These results indicate that the suggested scheme has a high resistance to differential attacks. The correlation coefficient values are very close to the optimal value. This indicates that the suggested scheme is better than the techniques shown in comparison. Hence it is highly secure.

Table 3.5: Comparison of experimental findings with some existing techniques

Measures	Channels	Proposed	Ref. [64]	Ref. [65]	Ref. [66]	Ref. [67]	Ref. [68]	Ref. [69]
Entropy	Red	7.9984	7.9974	7.9971	7.9798	7.9895	7.9913	7.9874
	Green	7.9987	7.9969	7.9969	7.9795	7.9894	7.9914	7.9872
	Blue	7.9989	7.9979	7.9962	7.9797	7.9894	7.9916	7.9866
NPCR	Red	99.6163	99.623	99.5864	99.5925	99.6369	99.6113	99.5990
	Green	99.6170	99.606	99.2172	99.5921	99.6174	99.6060	99.5777
	Blue	99.6259	99.652	99.8474	99.5927	99.6054	99.6052	99.5990
UACI	Red	33.6476	33.245	33.4834	33.5039	33.8547	33.4280	33.4808
	Green	33.6116	33.362	33.6399	33.5112	33.7619	33.4966	33.1617
	Blue	33.6068	33.521	33.2689	33.5037	33.6046	33.3779	33.6066
Correlation	Horizontal	-0.00243	-0.0009	0.0054	0.0037	0.0023	-0.0080	-0.0580
	Vertical	-0.00187	-0.0011	0.0062	0.0030	-0.0059	0.0098	-0.0024
	Diagonal	-0.00254	-0.0010	0.0017	-0.0029	0.0029	-0.0058	-0.0170

3.3. Proposed Image Encryption Scheme-II (PES-II)

At this stage, the second proposed encryption scheme is being explored. This proposed scheme consists of three modules. The flowchart of the proposed scheme is set out in Fig. 3.8, and then the module-wise process of the scheme is provided.

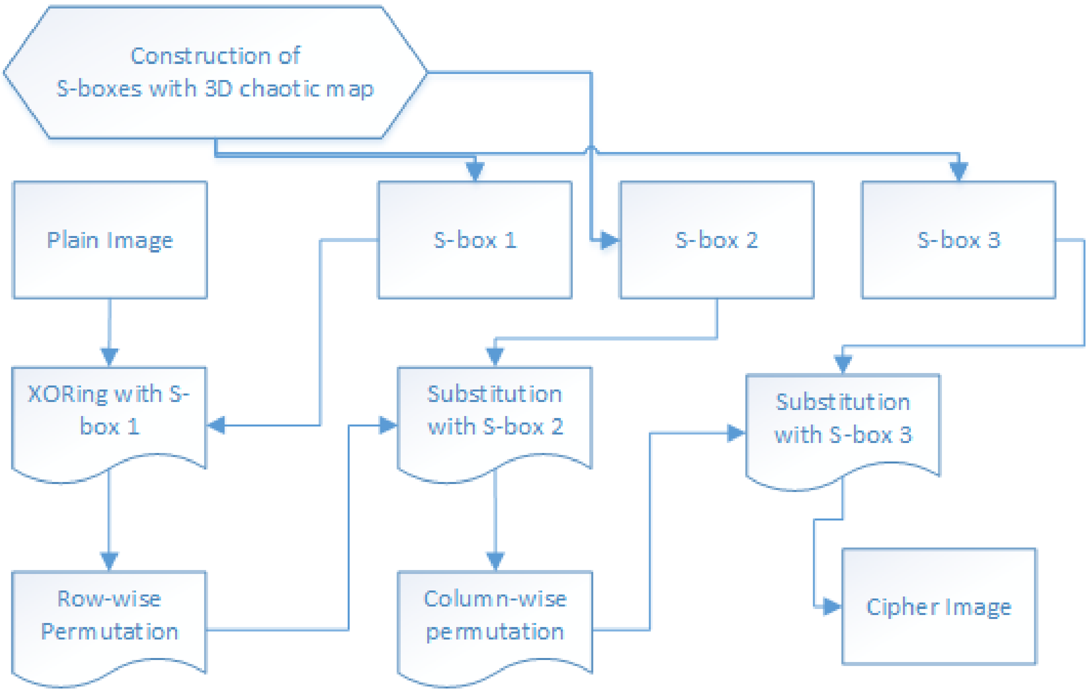


Figure 3.8. Flowchart of the proposed encryption scheme

The modules of the proposed scheme can be described as following.

Before the first module of the proposed scheme, a newly designed 3*D* mixed chaotic map is used for the construction of three S-boxes discussed in chapter 2. Due to proposed S-boxes, the confusion and diffusion in the plaintext are enhanced, which makes it a challenge for the cryptanalyst to determine any information in the encryption process. It is found that the proposed S-boxes with an increasing level of turbulence provide excellent results in any application for secure communication.

Module 1 The first module of the proposed scheme transforms the plain image into bits. After transformation, the *XOR* operation is performed on the plain image bits and one of the constructed substitution boxes.

Module 2 In this module, row wise permutation is performed on the result of the module 1. Here, one of the remaining two substitution boxes is used for the substitution of row-wise permuted bits.

Module 3 In the last module of the scheme, column wise permutation is performed on resulted bits of module 2. Here, third substitution box is used for the substitution of column-wise permuted bits. The result of this step is the final encrypted image.

Here is a description of the functionality of the module 1, 2, and 3.

3.3.1. Pixel Mixing

Assume $I(i, j)$ be the $S \times T$ dimensional plain image. Here i and j indicate the position of the pixels on the X-axis and Y-axis respectively. In the pixel mixing phase, firstly S-box 1 (S_1) is produced through Eq. (2.11). We have to find out the biggest random number in S_1. Let $S \times T$ be the required biggest random number in S_1. After this, the XOR operation is performed on the pixels of the image with each entry $p_k \in S_1$.

$$I_p(i, j) = I(i, j) \oplus p_k = I(i \oplus p_k, j \oplus p_k), \tag{3.18}$$

where $I_p(i, j)$ represents the image pixels after XORing with S_1 entries. We have utilized the XOR operation for bits because this operation is self inverse.

3.3.2. Row-wise Pixel Permutation

In this module, we produced S-box 2 (S_2) through Eq. (2.12). Considering S the biggest number in S_2. The equation used for this phase is given below:

$$I(i, j) = \begin{cases} i + p_k & \text{if } i + p_k \leq S \\ i + p_k - S & \text{if } i + p_k > S \end{cases}, \tag{3.19}$$

Where $p_k \in S_2$, $1 \leq i \leq S$. In this chapter, we have applied row-wise permutation on pixel locations. To increase the security of the scheme, corresponding to odd (resp. even) values of chaos, permutation can apply on pixels positions from right (resp. left) directions.

3.3.3. Column-wise Pixel Permutation

In this module, we produced S-box 3 (S_3) through Eq. (2.13). Considering T the biggest number in S_3. The equation used for this phase is given below:

$$I_e(i, j) = \begin{cases} j + p_k & \text{if } j + p_k \leq T \\ j + p_k - T & \text{if } j + p_k > T \end{cases}, \tag{3.20}$$

where $p_k \in S_3$, $1 \leq j \leq T$. To make the scheme extra protected, corresponding to odd (resp. even) values of chaos, permutation can apply on pixels position from upward (resp. downward) directions.

After performing these four steps, the output image has all cryptographic assets for a secure system.

3.4. Simulation Results and Analyses

In this subsection, we present a security analysis that includes histogram analysis, key sensitivity analysis, and statistical analysis that includes data entropy analysis, correlation analysis, and differential attack analytics of the proposed encryption scheme. Each analysis includes a discussion demonstrating the dominance of the proposed scheme. The encryption of the color image is given in Fig. 3.9.

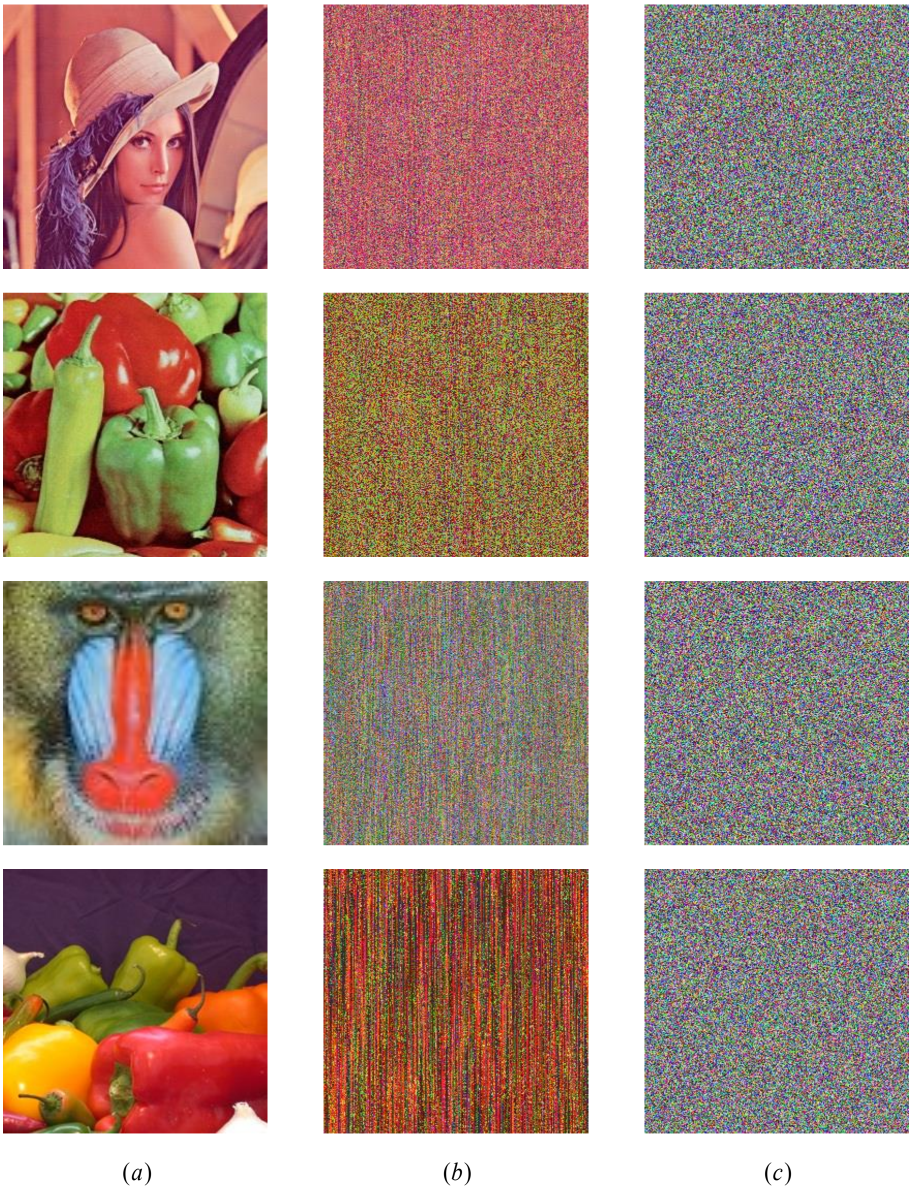


Figure 3.9: Encryption results.

3.9(*a*): Plain images; 3.9(*b*): XORing and row-wise permutation of pixels; 3.9(*c*): Column-wise permutation of pixels.

3.4.1. Security Analyses

To examine the security strength of the proposed scheme, we performed different analyses on it. The detail of these analyses on the proposed scheme is discussed critically.

3.4.1.1. Keyspace analysis

It is important to test the brute force attack to test the security strength of the cryptosystem [57]. A cryptosystem can withstand the brute force attack if its keyspace is greater than $10^{30} \approx 2^{100}$. Assume that the precision of the computer is 10^{15}. The keys and parameters of the 3D chaotic map are $n_1, n_2, n_3, \alpha_1, \beta_1$ and γ_1. Thus, the keyspace has a total of $10^{90} \approx 2^{299}$ possibilities. It shows that the keyspace of the proposed scheme is enormous in its ability to withstand the brute force attack.

3.4.1.2. Time execution analysis

The time required for algorithm execution is also of critical importance to test the value of a cryptosystem [58]. The proposed algorithm is tested on a machine with the following specs: Intel(R) Core (TM) i3-4010U processor @ 1.70GHz; 4.00 GB RAM; and Windows 10 Enterprise. For the execution of both the encryption and decryption process, the computerized simulations are conducted in MATLAB R2013a (8.1.0.604). The time taken to encrypt the RGB Test image is 8.292 seconds.

3.4.1.3. Key Sensitive Analysis

High penetration of encryption schemes against encryption keys describes a highly protected scheme [55]. In order words, the cipher image is different when a small change in the key is made. In Table 3.6, two keys K_1 and K_2 are listed which are used to analyze the sensitivity of the proposed scheme.

Table 3.6: Encryption Keys

Parameters Keys	α_1	α_2	α_3	θ_1	θ_2	θ_3	N_1	N_2	N_3
K_1	2	3	6	60	70	80	40	80	180
K_2	2.000001	3	6.000003	60	70	80	40	80	180

The encryption of plain image and decryption of cipher image with K_1 and K_2 respectively presented in Fig. 3.8. The plain image is given in Fig. $3.8(a)$. The encryption of plain images with K_1 and K_2 are given in Fig. 3.8(b) and Fig. 3.8(c), respectively. The difference between encrypted images is given in Fig. 3.8(d). During the decryption of Fig. 3.8(b) with key K_1, the original image is obtained, but this is not the case with the key K_2, where the obtained image is shown in Fig. 3.8(f). Likewise, during the decryption of Fig. Fig. 3.8(c) with key K_1, the obtained image is shown in Fig. 3.8(g) which is not same as the original image, at the same time we obtain the original image with key K_2. This analysis ensures the capability of the scheme to yield different ciphered images when encryption is performed with slightly different keys.

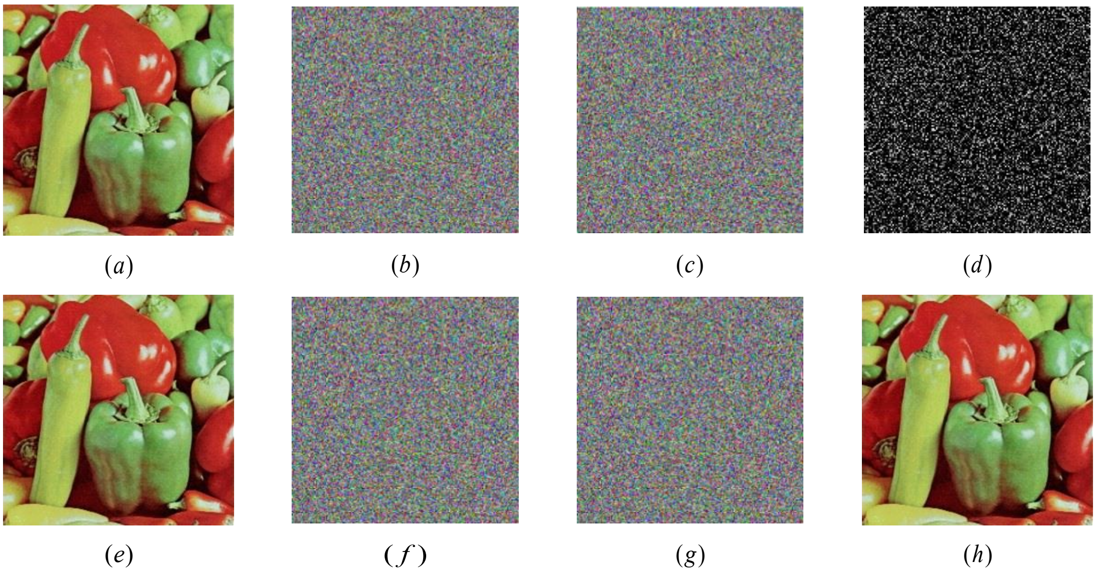
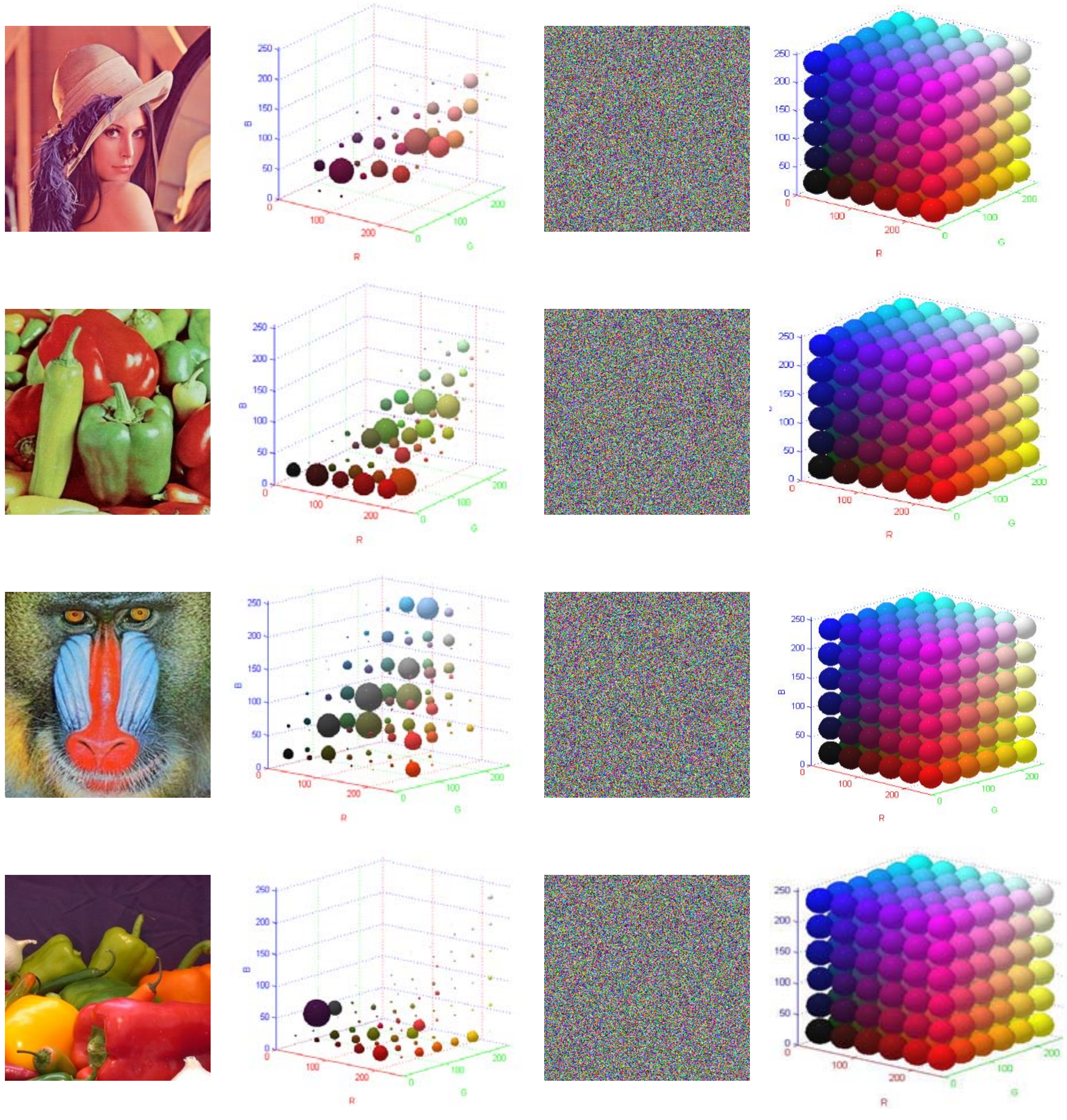


Figure 3.8: Key sensitive analysis

3.4.1.4. Histogram analysis

To authenticate the consistency of pixel values of the cipher image, histogram analysis is performed [54]. The probability of each gray value in the uniform histogram of the cipher image is the same. The uniformness of the histogram of the cipher image defines the resistance of the encryption scheme against statistical and differential attacks. The histograms of original and cipher images are given in Fig. 3.9(b) and Fig. 3.9(d) respectively. It shows that the distribution of pixel values of cipher images is uniform as compared to pixel values of original images. This illustration assumes that the proposed encryption scheme has high resistance against statistical and differential attacks.



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

Figure 3.9: Histogram analysis.

3.9(*a*): Plain image; 3.9(*b*): Histogram of the plain image; 3.9(*c*): Encrypted image; 3.9(*d*): Histogram of the encrypted image

3.4.2. Statistical Analyses

The key point of the proposed work is to transmute visually meaningful images into noise-like encrypted images. Several statistical analyses are used to evaluate the noise-like encrypted images. The information entropy and correlation analysis and differential attacks are presented in this subsection.

3.4.2.1. Information Entropy (IE)

Entropy estimates the strength of a cryptographic scheme in terms of how much it can disorganize the encrypted image [54], [61]. It measures the degree of randomness of an encryption scheme [62]. The results of the entropy analysis are presented in Table 3.7. Besides, comparisons with some of the existing schemes are given in Table 3.8.

Table 3.7: Information entropy analysis of the proposed technique

Test Image	Information entropy (Original)			Information entropy (Encrypted)		
	Red	Green	Blue	Red	Green	Blue
Lena	7.3277	7.6048	7.1326	7.9992	7.9985	7.9991
Peppers	7.3920	7.3920	7.1738	7.9970	7.9965	7.9970
Deblur	7.6646	7.1724	6.4954	7.9967	7.9973	7.9973
Mandrill	7.6634	7.3871	7.6646	7.9969	7.9972	7.9975

Table 3.8: Comparison of Information entropy analysis

Schemes	Test Images	Encrypted Images		
		Red	**Green**	**Blue**
Proposed	Lena	7.9992	7.9985	7.9991
Ref. [66]		7.9798	7.9795	7.9797
Ref. [70]		7.9895	7.9894	7.9894
Ref. [71]		7.9913	7.9914	7.9916
Ref. [72]		7.9893	7.9896	7.9903

3.4.2.2. Correlation analysis

It examines the strength of the encryption scheme to determine how much it can break the relationship of neighbouring pixels [63]. In the plain image, the adjacent pixels are highly correlated. A good encryption scheme can break this relationship [61]. Two thousand pairs are randomly chosen to analyze adjacent correlation coefficients. The results of the correlation analysis of the original and the ciphered images are presented in Fig. 3.10, and Table 3.9. Besides, comparisons with some of the existing schemes are given in Table 3.10. Fig. 3.10(*a-c*) to Fig. 3.10(*d-f*) represent the horizontal, vertical, and diagonal correlation of original and encrypted images, respectively.

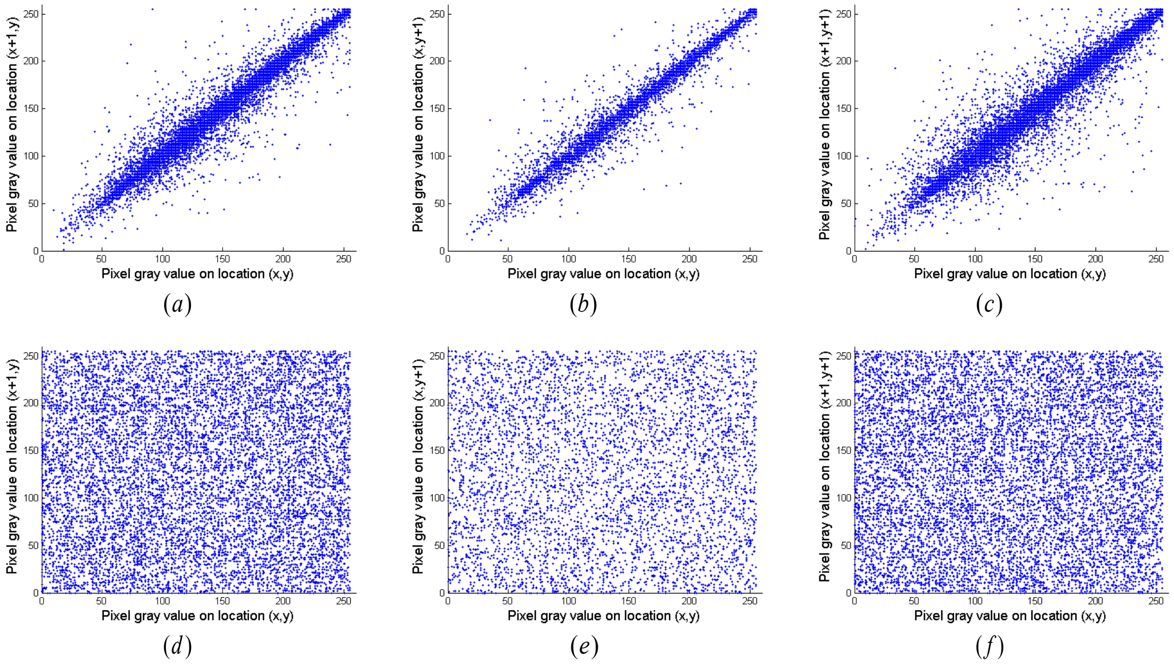


Figure 3.10: The correlation coefficient between pixel pairs for the original and encrypted image.

Table 3.9: Correlation analysis

Test Image	Correlation (Original)			Correlation (Encrypted)		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9452	0.9438	0.9048	-0.0358	-0.0382	0.0060
Peppers	0.9369	0.9272	0.9637	-0.0174	-0.0105	-0.0241
Deblur	0.9848	0.9903	0.9825	-0.0291	-0.0014	-0.0149
Mandrill	0.9419	0.9656	0.9114	0.0065	-0.0187	-0.0054

Table 3.10: Comparison of Correlation Coefficients

Schemes	Test Images	Correlation Coefficient		
		Horizontal	Vertical	Diagonal
Proposed	Lena	-0.00052	0.00068	-0.00932
Ref. [66]		0.0023	- 0.0059	0.0029
Ref. [70]		-0.0080	0.0098	-0.0058
Ref. [71]		0.0018	-0.0015	0.0018
Ref. [72]		0.0035	0.0024	0.0010

3.4.2.3. Differential Attacks

The association between the pixels of the plain image and the ciphered image is evaluated by the NPCR and UACI analyses [54]. These analyses are evaluated, and the findings are presented in Table 3.11.

Table 3.11: Comparison of NPCR and UACI results

Schemes	NPCR			UACI		
	Blue (%)	**Green (%)**	**Red (%)**	**Blue (%)**	**Green (%)**	**Red (%)**
Proposed	99.6163	99.6170	99.6259	33.4476	33.5116	33.5068
Ref. [66]	99.6054	99.6174	99.6369	33.8547	33.7619	33.6046
Ref. [70]	99.6052	99.6060	99.6113	33.4280	33.4966	33.3779
Ref. [71]	99.6097	99.5994	99.5975	33.4476	33.4655	33.4769
Ref. [72]	99.6100	99.6092	99.6099	33.4639	33.5042	33.4776

3.4.2.4. Discussion

The experimental findings of Entropy, Correlation coefficient, NPCR, and UACI of the suggested scheme are presented in Table 3.7 to Table 3.11. These results of NPCR and UACI indicate that the suggested scheme has a high resistance to differential attacks.

A cryptosystem has a high degree of randomness if its entropy estimation is 8. From Table 3.7, note that the randomness of the ciphered image is in proximity to the optimum value. Furthermore, the comparison of this analysis shows that the proposed scheme produces more coincidences than all the schemes presented in the comparison.

A cryptosystem has more strength if its correlation estimation is 0. The original image correlates close to 1 and the correlation of our test images is close to 0. This suggests that the proposed scheme is capable to break the relationship of adjacent pixels. Consequently, the suggested scheme is more secure.

Chapter 4

Small S-box Generation and its Image Processing Application by Mixed Chaotic Maps

In this chapter, an efficient image-encryption technique based on a two-dimensional (2*D*) chaotic system combine with the Galois Field is introduced. The proposed scheme consists of four modules which are the separation of bits, compression, 2*D* chaotic map, and small S-boxes. The proposed algorithm's encryption strength is determined through Entropy, Correlation coefficient, NPCR, and UACI analyses, which were then compared to the past techniques. The proposed image encryption procedure is fast as implementation is concerned because of comprising of one round only.

4.1. Introduction

The digital revolution, particularly at this age of advancement, is a good call for research into multimedia security. Image processing methods have been developed using a variety of technologies. SCAN [73], gray code [74], wave transmission [75], circular random grids [76], vector quantization [77], and elliptic curve ElGamal [78] are some examples of these technologies.

Chaotic systems are unpredictable, nonlinear, and highly penetrating to the starting values. The foundation of encryption with chaos are those dynamic systems that can produce the sequence of random numbers. In the encryption process, these sequences are utilized by different ways. These features make such systems ideal for encryption. Consequently, many researchers designed and utilized the chaotic systems in encryption procedures, new chaotic image encryption schemes have been developed.

Data compression can be utilized when either storage is short, or communication bandwidth is limited [79]. In particular, the data compression algorithm having a low bitrate is required in the wireless communication network for bandwidth limitations. To protect user privacy, encryption is performed [80]. The chaotic systems and compression algorithms are combined with the image encryption algorithm for constructing Chaos-based encryption algorithms and combined crypto-compression algorithms. These combinations are considered more efficient and secure for image encryption.

In Ref. [81], atta et al. established an encryption scheme utilizing S-boxes and chaotic map while in Ref. [82], Bukhari et al. proposed a technique for the construction of the S-boxes and their application in multimedia security. In Ref. [83], shah et al. constructed S-boxes using the irreducible polynomial of degree 8. Sajjad et al. in Ref. [13] constructed S-boxes using the chaotic tent-sine map. A highly secure scheme has a balance of confusion and diffusion. The ultimate objective of this chapter is to provide confusion through Substitution-box and diffusion is created by utilizing a chaotic map. A balanced scheme that covers both necessary aspects.

4.2. Preliminaries

In this section, the fundamental facts of suggested image encryption are explored. Firstly, the construction of S-boxes using Mobius transformation and their analyses are presented. Then, the sine map, the Tinkerbell map, and the mixed chaotic map are discussed. At the end of this section, the compression, compression ratio, and compression algorithm are described.

4.2.1. Construction of Substitution Box (S-box)

We utilized Linear Fractional Transformation (LFT) and its application over the Galois field $GF(2^4)$ through group action to design a new substitution box (S-box). The group action is defined as:

$$h : PGL\left(2, \frac{\mathbb{Z}_2[x]}{\langle \eta(x) \rangle}\right) \times \frac{\mathbb{Z}_2[x]}{\langle \eta(x) \rangle} \to \frac{\mathbb{Z}_2[x]}{\langle \eta(x) \rangle}$$

$$h(t) = \frac{at+b}{ct+d},\ ad-bc \neq 0 \tag{4.1}$$

where $t,a,b,c,d \in \mathbb{Z}_2[x]/\langle \eta(x) \rangle$, and $\eta(x) = x^4 + x + 1$. The image of $h(t)$in the field $\mathbb{Z}_2[x]/\langle \eta(x) \rangle$ is used to generate the S-box. It should be noted that the value of t is from 0 to 15 belongs to $\mathbb{Z}_2[x]/\langle \eta(x) \rangle$. These values are used in LFT after they are converted into polynomial form. When the condition $ad-bc \neq 0$ does not hold, the algorithm stops. Also, if the denominator becomes zero for any value of t. In that case, the missing one after the end of the process will place value at that position.

Here t is supposed as the solution of $\eta(x) = 0$ such that $\eta(t) = t^4 + t + 1 = 0$. The solution of $\eta(t) = 0$ is used to generate different elements of $GF(2^4)$. In this study we fix the values of

$a = 12,\ b = 4,\ c = 8$ and $d = 13$, then construct the S-box by using the transformation given as follows:

$$h(t) = \begin{cases} 12t + 4/8t + 13 & ,t \neq 0 \\ 8 & ,t = 0 \end{cases} \tag{4.2}$$

The elements of Galois Field $GF(2^4)$, their corresponding binary and decimal values along with elements of the Substitution box are presented in Table 4.1.

Table 4.1: Elements of $GF(2^4) = \mathbb{Z}_2[x]/\langle x^4 + x + 1 \rangle$ and an S-box

$GF(2^4)$	**Binary values**	**Decimal Form**	$h(t) = 12t + 4/8t + 13$	**Elements of S-box**
0	0000	0	$h(0) = (12(0)+4)/(8(0)+13)$	3
t	0010	2	$h(2) = (12(2)+4)/(8(2)+13)$	14
t^2	0100	4	$h(4) = (12(4)+4)/(8(4)+13)$	7
t^3	1000	8	$h(8) = (12(8)+4)/(8(8)+13)$	2
t^4	0011	3	$h(3) = (12(3)+4)/(8(3)+13)$	15
t^5	0110	6	$h(6) = (12(6)+4)/(8(6)+13)$	4
t^6	1100	12	$h(12) = (12(12)+4)/(8(12)+13)$	9
t^7	1011	11	$h(11) = (12(11)+4)/(8(11)+13)$	0
t^8	0101	5	$h(5) = (12(5)+4)/(8(5)+13)$	10
t^9	1010	10	$h(10) = (12(10)+4)/(8(10)+13)$	11
t^{10}	0111	7	$h(7) = (12(7)+4)/(8(7)+13)$	13
t^{11}	1110	14	$h(14) = (12(14)+4)/(8(14)+13)$	6
t^{12}	1111	15	$h(15) = (12(15)+4)/(8(15)+13)$	1
t^{13}	1101	13	$h(13) = (12(13)+4)/(8(13)+13)$	8
t^{14}	1001	9	$h(9) = (12(9)+4)/(8(9)+13)$	12
t^{15}	0001	1	$h(1) = (12(1)+4)/(8(1)+13)$	5

4.2.1.1. Algebraic Analysis for Substitution boxes

The standard measures to evaluate the strength of the Substitution boxes are nonlinearity, strict avalanche criteria (SAC), Linear proximation probability (LP), Differential approximation probability (DP), and Bit independence criteria (BIC) are given in this subsection. Nonlinearity computes the base separation between the arrangement of all *n*-variable affine functions and *n*-variable Boolean functions. Strict avalanche criteria measure the no. of bits changed in output by making a change of a single bit in the input. LP estimates the inconsistency of an occasion among input and output while DP ensured the uniqueness of the change in output for each change made in the input. Furthermore, BIC explores the unaltered bits. For detail, the study follows [36].

The SAC and Average SAC values of the suggested small S-box are provided in Tables 4.2 and 4.3 respectively. Further, the BIC and DP values are given in Tables 4.4 and 4.5.

Table 4.2: The SAC analysis

0	4	4	4
4	0	4	4
4	4	0	4
4	4	4	0

Table 4.3: The Average SAC analysis

0.5000	0.6250	0.6250	0.7500
0.5000	0.6250	0.3750	0.5000
0.5000	0.6250	0.5000	0.2500
0.5000	0.5000	0.6250	0.2500

Table 4.4: The BIC analysis

4	1	1	2
1	4	0	1
1	0	4	1
2	1	1	4

Table 4.5: The DP analysis

2	4	4	4
2	4	6	4
4	2	4	6
4	2	4	16

The nonlinearity of our suggested small S-boxes is 4, which is the optimum value of nonlinearity of 4 bits S-boxes. The values of the SAC, Average SAC, the BIC, and the DP satisfying all measurements for the suggested small S-boxes. The performance analyses indicate that the suggested S-boxes have almost the optimized results when it comes to randomness, resistance against the various linear and differential attacks.

4.2.3. Chaotic Map

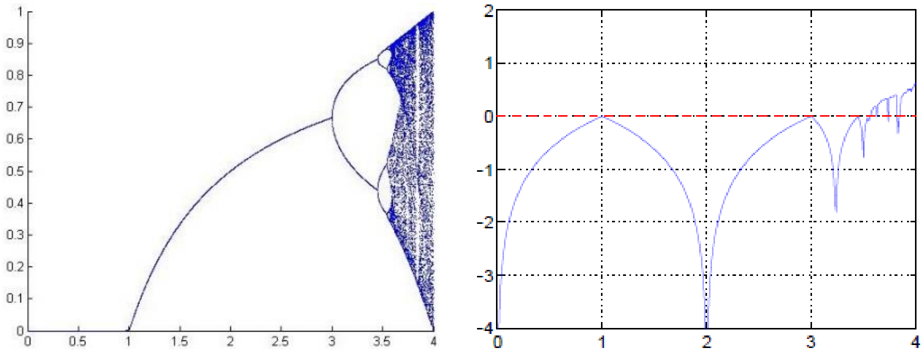
Chaotic maps are defined as recursive functions. These maps can also be any number of dimensions. The chaotic maps used in the algorithm are described below.

4.2.3.1. Sine Map

The subsequent iterated equation is an equation of one of the discrete chaotic maps that is a sine map.

$$\mu_{t+1} = S(a,\mu_t) = a\sin(\pi\cdot\mu_t) \tag{4.3}$$

where a is used as a parameter and its range is $(0,1]$ and the range of μ_t is $(0,1)$. When the value of a is equal to 1, then this function is in a state of chaos. The Bifurcation and Lyapunov diagrams of the Sine map are given in Fig. 4.1(a) and Fig. 4.1(b), respectively.



(a) (b)

Figure 4.1: Bifurcation and Lyapunov diagrams of Sine map

4.2.3.2. Tinkerbell Map

Tinkerbell map, the two-dimensional chaotic map, is a discrete map defined by following subsequent iterated equations as:

$$x_{t+1} = x_t^2 - y_t^2 + p'x_t + q'y_t \tag{4.4}$$

$$y_{t+1} = 2x_t y_t + m'x_t + n'y_t \tag{4.5}$$

where p', q', m' and n' are the parameters from real numbers or any interval. The most frequently used values of p', q', m' and n' are $p' = 0.9, q' = 0.6013, m' = 2.0, n' = 0.50$ and $p' = 0.3, q' = 0.6000,\ m' = 2.0, n' = 0.27$.

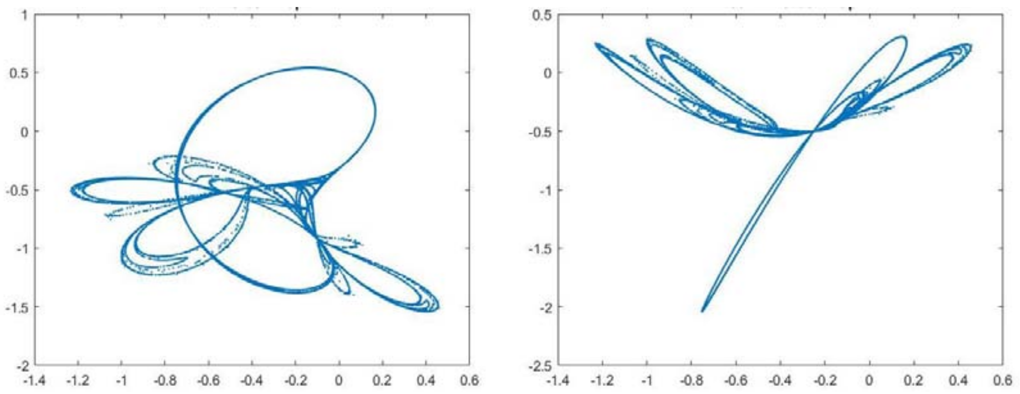
Like other chaotic maps, this chaotic map has also periods. The root of mapping's name Tinkerbell is unknown. However, the graphical representation of this map depicts an analogy to the motion of a fictional character Tinkerbell in Cinderella castle.

4.2.3.3. Mixed Chaotic map

The Tinkerbell map and sine map are mixed up to design the suggested map which is a nonlinear combination of the above-mentioned maps. The mix-up process is represented by the following equation.

$$\begin{aligned} Z_{t+1} &= \zeta_{ST}(r, Z_t^a) \\ Z_{t+1} &= \left[S(a, Z_t^a) + T(p', q', m', n', Z_t^a) \right] \bmod 1 \end{aligned} \tag{4.6}$$

Where $\zeta_{ST}(r, Z_t^a)$ is mixed two dimensional chaotic map of sine map and Tinkerbell map, $S(a, Z_t^a)$ is a one-dimensional chaotic map having a as its parameter, and $T(p', q', m', n', Z_t^a)$ is a two-dimensional chaotic map having $p', q', m',$ and n' as its parameters, mod represents modulo operation whose range is [0,1) and t depicts the iteration's number. The Tinkerbell map attractor and mixed chaotic map attractor are given in Fig. 4.2.



(a) (b)

Figure 4.2: Attractor diagrams, 4.2(a): Tinkerbell map attractor, 4.2(b): Mixed chaotic map attractor

The mixed chaotic map has a better chaotic range and randomness. The main advantage of mixing the 1D sine map and 2D Tinkerbell map is to use the parameters to double the keyspace for high resistance against brute force attack. This is one example of the proposed encryption scheme otherwise; we can use or mix any two chaotic maps for the proposed encryption algorithm.

4.2.4. Data Compression

The method of terminating the data redundancies from documents to decrease the cost of data storing is data compression [84]. Mostly, compression is used to make the best use of bandwidth through a distribution link. It is also used to enhance disk space while saving documents. All compression methods can compress the data to a certain limit. This limit is directly connected to the different types and consistency of data [84].

4.2.4.1. Compression ratio

It is the measure of compression and is defined in terms of disk utilization [84].

$$Compression\ ratio = \left(1 - \frac{compressed\ file\ size}{uncompressed\ file\ size}\right) \times 100\% \tag{4.7}$$

4.2.4.2. Lempel-Zev-Welch algorithm

Dictionary-based compression algorithms do not rely on the statistical model. In its place, they depend on a dictionary, which consists of all that one can think of words of a language, which are kept in a table-like construction. For the representation of larger and repeating words of the dictionary, the table uses indexes of entries. An algorithm that works using this dictionary is the Lempel-Zev-Welch algorithm or the LZW algorithm for short. In the LZW method, for storing and indexing earlier seen string configurations, a dictionary is used. During the compression procedure, the algorithm does not use repeating string configurations and a dictionary is generated dynamically. There is no compulsion on this dictionary to move it with the coded data for the decompression process. During decompressing, the same dictionary is generated dynamically and is used for decryption purposes. Hence, it is an effective compression algorithm for adaptation [84].

4.3. Proposed Image Encryption Technique

This section comprises the suggested image encryption technique, security analyses, and comparisons.

The suggested technique applies to the RGB image, which consists of four modules. The RGB image of dimension $M \times N \times 3$ is split into the three-color components of dimension $M \times N$ before the first module of the encryption process. Afterward, encrypt each component of the image independently. The four modules of the suggested technique are described as follows.

Module I: The scheme divides the block of the image into two sub-blocks; LSB block and MSB block, and then convert the MSB into LSB. Subsequently amalgamate the two matrices into a single block, consequently, get three new blocks of dimension $2M \times 2N$.

Module II: The scheme applies the LZW compression algorithm on the bits of the new data blocks. The aim of using LZW is to eliminate unnecessary data from the original image.

Module III: Since the pixels of the plain image are highly correlated with one another. Therefore, the scheme uses a $2D$ mixed chaotic map to permutes the obtained data of module II. The permutation step aims to diminish the correlation among the neighbouring pixels of the image and mix up the LSB of the image with the newly converted LSBs of the image. The permutation step is given as follows:

$$Z_{t_M} = floor(Z_t \times 10^{10} \bmod M) \tag{4.8}$$

$$Z_{t_{2N}} = floor(Z_t \times 10^{10} \bmod 2N) \tag{4.9}$$

$$Z'_{t_M} = unique(Z_{t_M}, stable) \tag{4.10}$$

$$Z'_{t_{2N}} = unique(Z_{t_{2N}}, stable) \tag{4.11}$$

Apply

$$C(i,j) = I\left(Z'_{i_M}, Z'_{j_{2N}}\right) \text{ if } Z'_{i_M} > 0 \text{ and } Z'_{j_{2N}} > 0 \tag{4.12}$$

Apply

$$C(i,j) = I\left(Z'_{i+1_M}, Z'_{j_{2N}}\right) \text{ if } Z'_{i_M} = 0 \text{ and } Z'_{j_{2N}} > 0 \tag{4.13}$$

Apply

$$C(i,j) = I\left(Z'_{i_M}, Z'_{j+1_{2N}}\right) \text{ if } Z'_{i_M} > 0 \text{ and } Z'_{j_{2N}} = 0 \tag{4.14}$$

Apply

$$C(i,j) = I\left(Z'_{i+1_M}, Z'_{j+1_{2N}}\right) \text{ if } Z'_{i_M} = 0 \text{ and } Z'_{j_{2N}} = 0 \tag{4.15}$$

$I(i,j)$ indicates the pixel position of the compressed data matrix and $C(i,j)$ denotes the pixel position of the mixed-up permuted data matrix. Module III yields a mixed-up permuted matrix.

Module IV: The scheme uses the generated S-box and substitutes the mixed-up permuted matrix to produce confusion in the ciphered data. The substitution process is the same as the mini-AES substitution. Subsequently, divide the substituted block in two subblocks of dimension $M \times N$, and transform the data of the first Block into MSB and combine with the LSB of the second block. The obtained block is the required encrypted image. For the decryption process, start from the end of the encryption process in reverse order.

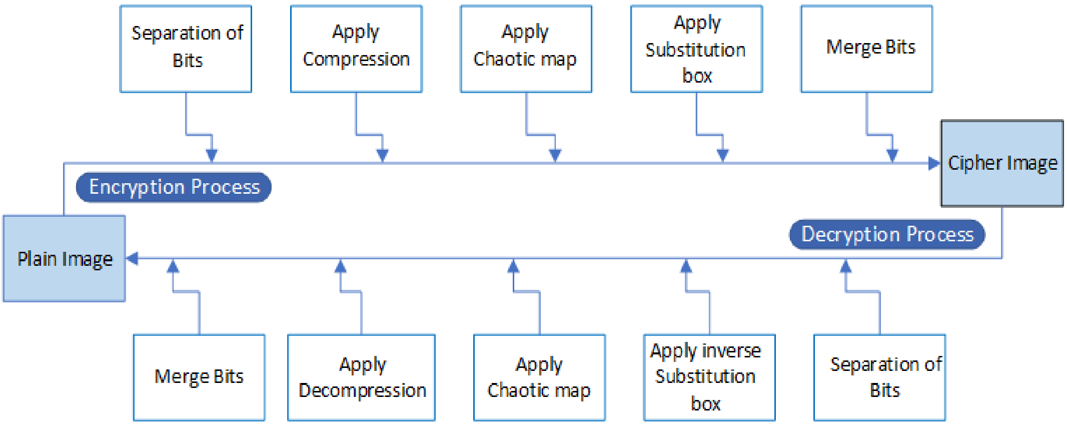


Figure 4.3: Flowchart of the proposed technique

The flowchart of the encryption and decryption process is shown in Fig. 4.3.

The encryption result along with histograms is illustrated in Fig. 4.4. The plain images of Lena, Deblur, Mandrill, and Pepper and their corresponding histograms are presented in In Fig. 4.4(a) and Fig. 4.4(b), While the encrypted images and their corresponding histograms are presented in Fig. 4.4(c) and Fig. 4.4(d), respectively.

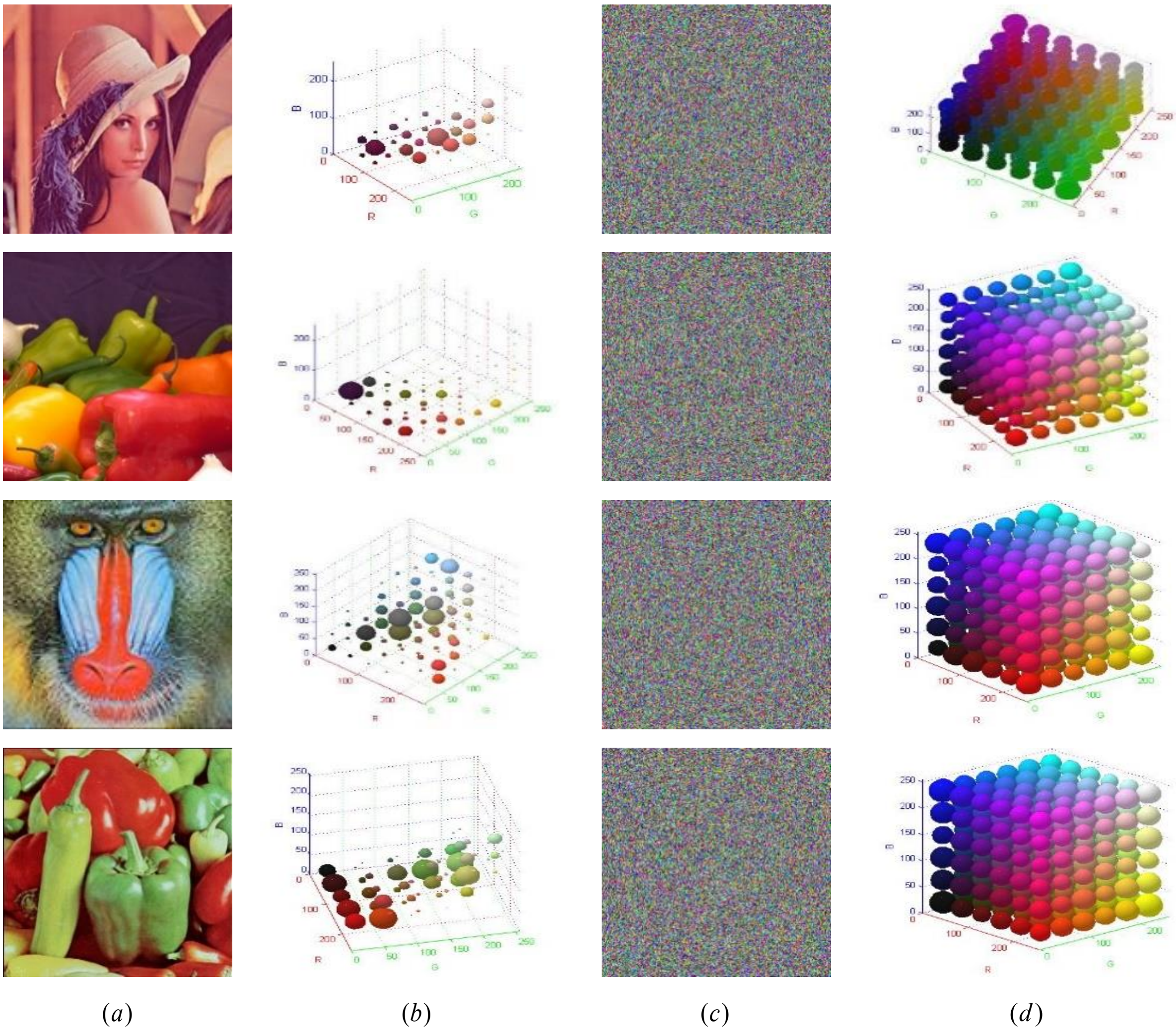

(a) (b) (c) (d)

Figure 4.4: Encryption results of the proposed technique

4.4. Simulation Results and Analyses

4.4.1. Security Analyses

An excellent encryption method should be both robust and effective. Robustness means that the cipher should apply to any plaintext image written in a supported format. Effectiveness implies that the cipher can generate eligible ciphertext images, which hide information from possible intruders.

4.4.1.2. Key sensitivity

It is very significant to observe the effect of different keys in the algorithm [55]. What kind of change occurred when a key is changed in the algorithm. Two keys (say) K_1 and K_2 are considered which are $S\left(0,0\right)=0.5,\ r=[0.5,1,1.5,2,2.5]$ and $S\left(0,0\right)=0.97542,$ $r=[0.50000001,1,1.5,2,2.5]$. The Lena image is encrypted with these two different keys, and it is shown in Fig. 4.5.

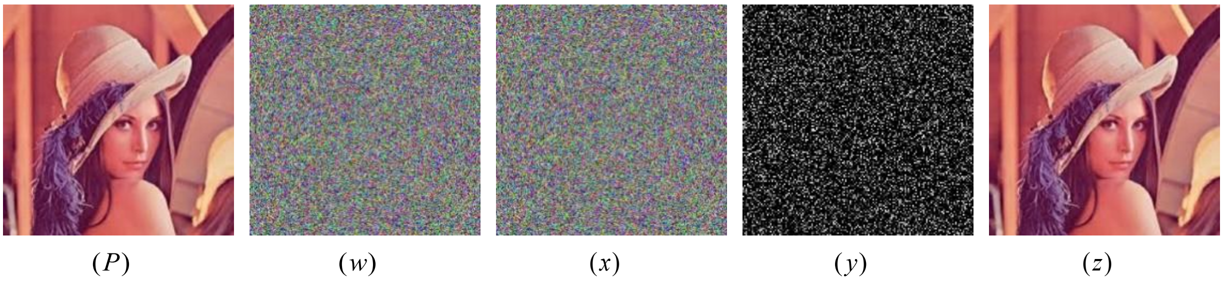


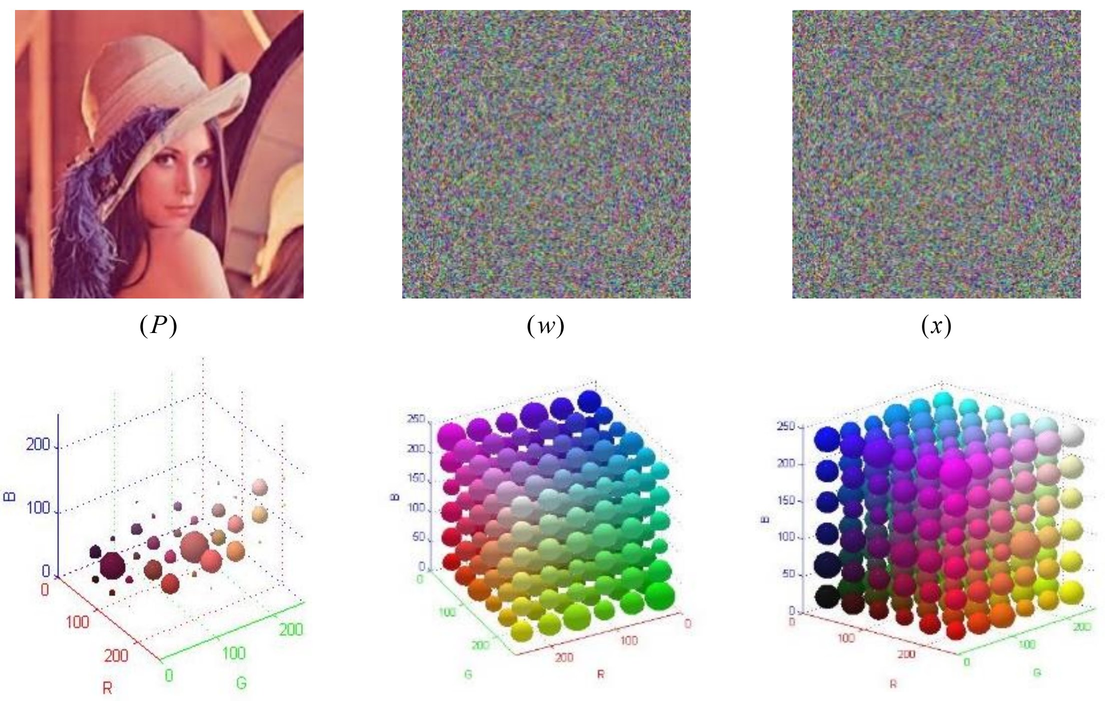
Figure 4.5: Key sensitivity test with different keys

4.4.1.3. Time complexity

The Time complexity of an algorithm describes the amount of time required for execution [58]. Typically, marked by big O. The modules of the suggested technique are completely based on the arithmetic operations addition and multiplication. Thus, the time complexity of the third module III is $O(2M \times N)$. In Module IV, the arithmetic operation multiplication and inversion in the Galois field $\mathbb{F}_{2^4}$ have been used one time, consequently the execution of module I requires $O(2^4)$, which is constant. The time complexity of the overall algorithm is $O(2M \times N)$. One can see that the time complexity of the suggested technique is linear time. Thus, the suggested technique is secure and having less time complexity.

4.4.1.4. Chosen plaintext attack

For an image encryption technique to withstand the chosen plaintext attacks, it should have outstanding diffusion property [54]. However, using the same security keys in many existing encryption schemes, their encrypted image is duplicate. This security weakness aspect offers the chance for attackers to break down the encryption scheme using the chosen plaintext attack. This analysis demonstrates that if we use the same key on the same message, we get a different result every time, which makes it impossible for a hacker to use the same message's encryption for finding the decryption procedure or guessing the message twice successively.



(*P*) (*w*) (*x*)

(*y*) (*z*) (*u*)

Figure 4.6: Chosen plaintext attack analysis

4.4.2. Statistical Analyses

The key point of the suggested work is to transmute the visually important image data into noise-like encrypted images. Several statistical methods are used to evaluate the noise-like encrypted images.

4.4.2.1. Information entropy (IE)

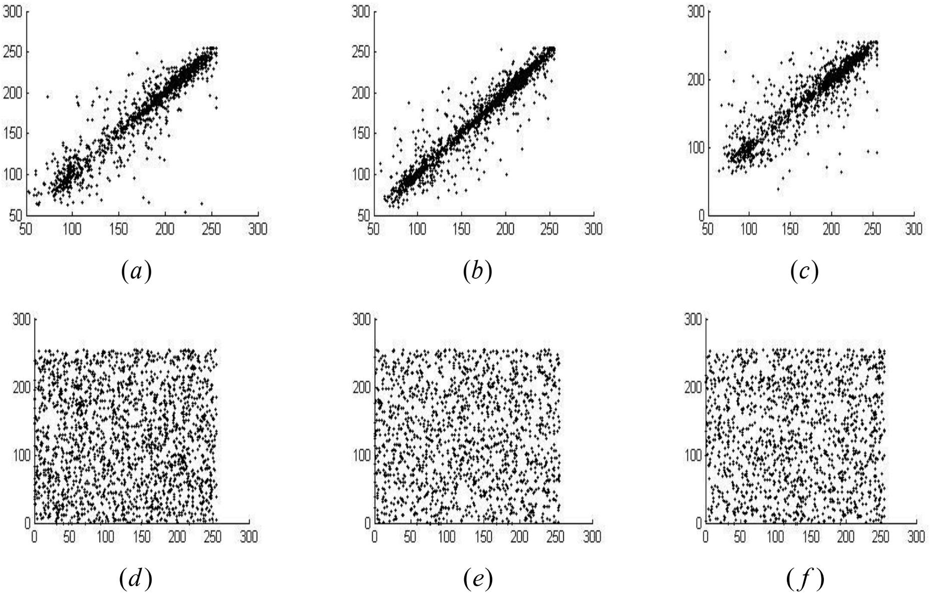
This measure is used to compute the randomness of an image [54], [61]. The IE results of the suggested technique are presented in Table 4.6 and compared in Table 4.8.

Table 4.5: Information entropy analysis

Test Image	Information entropy (Original)			Information entropy (Encrypted)		
	Red	Green	Blue	Red	Green	Blue
Lena	7.3277	7.6048	7.1326	7.9984	7.9987	7.9989
Peppers	7.3920	7.3920	7.1738	7.9970	7.9965	7.9970
Deblur	7.6646	7.1724	6.4954	7.9967	7.9973	7.9973
Mandrill	7.6634	7.3871	7.6646	7.9969	7.9972	7.9975

4.4.2.2. Correlation analysis

In an image that is not encrypted, the color dissolves into the dark to lighter shades, which makes the pixel values correlated with its neighbouring [63]. The purpose of encryption is to break every relation in the image pixels. The analysis of the correlation coefficient and their comparison with existing algorithms are given in Fig. 4.7, Table 4.7, and 4.8, respectively. The suggested technique shows a very low correlation coefficient. So, the suggested technique is secure.



(a) (b) (c)

(d) (e) (f)

Figure 4.7: The correlation coefficient analysis.
$4.7(b)$, $4.7(f)$: Horizontal; $4.7(c)$, $4.7(g)$: Vertical; $4.7(d)$, $4.7(h)$: Diagonal.

Table 4.7: Correlation analysis

Test Image	Correlation (Original)			Correlation (Encrypted)		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9452	0.9438	0.9048	-0.0358	-0.0382	0.0060
Peppers	0.9369	0.9272	0.9637	-0.0174	-0.0105	-0.0241
Deblur	0.9848	0.9903	0.9825	-0.0291	-0.0014	-0.0149
Mandrill	0.9419	0.9656	0.9114	0.0065	-0.0187	-0.0054

Table 4.8: Comparison of information entropy and Correlation analysis

Schemes	Test Images	Encrypted Images			Correlation Coefficient		
		Red	Green	Blue	Horizontal	Vertical	Diagonal
Proposed	Lena	7.9984	7.9987	7.9989	0.0043	-0.0187	-0.0054
Ref. [66]		7.9798	7.9795	7.9797	0.0037	0.0030	-0.0029
Ref. [67]		-	-	-	0.00231	- 0.00590	0.00291
Ref. [70]		7.9893	7.9896	7.9903	-	-	-
Ref. [65]		7.9974	7.9969	7.9973	0.00350	0.00247	0.0010
Ref. [64]		7.9970	7.9964	7.9976	0.0075	0.0041	0.0002
Ref. [68]		7.9913	7.9914	7.9916	0.00186	-0.00155	0.00185
Ref. [69]		7.9874	7.9872	7.9866	-0.0580	-0.0024	-0.0170

4.4.2.3. Differential attacks

The two most routine measures used to assess the quality of picture encryption are the NPCR and UACI [43]. NPCR quantifies the absolute number of pixels which changes the value in differential attacks while the UACI computes the averaged difference between two paired cipher images. A high NPCR and UACI demonstrate high protection from differential assaults. These measures must lie in [99, 100] and [33, 34], respectively.

The results of these measurements lie in the abovementioned range. They are presented and compared in Table 4.9.

Table 4.9: NPCR and UACI comparison

Schemes	NPCR			UACI		
	Blue (%)	Green (%)	Red (%)	Blue (%)	Green (%)	Red (%)
Proposed	99.6163	99.6170	99.6259	33.4476	33.5316	33.5068
Ref. [66]	99.5925	99.5921	99.5927	33.5037	33.5112	33.5039
Ref. [67]	99.6054	99.6174	99.6369	33.8547	33.7619	33.6046
Ref. [70]	99.6100	99.6092	99.6099	33.4639	33.5042	33.4776
Ref. [65]	99.6041	99.5920	99.5992	33.4635	33.5418	33.4001
Ref. [64]	99.6550	99.6535	99.6492	33.5160	33.5316	33.5237
Ref. [68]	99.6097	99.5994	99.5975	33.4476	33.4655	33.4769

Chapter 5

A Novel Design of Legendre Chaotic Map and its Implementation in Image Processing

This chapter is devoted to analysing a chaotic oscillator generated by the Legendre differential equation which produces confusion and diffusion in the plaintext message to achieve the desired secrecy. The produced chaotic sequence of random numbers from the dynamical system is utilized to scramble the pixels of an image to get an encrypted image. Chaos-based encryption technique is found secure enough to tackle chosen plaintext attacks and brute force attacks. The specific attributes of a chaotic system like, sensitivity to initial conditions, randomness, and uncertainty make it suitable for the design of cryptosystem. The dominance of the proposed scheme is acknowledged due to the fact of better cryptographic properties when compared with the algorithms developed already in the literature.

5.1. Introduction

The advancement of the internet and information age has a huge interest of study related to the security of multimedia. Multiple technologies have been utilized in the construction of a cryptosystem.

Recently many researchers are working on image encryption techniques utilizing different algebraic structures as well as chaotic maps. Iqtadar et al. [85] used the permutation of the symmetric group for the construction of the encryption technique. In another article, Ayesha et al. [86] considered triangular groups for the construction of substitution boxes with an application in patent safety. Chaotic systems are highly penetrating to initial values and unpredictable, nonlinear, random, and unsystematic. In [23], [87], the authors proposed their schemes based on a single $1D$ map and multiple chaotic maps. In [88]–[90], the researchers discussed the combine maps with enhanced unpredictability having more complex puzzling behaviours. Many researchers have been proposed several chaos-based cryptosystems, not all these proposed models are perfect.

In this modern age of technology, data compression is essential for digital communication. Without it, we could not have digital televisions, smarts-phones, satellite communications, and the internet [79]. Further, data compression can be utilized when either storage is short, or communication bandwidth is limited. In particular, the data compression algorithm having a low bitrate is required in the wireless communication network for bandwidth limitations. To protect user privacy, encryption is performed [80]. The combination of the chaotic system and compression has provided efficient and secure schemes for image encryption.

Zhou et al. [23], Al-Maadeed et al. [80], and Farajallah et al. [91], [92] investigated on joint chaos-based and compression-based cryptosystems. They inspired us to construct a chaos-compression-based image encryption system having efficient and better security and statistical results.

The zero-one test is used to build a novel chaotic system using the Legendre polynomial. The zero-one test verifies the Legendre chaotic map's chaotic behaviour. This is the first time we employ Legendre polynomials only for this aspect. A stronger and more secure picture encryption method with confusion and diffusion is presented for use in multimedia security.

5.2. Preliminaries

In this section, the Legendre differential equation, Zero-One test, and Lempel-Ziv Welch compression algorithm are illustrated.

5.2.1 Legendre differential equation

In 1784, French mathematician Adrien-Marie Legendre introduced differential equations which are named Legendre differential equations. Legendre's differential equations are a very significant case in Sturm-Liouville's Boundary value problems. These differential equations appear in several problems, particularly in those that exhibit spherical symmetry. There are many other non-linear systems which are capable to produce chaotic behaviour. Since the Legendre Polynomials exhibit spherical symmetry (symmetricity), that why, we investigated the chaotic behaviour using the Legendre Polynomials. The chaotic sequences and their chaotic behaviour are analyzed using Zero-One test.

Legendre’s Differential Equation is expressed as follows:

$$(1-x^2)y''-2xy'+n(n+1)y=0 \tag{5.1}$$

Where n represents a real number. The solutions of Eq. (5.1) are known as Legendre functions. The degree of these Legendre functions is same as the real number n. For any non-negative integer n, the Legendre functions are frequently known as Legendre polynomials $P_n(x)$. Illustration of some Legendre polynomials are provided in Fig. 5.1.

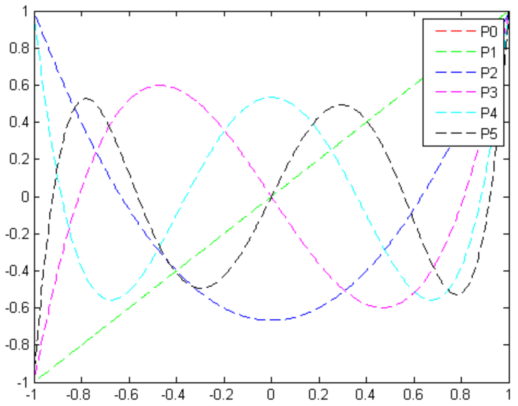


Figure 5.1: Graphical Illustration of some Legendre polynomials

5.2.2. Z1 Test

Gottwald and Melbourne [93], [94] introduced the Z1 test and its validity. The non-regular stationary responses of dynamical systems of any sort can be detected by Zero–one test (Z1). This test discussed the amount of chaos in a sequence in a single value between 0 and 1. As the amount of chaos in sequence increases, the outcome gets closer to 1. We can verify our newly generated chaotic map employing this test. The Zero-one test can be précised in four steps.

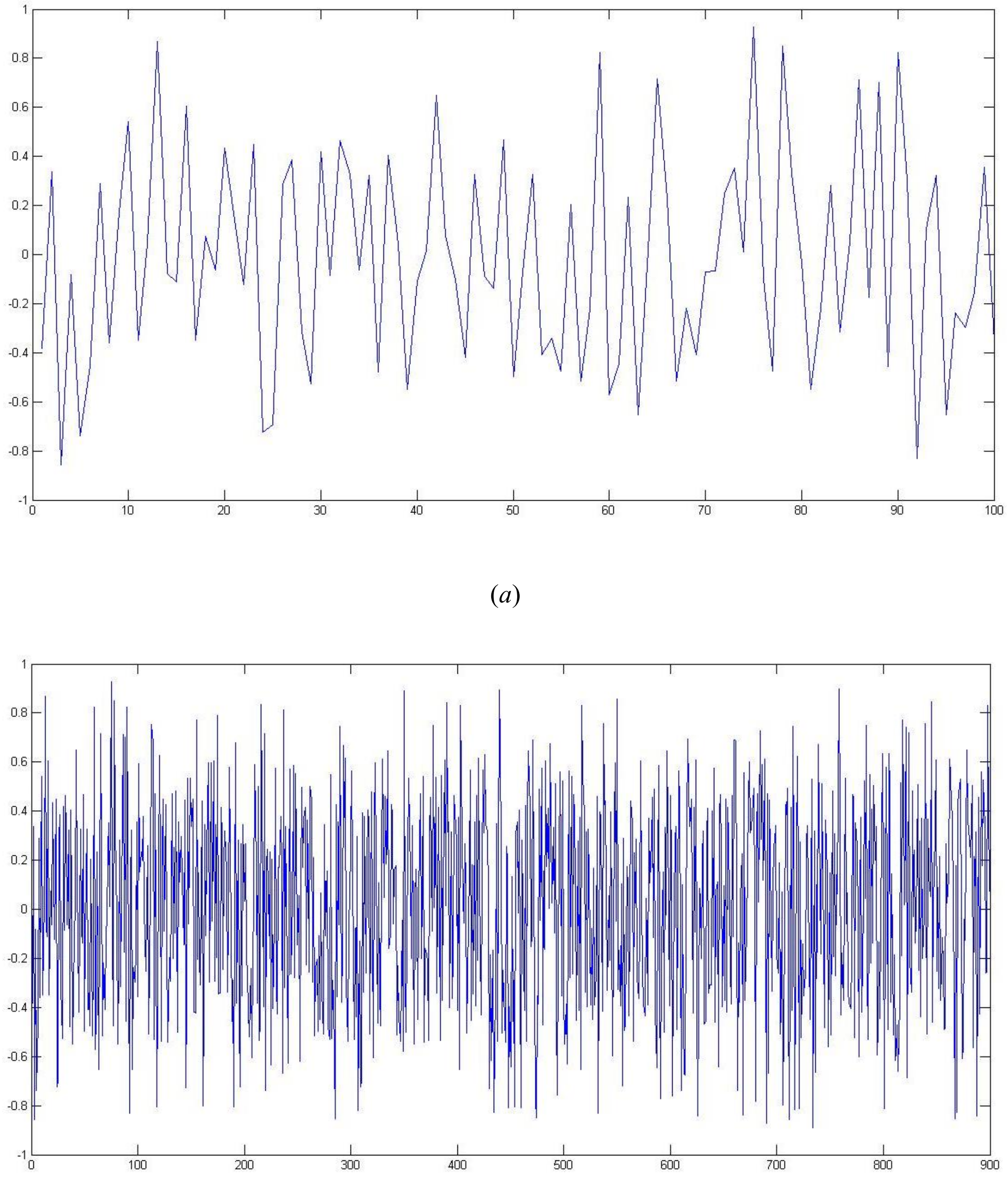
1. Calculate the translation variable
2. Analyze the diffusive behaviour
3. Discuss the asymptotic growth rate
4. Compute the median

5.2.2.1. Outcomes of Z1 test for proposed sequence

In this subsection, the chaotic sequences along with the statistical results of the Z1 test are revealed via MATLAB. The chaotic performance of suggested sequences is illustrated in Fig. 5.2 while, the statistical results of the Zero-One test are presented in Table 5.1.

Table 5.1: Proposed chaotic system analysis, Z1 test

Size of sequence	Z1 test result
100	0.9950
900	0.9977
10,000	0.9982



(*a*)

(*b*)

Figure 5.2: Chaotic performance of suggested sequences

The above experimental data show that as the length of the sequence increases, the amount of chaos in the sequence enhances. This is because the three conditions of chaotic maps can be observed better in a bigger sequence.

5.2.4. Data Compression

The method of terminating the data redundancies which occur in many documents to decrease the cost of data storing is known as data compression [84]. Mostly, compression is used to make the best use of bandwidth through a distribution link. It is also used to enhance disk space while saving documents. Data compression techniques compress data to an extent, but the compression depends on the type and texture of data [84]. In this research, a compression technique is used as a function that will compress or decompress the image data.

5.2.4.1. Compression ratio

Compression ratio is a measure of compression and is defined in terms of disk utilization [84].

$$CR = (1 - \frac{C}{U}) \times 100\% \tag{5.2}$$

where '*CR*' represents compression ratio, '*C*' represents compressed file size and '*U*' defined as uncompressed file size.

5.2.4.2. Lempel-Zev-Welch algorithm

It's a dictionary-based compression method that doesn't rely on a statistical model. Instead, it uses a dictionary, which is a table-like structure that contains all conceivable worlds of a language. For the presentation of higher and repeated terms in the dictionary, the table uses indexes of entries.

A dictionary is employed in the LZW technique for storing and indexing previously encountered text configurations. The technique does not employ repeated string configurations during compression, and a dictionary is built dynamically. This dictionary is not obligated to travel with the coded data during the decompression process. The same dictionary is produced dynamically for decryption during decompression. As a result, it is an excellent adaption compression algorithm [84].

5.3. Proposed Image Encryption Algorithm

In this section, the proposed image encryption algorithm is presented. This algorithm is described in five steps. The third step of the algorithm is further consisting of five modules. These five modules are explored in subsection 5.3.1.

Flowchart of the proposed algorithm is given in Fig. 5.3, while the demonstration is provided in Fig. 5.4. At the end of this section, the proposed scheme is analyzed using standard measures.

5.3.1. Proposed Encryption Algorithm

The proposed algorithm can be described in the following five steps.

Firstly, the algorithm applies the LZW compression technique on bits of the plain image, which is lossless, common, and very simple to implement. The goal of using LZW is to eliminate the unnecessary data from the original image and reduce the range of the pixel values.

Secondly, the algorithm divides the bits of the image into two sub-blocks of LSB's and MSB's.

Thirdly, the algorithm performs four rounds of the following modules on MSB's:

5.3.1.1. Random Pixel Insertion

5.3.1.2. Row Separation

5.3.1.3. 1*D* substitution

5.3.1.4. Row Combination

5.3.1.5. Image Rotation

These modules are explored hereunder.

5.3.1.1. Random Pixel Insertion

The first module of the third step is defined as follows:

$$P(j,k)=\begin{cases} Rand(j) & if\ k=1 \\ I(j,k-1) & otherwise \end{cases} \tag{5.3}$$

where I and $P(j,k)$ denote the input and processed image whose sizes are, $S\times T$, $S\times(T+1), 1\le j\le S$ and $1\le k\le(T+1)$, respectively and *Rand*(*j*) is a random function used to generate random values/numbers.

5.3.1.2. Row Separation

This module is a transformation of the image into the 1*D* matrix by using all pixel rows of the image one by one.

$$R_j(k)=P(j,k), \tag{5.4}$$

where R_j shows the j^{th} 1*D* row matrix having length $(T+1)$.

5.3.1.3. 1*D* substitution

In this module, all the data values in each 1*D* matrix R_j undergo the process of alteration. The 1*D* substitution can be defined as:

$$Q_j(k) = \begin{cases} R_j(k) & \text{if } k = 1 \\ W & \text{otherwise} \end{cases} \tag{5.5}$$

where, $W = Q_j(k-1) \oplus R_j(k) \oplus \left(\left\lfloor N_l(j,k) \times 10^{10} \right\rfloor \bmod 256 \right)$, and $\oplus$ indicates the bit-level *XOR* operation, $\lfloor \cdot \rfloor$ is the floor function and $N_l(j,k)$ denote the random sequence for $k^{th}, (k = 1, 2, 3, 4)$ encryption round.

5.3.1.4. Row Combination

This module is the inverse of the first and second modules. This module adjoins all 1*D* matrices to make a two-dimensional image matrix and then eliminates the first added pixel from each row. It is mathematically defined as:

$$O(j,k) = Q_j(k+1), \tag{5.6}$$

where *O* express the two-dimensional image matrix with the size of $S \times T$ with $k \leq T$.

5.3.1.5. Image Rotation

In the last module, the two-dimensional image matrix is rotated at an angle of 90 degrees counter clockwise given as follows:

$$D(j,k) = O(k, T - i + 1) \tag{5.7}$$

Hence, with the completion of this module, one encryption round completes successfully. Then *D* moves towards the 1st module (random pixel insertion) for the second round. Four rounds of these modules are performed. Finally, we get the required encrypted bits.

In the fourth step, the algorithm applies the *XOR* operation on the LSB's and the new chaotic system.

In the fifth step, the algorithm merges the resulted bits of the 3rd and 4th steps. The resulted image is the encrypted image.

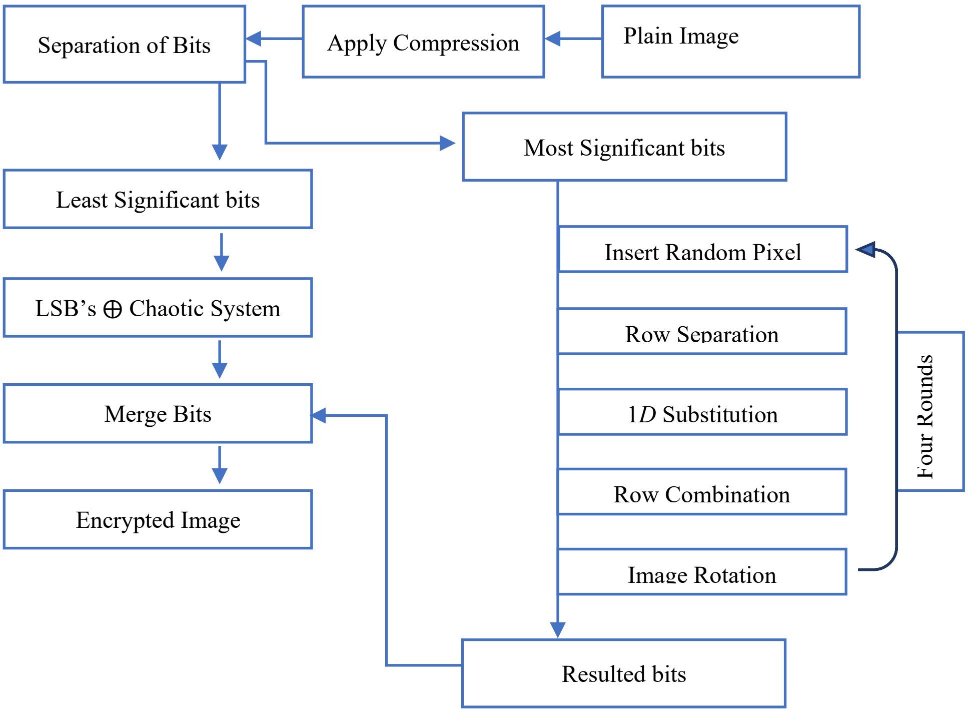


Figure 5.3: Flowchart of the proposed algorithm

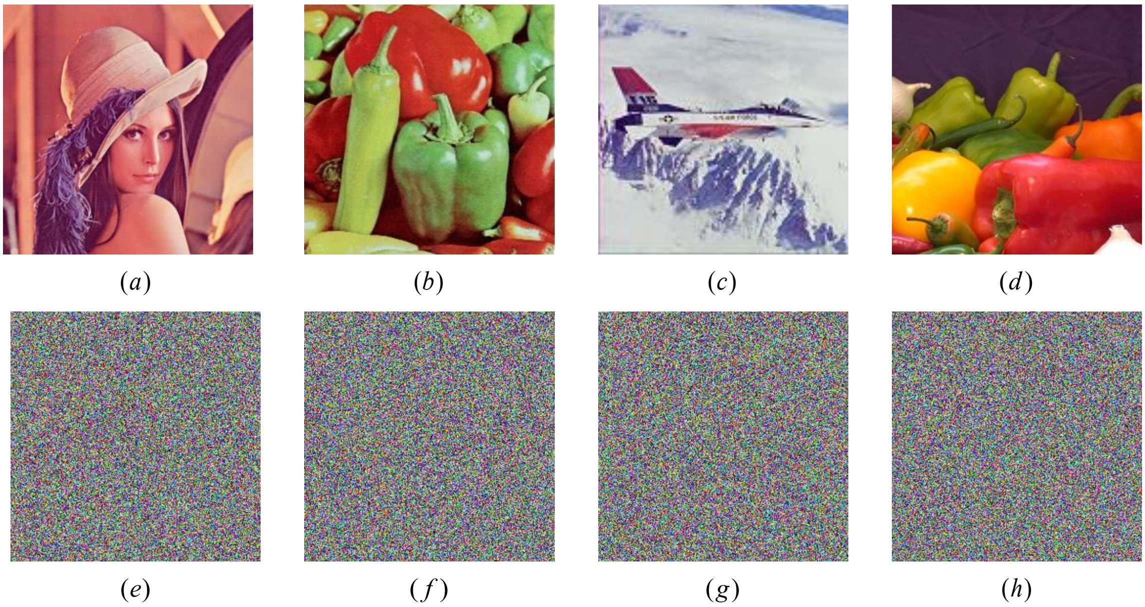


Figure 5.4: Experimental outcomes.

5.4(*a*-*d*): Plain images; 5.4(*e*-*h*): encrypted images

5.4. Simulation results and discussions

The security analysis uncovers that the cryptosystem holds certain serious security defects and is incapable to secure encrypted content. There are lot of statistical analyses that are used to evaluate secure encrypted content.

In this research, standard color images of "Lena", "Peppers", "Mandrill", and "Deblur" have been used as test images.

5.4.1. Security Analyses

To examine the security strength of the proposed scheme, we performed different analyses on it. The detail of these analyses on the proposed scheme is discussed comprehensively.

5.4.1.1. Key sensitivity

It is very significant to observe the effect of slightly different keys in the algorithm [55]. To analyze this effect of the proposed algorithm, two keys are used for encryption. These keys are:

$$\begin{aligned}&K_1:\\&S(0,0)=0.5, r=[0.5,1,1.5,2,2.5]\\&K_2:\\&S(0,0)=0.97542, r=[0.50000001,0.5,1,1.5,2,2.5]\end{aligned}$$

The same keys will be used for the decryption process to get the respective case results. The encryption of the same image using two slightly different keys is shown in Fig. 5.6.

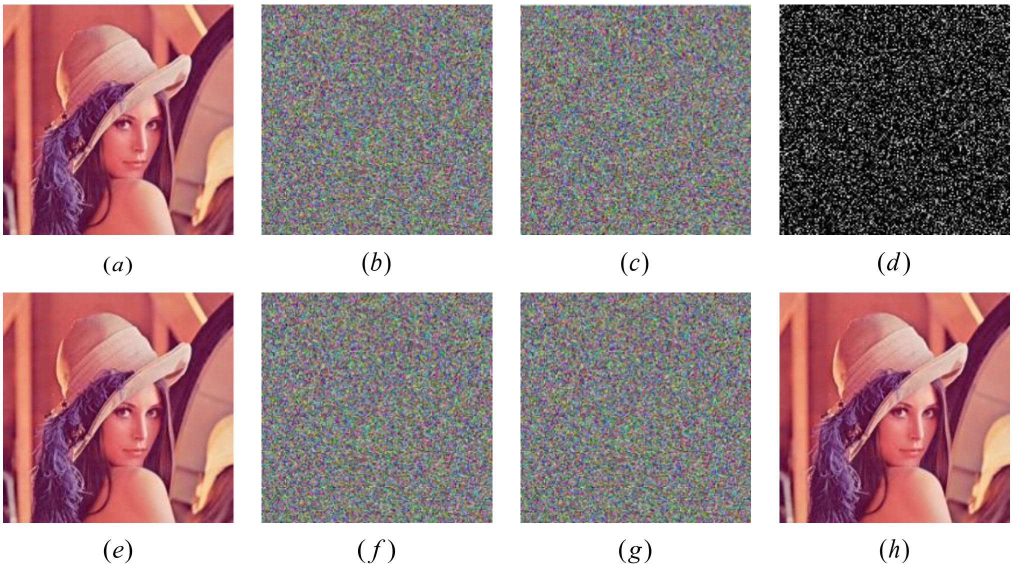


Figure 5.6: Key sensitivity analysis

In the above figure, the plain image is symbolized by (*a*); Encryption using keys K_1 and K_2 are symbolized by (*b*) and (*c*) respectively, while the difference between both encryptions is symbolized by (*d*). On decryption of (*b*) and (*c*) with K_1 and K_2, respectively, the original images are obtained by using different keys, decrypted images are not as the original image which is shown in Fig. 5.6(*e*) to Fig. 5.6(*h*).

5.4.1.2. Histogram analysis

The histogram analysis is presented to evaluate the uniform distribution of ciphered [54]. A cryptosystem has a high resistance to statistical attacks if the probability of each gray value in the uniform histogram is the same [54].

In Fig. 5.7, the original, ciphered, and their corresponding histograms are displayed. These histograms demonstrate that the pixels of the ciphered images are more evenly spread than the original images. This aspect ensures that the proposed scheme has high resistive capability against differential, plaintext, and statistical attacks.

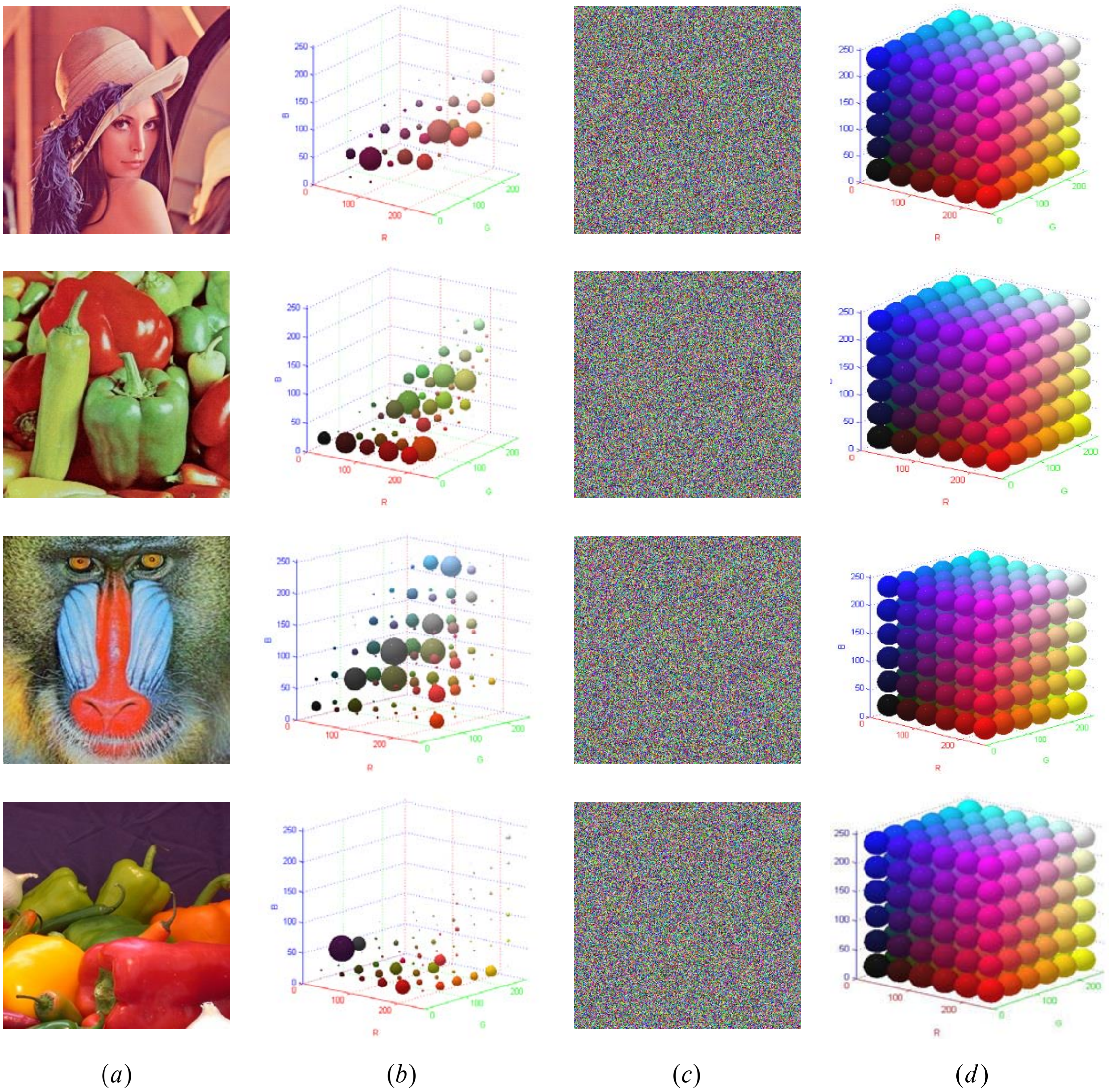


Figure 5.7: Histogram analysis.
5.7(*a*): plain images; 5.7(*b*): corresponding histograms; 5.7(*c*): encrypted images; 5.7(*d*): corresponding histograms

5.4.1.3. Information entropy

Information entropy analysis is used to calculate the randomness of an image [54], [61]. The Information entropy analysis of a perfectly random grayscale image (with pixel values in the range [0,255]) is 8, so if the resulting image has its information entropy equal to 8 or close to 8, we have a strong encryption method. The results, we obtained from the proposed algorithm are analyzed in Table 5.2.

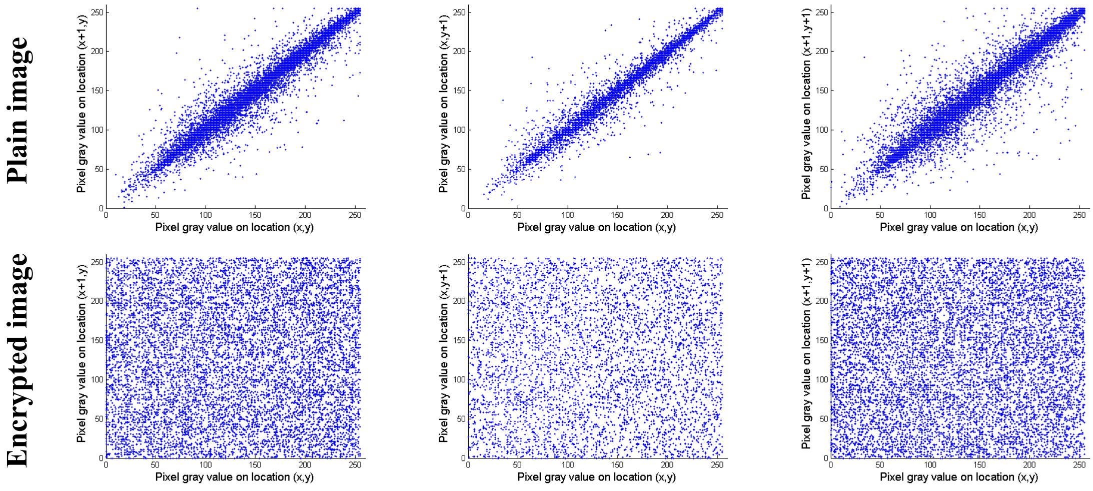
Table 5.2: Information entropy analysis

Name	Entropy	Proposed	**Ref.** [23]	**Ref.** [95]	**Ref.** [96]
Lena	7.7849	7.9983	7.9821	7.9278	7.9807
Pepper	7.7383	7.9989	7.9811	7.9744	7.9879
Baboon	7.6831	7.9975	7.9807	7.9705	7.9845

5.4.1.4. Correlation analysis

In an image that is not encrypted, the color dissolve into the dark to lighter shades which makes the pixel values correlated with its neighbouring [63]. Applying the encryption, we try to break every relation in the image's pixels which makes the values go random.

Therefore, for an encryption system to be strong, the value from the above equation will be equal to or close to zero. In Table 5.3, the results of the correlation coefficient are presented and compared with some schemes. Fig. 5.8 shows the correlation distribution of original and encrypted images in horizontal, vertical, and diagonal directions. The test image Lena.jpg gives high correlation values and all the encrypted images are very close to zero.



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

Figure 5.8: The correlation coefficient.

5.8(*a*): Horizontal correlation; 5.8(*b*): Vertical correlation; 5.8(*c*): Diagonal correlation

Table 5.3: Comparison of Correlation Analysis

Algorithms	Images	Encrypted Images		
		Horizontal	Vertical	Diagonal
Proposed	Peppers	0.0007	0.0008	-0.0009
Ref. [97]	Peppers	0.0038	0.0023	0.0009
Ref. [75]	Peppers	0.0064	0.0092	0.0010
Ref. [98]	Peppers	0.0094	0.0894	0.0542
Proposed	Lena	0.0064	-0.0177	-0.0059
Ref. [96]	Lena	0.0075	0.0041	0.0002
Ref. [99]	Lena	0.1257	0.0581	0.0504
Ref. [100]	Lena	-0.0580	-0.0024	-0.0170

5.4.1.5. Differential Attacks

The number of Pixels Changing Rate (NPCR) and the Unified Averaged Changing Intensity (UACI) are the two most regular measures used to evaluate the quality of image encryption [54]. A high NPCR and UACI demonstrate high protection from differential attacks.

A security system has good resistance against differential attacks if its NPCR and UACI are very close to 99.60 and 33.40, respectively. The results of NPCR and UACI are presented in Table 5.4. This ensures that the proposed algorithm is highly secure against differential attacks.

Table 5.4: NPCR and UACI results

Image	NPCR	UACI
Boat	99.6465	33.4587
Lena	99.5863	33.4476
Baboon	99.5968	33.3768
Pepper	99.6211	33.3816

5.4.1.6. Energy, contrast, and homogeneity

To testify the encryption quality, the energy, the contrast, and homogeneity analyses are evaluated. The outcomes of these analyses are presented in Table 5.5.

Table 5.5: The contrast, homogeneity, and energy analyses

Analysis	**Lena Image**	
	Host	Encrypted
Contrast	0.7904	10.3173
Homogeneity	0.8114	0.3918
Energy	0.1188	0.0157
	Peppers Image	
	Host	Encrypted
Contrast	0.5271	2.7808
Homogeneity	0.8597	0.5322
Energy	0.1244	0.0402

5.5. Internal Comparison of Proposed Algorithms

Four encryption algorithms are proposed in this thesis. All algorithms show optimum output of all statistical and security analyses. Additionally, first ecryption algorithm encrypts channel wise single and multi-color images to enhance the data security. Second encryption algorithm is applicable for single color images with different encryption approach as compared to first encryption algorithm. The third and fourth encryption algorithm uses data compression to squeeze the data and then encryption is performed. These two algorithms are helpful to reduce the storage cost and to improve the data transfer rate.

Chapter 6

Conclusion

In the beginning, a 3*D* chaotic map is presented. The chaotic behaviour of a chaotic map is outstanding. The chaotic behaviour is judged through histograms. Due to the randomness property of this chaotic map, it is very useful for S-box construction. For this purpose, we present an S-box construction scheme. The proposed S-box is then critically analysed and its comparison with some currently constructed S-boxes is presented. From the analysis, the proposed S-box has good nonlinearity and SAC, BIC, LP, and DP are also close to optimal values. Statistical analyses are also analysed to judge the suitability of the constructed S-box in image encryption applications. The statistical analyses of the proposed S-box are excellent. The anticipated S-box is very effective in image encryption. From algebraic and statistical analyses, the proposed S-box is outstanding in cryptographic properties.

Another construction of S-boxes is presented in this chapter. Again, a 3*D* chaotic map is used as a source of a random number generator. Interestingly, each dimension of the chaotic map constructs one S-box as the algorithm runs once. So, we obtained three S-boxes and by running the algorithm again and again, a bunch of S-boxes can be obtained. For analyses, we just analysed three S-boxes as a sample. The algebraic analyses of these sample S-boxes are good, and the statistical analyses are also impressive. The analyses show that the proposed S-boxes are suitable for any cryptosystem.

Applications in image encryption of constructed S-boxes in Chapter 2 are presented in Chapter 3. Two image encryption techniques are presented. The first image encryption technique is the multi-image encryption technique and the single image encryption technique. The proposed encryption scheme consists of four steps. The first step is to separate the red, green, and blue channels. Second step permutation RGB channels row wise and column wise. This step induced diffusion in the scheme. In the third step, the S-boxes are constructed using a chaotic map and in the fourth step, the S-box is substituted in each RGB channel. This step induced confusion in the encryption scheme. The proposed scheme is critically analysed with the help of standard analyses. The encryption scheme has a large key space, sensitive with key, highly random and the relationship between pixels is broken. These features demonstrate that the proposed scheme is adoptable and has high resistance to different cryptanalysis.

The second encryption scheme consists of three steps. The first three S-boxes are constructed utilizing the $3D$ chaotic map mentioned in Chapter 2 second construction. In the first step, pixels are XOR with S-box 1 entries. In the second step, permute the pixels row-wise and substitute the entries of S-box 2. In the last step, permute the pixels column wise and substitute S-box entries. The last two steps induced confusion and diffusion in this encryption scheme. The security analyses of the anticipated scheme are made and comparisons with the latest and classical encryption schemes are presented. From the security analyses, the proposed scheme is more secure in comparison to other encryption algorithms.

Small S-boxes are vital in light-weight cryptography. The Small S-boxes construction technique and its application in image encryption are presented in Chapter 4. The small S-box is constructed by utilizing linear fractional transformation. The designed S-box fulfils algebraic analysis and preserves all cryptographic properties. An image scheme is proposed using compression, chaotic map, and S-box. Compression is applied for the purpose of making big data small, and it also increases the effectiveness of the algorithm because compression is also a weak encryption itself. A two-dimensional chaotic map is applied to randomize the pixels. This action gives rise to diffusion in the encryption algorithm. The constructed S-box is substituted to create confusion in the algorithm. Security analyses are conducted to judge the strength of an algorithm. From security analyses proposed scheme fulfils all the requirements of the image encryption algorithm.

The last chapter is devoted to analysing a chaotic oscillator generated by the Legendre differential equation, which produces confusion and diffusion in the plaintext message to achieve the desired secrecy. The produced chaotic sequence of random numbers from the dynamical system is utilized to scramble the pixels of an image to get an encrypted image. The proposed encryption scheme consists of five modules. These modules are random pixel insertion, row separation, $1D$ substitution, row combination, and image rotation. $1D$ substitution provides confusion and all other modules provide diffusion. The proposed scheme is highly sensitive and has a large key space. The security analyses of the proposed scheme are excellent and are better in comparison with the latest scheme present in literature.

References

[1] C. E. Shannon, “Communication theory of secrecy systems. 1945.,” *MD. Comput.*, vol. 15, no. 1, pp. 57–64, 1998.

[2] A. U. Rehman, J. S. Khan, J. Ahmad, and S. O. Hwang, “A New Image Encryption Scheme Based on Dynamic S-Boxes and Chaotic Maps,” *3D Res.*, vol. 7, no. 1, pp. 1–8, Mar. 2016, doi: 10.1007/s13319-016-0084-9.

[3] S. S. Jamal, M. U. Khan, and T. Shah, “A Watermarking Technique with Chaotic Fractional S-Box Transformation,” *Wirel. Pers. Commun.*, vol. 90, no. 4, pp. 2033–2049, Oct. 2016, doi: 10.1007/s11277-016-3436-0.

[4] L. Burmett, “Heuristic Optimization of boolean functions and substitution boxes for cryptography,” QUT, 2005.

[5] L. Kocarev, “chaos based Cryptography: A Brief Overview,” *Circuits Syst. Mag. IEEE*, vol. 1, no. 3, pp. 6–21, 2001.

[6] I. Hussain and T. Shah, “Literature survey on nonlinear components and chaotic nonlinear components of block ciphers,” *Nonlinear Dynamics*, vol. 74, no. 4. pp. 869–904, Dec. 2013, doi: 10.1007/s11071-013-1011-8.

[7] F. Dachselt and W. Schwarz, “Chaos and cryptography,” *IEEE Trans Circuits Syst*, vol. 48, no. 12, pp. 1498–509, 2001.

[8] Attaullah, A. Javeed, and T. Shah, “Cryptosystem techniques based on the improved Chebyshev map: an application in image encryption,” *Multimed. Tools Appl.*, vol. 78, no. 22, pp. 31467–31484, Nov. 2019, doi: 10.1007/s11042-019-07981-8.

[9] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, “Generalized majority logic criterion to analyze the statistical strength of s-boxes,” *Zeitschrift fur Naturforsch. - Sect. A J. Phys. Sci.*, vol. 67, no. 5, pp. 282–288, 2012, doi: 10.5560/ZNA.2012-0022.

[10] Y. Wu *et al.*, *No Title*, vol. 21, no. 1. SPIE-Intl Soc Optical Eng, 2012, p. 013014.

[11] A. Rukhin *et al.*, “A statistical test suit for random and pseudo random number generators for cryptographic applications,” *NIST Spec. Publ. 800-22*, 2001.

[12] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, “2D Sine Logistic modulation map for image encryption,” *Inf. Sci. (Ny).*, vol. 297, pp. 80–94, 2015, doi: 10.1016/j.ins.2014.11.018.

[13] A. Ullah, S. S. Jamal, and T. Shah, “A novel construction of substitution box using a combination of chaotic maps with improved chaotic range,” *Nonlinear Dyn.*, 2017, doi: 10.1007/s11071-017-3409-1.

[14] G. P. Williams, *Chaos Theory Tamed*. A Joseph Henry Press Book, 1997.

[15] R. May, “Simple mathematical models with very complicated dynamics,” *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[16] N. K. Pareek, V. Patidar, and K. K. Sud, “Image encryptoin using chaotic logistic map,” *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[17] R. L. Devaney, *Fractal pattern arising in chaotic dynamical systems, The Science of Fractal Images*. 1988.

[18] M. Khan and Z. Asghar, “No Title,” *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. , doi: 10.1007/s00521-016-2511-5.

[19] M. Henon, “A two-dimentional mapping with a strange attractor,” *Commun. Math. Phys.*, vol. 50, no. 1, pp. 69–77, 1976.

[20] M. Khan, T. Shah, and S. I. Batool, “Construction of S-box based on chaotic Boolean functions and its application in image encryption,” *Neural Comput. Appl.*, vol. 27, no. 3, pp. 677–685, Apr. 2016, doi: 10.1007/s00521-015-1887-y.

[21] G. Jakimoski and L. Kocarev, “Chaos and Cryptography: Block Encryption Ciphers Based on Chaotic Maps,” 2001.

[22] J. Daemen and V. Rijmen, *The design of Rijndael : AES--the Advanced Encryption Standard*. Springer, 2002.

[23] Y. Zhou, L. Bao, and C. L. P. Chen, “A new 1D chaotic system for image encryption,” *Signal Processing*, vol. 97, pp. 172–182, 2014, doi: 10.1016/j.sigpro.2013.10.034.

[24] P. E. Trahanias and A. N. Venetsanopoulos, “Color image enhancement through 3-D histogram equalization,” *Proc. - Int. Conf. Pattern Recognit.*, vol. 3, pp. 545–548, 1992, doi: 10.1109/ICPR.1992.202045.

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

[26] I. Hussain, T. Shah, and M. A. Gondal, “A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm,” *Nonlinear Dyn.*, vol. 70, no. 3, pp. 1791–1794, 2012, doi: 10.1007/s11071-012-0573-1.

[27] F. Özkaynak, “Construction of robust substitution boxes based on chaotic systems,” *Neural Comput. Appl.*, vol. 31, no. 8, pp. 3317–3326, 2019, doi: 10.1007/s00521-017-3287-y.

[28] A. Belazi and A. A. A. El-Latif, “A simple yet efficient S-box method based on chaotic sine map,” *Optik (Stuttg).*, vol. 130, pp. 1438–1444, 2017, doi:

10.1016/j.ijleo.2016.11.152.

[29] Y. Naseer, T. Shah, D. Shah, and S. Hussain, “A Novel Algorithm of Constructing Highly Nonlinear S-p-boxes,” *Cryptography*, vol. 3, no. 1, p. 6, Jan. 2019, doi: 10.3390/cryptography3010006.

[30] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, “Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption,” *Nonlinear Dyn.*, vol. 87, no. 1, pp. 337–361, Jan. 2017, doi: 10.1007/s11071-016-3046-0.

[31] I. Hussain, M. A. Gondal, and A. Hussain, “Construction of Substitution Box Based on Piecewise Linear Chaotic Map and S8 Group,” *3D Res.*, vol. 6, no. 1, pp. 1–5, Mar. 2015, doi: 10.1007/s13319-014-0032-5.

[32] G. Tang, X. Liao, and Y. Chen, “A novel method for designing S-boxes based on chaotic maps,” *Chaos, Solitons and Fractals*, vol. 23, no. 2, pp. 413–419, Jan. 2005, doi: 10.1016/j.chaos.2004.04.023.

[33] F. Özkaynak and A. B. Özer, “A method for designing strong S-Boxes based on chaotic Lorenz system,” *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 374, no. 36, pp. 3733–3738, Aug. 2010, doi: 10.1016/j.physleta.2010.07.019.

[34] A. Altaleb, M. S. Saeed, I. Hussain, and M. Aslam, “An algorithm for the construction of substitution box for block ciphers based on projective general linear group,” *AIP Adv.*, vol. 7, no. 3, Mar. 2017, doi: 10.1063/1.4978264.

[35] M. Khan, T. Shah, H. Mahmood, and M. A. Gondal, “An efficient method for the construction of block cipher with multi-chaotic systems,” *Nonlinear Dyn.*, vol. 71, no. 3, pp. 489–492, Feb. 2013, doi: 10.1007/s11071-012-0675-9.

[36] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, “Statistical analysis of S-box in image encryption applications based on majority logic criterion,” *Int. J. Phys. Sci.*, vol. 6, no. 16, pp. 4110–4127, 2011, [Online]. Available: http://www.academicjournals.org/IJPS.

[37] National Institute of Standards and Technology, “SKIPJACK and KEA Algorithm Specifications.” pp. 1–23, 1998, [Online]. Available: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:SKIPJACK+and+KEA+Algorithm+Specifications#2.

[38] B. Wang, B. F. Zhang, and X. W. Liu, “An image encryption approach on the basis of a time delay chaotic system,” *Optik (Stuttg).*, vol. 225, no. September 2020, p. 165737, 2021, doi: 10.1016/j.ijleo.2020.165737.

[39] A. Babaei, H. Motameni, and R. Enayatifar, “A new permutation-diffusion-based

image encryption technique using cellular automata and DNA sequence," *Optik (Stuttg).*, vol. 203, p. 164000, 2020, doi: 10.1016/j.ijleo.2019.164000.

[40] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik (Stuttg).*, vol. 147, pp. 88–102, 2017, doi: 10.1016/j.ijleo.2017.08.028.

[41] A. A. A. EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "Controlled alternate quantum walk-based pseudo-random number generator and its application to quantum color image encryption," *Phys. A Stat. Mech. its Appl.*, vol. 547, p. 123869, 2020, doi: 10.1016/j.physa.2019.123869.

[42] M. Wang, Y. Pousset, P. Carré, C. Perrine, N. Zhou, and J. Wu, "Optical image encryption scheme based on apertured fractional Mellin transform," *Opt. Laser Technol.*, vol. 124, no. November 2019, p. 106001, 2020, doi: 10.1016/j.optlastec.2019.106001.

[43] A. Vaish and M. Kumar, "Color image encryption using MSVD, DWT and Arnold transform in fractional Fourier domain," *Optik (Stuttg).*, vol. 145, pp. 273–283, 2017, doi: 10.1016/j.ijleo.2017.07.041.

[44] Z. Zhuang *et al.*, "Image Encryption Using Josephus Problem and Filtering Diffusion," *Nonlinear Dyn.*, vol. 8, no. 1, pp. 8660–8674, Dec. 2019, doi: 10.1016/j.optcom.2009.02.044.

[45] T.-Y. Li and J. A. Yorke, "Period Three Implies Chaos," *Am. Math. Mon.*, vol. 82, no. 10, p. 985, 1975, doi: 10.2307/2318254.

[46] Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over Blockchain," *Opt. Laser Technol.*, vol. 135, no. February 2020, p. 106610, 2021, doi: 10.1016/j.optlastec.2020.106610.

[47] X. Y. Wang and Z. M. Li, "A color image encryption algorithm based on Hopfield chaotic neural network," *Opt. Lasers Eng.*, vol. 115, no. July 2018, pp. 107–118, Apr. 2019, doi: 10.1016/j.optlaseng.2018.11.010.

[48] F. Hu, X. Xu, T. Peng, C. Pu, and L. Li, "A fast pseudo-stochastic sequential cipher generator based on RBMs," *Neural Comput. Appl.*, vol. 30, no. 4, pp. 1277–1287, 2018, doi: 10.1007/s00521-016-2753-2.

[49] K. Ratnavelu, M. Kalpana, P. Balasubramaniam, K. Wong, and P. Raveendran, "Image encryption method based on chaotic fuzzy cellular neural networks," *Signal Processing*, vol. 140, pp. 87–96, 2017, doi: 10.1016/j.sigpro.2017.05.002.

[50] N. Bigdeli, Y. Farid, and K. Afshar, “A novel image encryption/decryption scheme based on chaotic neural networks,” *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 753–765, 2012, doi: 10.1016/j.engappai.2012.01.007.

[51] W. Huang, D. Jiang, Y. An, L. Liu, and X. Wang, “A novel double-image encryption algorithm based on Rossler hyperchaotic system and compressive sensing,” *IEEE Access*, vol. 9, 2021, doi: 10.1109/ACCESS.2021.3065453.

[52] L. Lidong, D. Jiang, X. Wang, L. Zhang, and X. Rong, “A Dynamic Triple-Image Encryption Scheme Based on Chaos, S-Box and Image Compressing,” *IEEE Access*, vol. 8, pp. 210382–210399, 2020, doi: 10.1109/ACCESS.2020.3039891.

[53] K. A. K. Patro, A. Soni, P. K. Netam, and B. Acharya, “Multiple grayscale image encryption using cross-coupled chaotic maps,” *J. Inf. Secur. Appl.*, vol. 52, p. 102470, 2020, doi: 10.1016/j.jisa.2020.102470.

[54] Y. Naseer, D. Shah, and T. Shah, “A novel approach to improve multimedia security utilizing 3D mixed chaotic map,” *Microprocess. Microsyst.*, vol. 65, pp. 1–6, 2019, doi: 10.1016/j.micpro.2018.12.003.

[55] S. M. Pan, R. H. Wen, Z. H. Zhou, and N. R. Zhou, “Optical multi-image encryption scheme based on discrete cosine transform and nonlinear fractional Mellin transform,” *Multimed. Tools Appl.*, vol. 76, no. 2, pp. 2933–2953, 2017, doi: 10.1007/s11042-015-3209-x.

[56] D. S. Malik and T. Shah, “Color multiple image encryption scheme based on 3D-chaotic maps,” *Math. Comput. Simul.*, vol. 178, pp. 646–666, Dec. 2020, doi: 10.1016/j.matcom.2020.07.007.

[57] H. Yang, K. W. Wong, X. Liao, W. Zhang, and P. Wei, “A fast image encryption and authentication scheme based on chaotic maps,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 15, no. 11, pp. 3507–3517, 2010, doi: 10.1016/j.cnsns.2010.01.004.

[58] L. Liu, D. Jiang, T. An, and Y. Guan, “A Plaintext-Related Dynamical Image Encryption Algorithm Based on Permutation-Combination-Diffusion Architecture,” *IEEE Access*, vol. 8, pp. 62785–62799, 2020, doi: 10.1109/ACCESS.2020.2983716.

[59] T. ul Haq and T. Shah, “12×12 S-box Design and its Application to RGB Image Encryption,” *Optik (Stuttg).*, vol. 217, no. May, p. 164922, 2020, doi: 10.1016/j.ijleo.2020.164922.

[60] F. Pareschi, R. Rovatti, and G. Setti, “On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution,” *IEEE Trans. Inf. Forensics Secur.*, vol. 7, no. 2, pp. 491–505, 2012, doi: 10.1109/TIFS.2012.2185227.

[61] Y. Wu, J. P. Noonan, and S. Agaian, “NPCR and UACI Randomness Tests for Image Encryption,” *Cyberjournals.Com*, 2011, [Online]. Available: http://www.cyberjournals.com/Papers/Apr2011/05.pdf.

[62] G. Hanchinamani and L. Kulkarni, “An Efficient Image Encryption Scheme Based on a Peter De Jong Chaotic Map and a RC4 Stream Cipher,” *3D Res.*, vol. 6, no. 3, 2015, doi: 10.1007/s13319-015-0062-7.

[63] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat, “IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata,” *Multimed. Tools Appl.*, no. 1998, 2020, doi: 10.1007/s11042-020-09880-9.

[64] A. Girdhar and V. Kumar, “A RGB image encryption technique using Lorenz and Rossler chaotic system on DNA sequences,” *Multimed. Tools Appl.*, vol. 77, no. 20, pp. 27017–27039, 2018, doi: 10.1007/s11042-018-5902-z.

[65] X. Wei, L. Guo, Q. Zhang, J. Zhang, and S. Lian, “A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system,” *J. Syst. Softw.*, vol. 85, no. 2, pp. 290–299, 2012, doi: 10.1016/j.jss.2011.08.017.

[66] A. Ullah, S. S. Jamal, and T. Shah, “A novel scheme for image encryption using substitution box and chaotic system,” *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, Jan. 2018, doi: 10.1007/s11071-017-3874-6.

[67] Z. Hua and Y. Zhou, “Exponential Chaotic Model for Generating Robust Chaos,” *IEEE Trans. Syst. Man, Cybern. Syst.*, pp. 1–12, Aug. 2019, doi: 10.1109/tsmc.2019.2932616.

[68] Y. Wu, G. Yang, H. Jin, and J. P. Noonan, “Image Encryption using the Two-dimensional Logistic Chaotic Map.” [Online]. Available: https://sites.google.com/site/tuftsyuewu/source-code.

[69] L. Y. Zhang, X. Hu, Y. Liu, K. W. Wong, and J. Gan, “A chaotic image encryption scheme owning temp-value feedback,” *Commun. Nonlinear Sci. Numer. Simul.*, vol. 19, no. 10, pp. 3653–3659, 2014, doi: 10.1016/j.cnsns.2014.03.016.

[70] X. Wu, J. Kurths, and H. Kan, “A robust and lossless DNA encryption scheme for color images,” *Multimed. Tools Appl.*, vol. 77, no. 10, pp. 12349–12376, May 2018, doi: 10.1007/s11042-017-4885-5.

[71] A. Kadir, M. Aili, and M. Sattar, “Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections,” *Optik (Stuttg).*, vol. 129, pp. 231–238, Jan. 2017, doi: 10.1016/j.ijleo.2016.10.036.

[72] X. Wu, H. Kan, and J. Kurths, "A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps," *Appl. Soft Comput. J.*, vol. 37, pp. 24–39, Dec. 2015, doi: 10.1016/j.asoc.2015.08.008.

[73] R. J. Chen and S. J. Horng, "Novel SCAN-CA-based image security system using SCAN and 2-D von Neumann cellular automata," *Signal Process. Image Commun.*, vol. 25, no. 6, pp. 413–426, 2010, doi: 10.1016/j.image.2010.03.002.

[74] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-Gray code for image systems," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 515–529, Apr. 2013, doi: 10.1109/TSMCB.2012.2210706.

[75] X. Liao, S. Lai, and Q. Zhou, "A novel image encryption algorithm based on self-adaptive wave transmission," *Signal Processing*, vol. 90, no. 9, pp. 2714–2722, Sep. 2010, doi: 10.1016/j.sigpro.2010.03.022.

[76] T. H. Chen and K. C. Li, "Multi-image encryption by circular random grids," *Inf. Sci. (Ny).*, vol. 189, pp. 255–265, 2012, doi: 10.1016/j.ins.2011.11.026.

[77] T. H. Chen and C. S. Wu, "Compression-unimpaired batch-image encryption combining vector quantization and index compression," *Inf. Sci. (Ny).*, vol. 180, no. 9, pp. 1690–1701, May 2010, doi: 10.1016/j.ins.2009.12.021.

[78] L. Li, A. A. Abd El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," *Signal Processing*, vol. 92, no. 4, pp. 1069–1078, Apr. 2012, doi: 10.1016/j.sigpro.2011.10.020.

[79] B. Carpentieri, "Efficient compression and encryption for digital data transmission," *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/9591768.

[80] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," *J. Electr. Comput. Eng.*, 2012, doi: 10.1155/2012/179693.

[81] A. Javeed, T. Shah, and A. Ullah, "A color image privacy scheme established on nonlinear system of coupled differential equations," *Multimed. Tools Appl.*, vol. 79, no. 43–44, pp. 32487–32501, Nov. 2020, doi: 10.1007/s11042-020-09582-2.

[82] S. Bukhari, A. Yousaf, S. Niazi, and M. R. Anjum, "The Nucleus A Novel Technique for the Generation and Application of Substitution Boxes (s-box) for the Image Encryption," 2018. [Online]. Available: www.thenucleuspak.org.pk.

[83] T. Shah and D. Shah, "Construction of highly nonlinear S-boxes for degree 8 primitive irreducible polynomials over ℤ2," *Multimed. Tools Appl.*, vol. 78, no. 2, pp. 1219–1234, Jan. 2019, doi: 10.1007/s11042-018-6250-8.

[84] R. Gupta, M. Kumar, and R. Bathla, "Data Compression - Lossless and Lossy

Techniques," *Int. J. Appl. or Innov. Enginnerring Manag.*, vol. 5, no. 7, pp. 120–125, 2016.

[85] I. Hussain, A. Anees, T. A. Al-Maadeed, and M. T. Mustafa, "A novel encryption algorithm using multiple semifield S-boxes based on permutation of symmetric group," Apr. 2020, [Online]. Available: http://arxiv.org/abs/2004.12264.

[86] A. Rafiq and M. Khan, "Construction of new S-boxes based on triangle groups and its applications in copyright protection," *Multimed. Tools Appl.*, vol. 78, no. 11, pp. 15527–15544, Jun. 2019, doi: 10.1007/s11042-018-6953-x.

[87] G. . Sathishkumar, K. Bhoopathy bagan, and N. Sriraam, "Image Encryption Based On Diffusion And Multiple Chaotic Maps," *Int. J. Netw. Secur. Its Appl.*, vol. 3, no. 2, pp. 181–194, Mar. 2011, doi: 10.5121/ijnsa.2011.3214.

[88] Z. Hua, S. Yi, Y. Zhou, C. Li, and Y. Wu, "Designing Hyperchaotic Cat Maps with Any Desired Number of Positive Lyapunov Exponents," *IEEE Trans. Cybern.*, vol. 48, no. 2, pp. 463–473, Feb. 2018, doi: 10.1109/TCYB.2016.2642166.

[89] H. Zhu, W. Qi, J. Ge, and Y. Liu, "Analyzing Devaney Chaos of a Sine-Cosine Compound Function System," *Int. J. Bifurc. Chaos*, vol. 28, no. 14, Dec. 2018, doi: 10.1142/S0218127418501766.

[90] S. S. Jamal, A. Anees, M. Ahmad, M. F. Khan, and I. Hussain, "Construction of Cryptographic S-Boxes Based on Mobius Transformation and Chaotic Tent-Sine System," *IEEE Access*, vol. 7, pp. 173273–173285, Nov. 2019, doi: 10.1109/access.2019.2956385.

[91] M. Farajallah, "Chaos-based crypto and joint crypto-compression systems for images and videos." [Online]. Available: https://hal.archives-ouvertes.fr/tel-01179610.

[92] S. El Assad and M. Farajallah, "A new chaos-based image encryption system," *Signal Process. Image Commun.*, vol. 41, pp. 144–157, Feb. 2016, doi: 10.1016/j.image.2015.10.004.

[93] G. A. Gottwald and I. Melbourne, "The 0-1 Test for Chaos: A review."

[94] G. A. Gottwald and I. Melbourne, "On the validity of the 0-1 test for chaos," *Nonlinearity*, vol. 22, no. 6, pp. 1367–1382, 2009, doi: 10.1088/0951-7715/22/6/006.

[95] K. A. K. Patro and B. Acharya, "Secure multi–level permutation operation based multiple colour image encryption," *J. Inf. Secur. Appl.*, vol. 40, pp. 111–133, Jun. 2018, doi: 10.1016/j.jisa.2018.03.006.

[96] C. Y. Song, Y. L. Qiao, and X. Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," *Optik (Stuttg).*, vol. 124, no. 18, pp. 3329–3334, Sep. 2013,

doi: 10.1016/j.ijleo.2012.11.002.

[97] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, “A novel algorithm for image encryption based on mixture of chaotic maps,” *Chaos, Solitons and Fractals*, vol. 35, no. 2, pp. 408–419, Jan. 2008, doi: 10.1016/j.chaos.2006.05.011.

[98] G. Chen, Y. Mao, and C. K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps,” *Chaos, Solitons and Fractals*, vol. 21, no. 3, pp. 749–761, Jul. 2004, doi: 10.1016/j.chaos.2003.12.022.

[99] C. K. Huang and H. H. Nien, “Multi chaotic systems based pixel shuffle for image encryption,” *Opt. Commun.*, vol. 282, no. 11, pp. 2123–2127, 2009, doi: 10.1016/j.optcom.2009.02.044.

[100] H. Liu, X. Wang, and A. Kadir, “Color image encryption using Choquet fuzzy integral and hyper chaotic system,” *Optik (Stuttg).*, vol. 124, no. 18, pp. 3527–3533, Sep. 2013, doi: 10.1016/j.ijleo.2012.10.068.

Turnitin Originality Report

Design of Symmetric Key Cryptosystems Based on Chaos and Algebra: Applications in Image Processing by Muhammad Tanveer .

From CL QAU (DRSML)

- Processed on 06-Oct-2022 14:30 PKT
- ID: 1918116233
- Word Count: 24785

Similarity Index
19%
Similarity by Source

Internet Sources:
10%
Publications:
15%
Student Papers:
3%

sources:

1 1% match (Internet from 23-Sep-2022)

https://www.researchgate.net/publication/341363349_Lightweight_secure_image_encryption_scheme_based_on_chaotic_differential_equation

2 1% match (Tanveer ul Haq, Tariq Shah. "4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion", Journal of Information Security and Applications, 2021)

Tanveer ul Haq, Tariq Shah. "4D mixed chaotic system and its application to RGB image encryption using substitution-diffusion", Journal of Information Security and Applications, 2021

3 1% match (student papers from 27-Aug-2018)

Submitted to Higher Education Commission Pakistan on 2018-08-27

4 1% match (Tariq Shah, Tanveer ul Haq, Ghazanfar Farooq. "Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation", IEEE Access, 2020)

Tariq Shah, Tanveer ul Haq, Ghazanfar Farooq. "Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation", IEEE Access, 2020

5 1% match (Dawood Shah, Tariq Shah. "Binary Galois Field Extensions Dependent Multimedia Data Security Scheme", Microprocessors and Microsystems, 2020)

Dawood Shah, Tariq Shah. "Binary Galois Field Extensions Dependent Multimedia Data Security Scheme", Microprocessors and Microsystems, 2020

6 < 1% match (Internet from 23-Sep-2022)

https://www.researchgate.net/publication/347530617_An_image_encryption_approach_on_the_basis_of_a_time_delay_chaotic_system

7 < 1% match (Internet from 23-Sep-2022)

https://www.researchgate.net/publication/223564440_A_fast_image_encryption_and_authentication_scheme_based_on_chaotic_maps

8 < 1% match (Internet from 23-Sep-2022)

https://www.researchgate.net/publication/355122987_Secure_and_Fast_Image_Encryption_Algorithm_Using_Hyper-Chaos-Based_Key_Generator_and_Vector_Operation/fulltext/615eef205a481543a88ff6e4/355122987_Secure_and_Fast_Image_Encryption_Algorith Chaos-Based_Key_Generator_and_Vector_Operation.pdf

9 < 1% match (Internet from 18-Mar-2022)

https://www.researchgate.net/publication/358823219_RGB_Image_Encryption_through_Cellular_Automata_S-Box_and_the_Lorenz_System

10 < 1% match (Internet from 28-Jan-2022)

https://www.hindawi.com/journals/cin/2019/9524080/

11 < 1% match (Internet from 06-Sep-2022)

https://www.hindawi.com/journals/sp/2021/6610655/