DESIGN AND OPTIMIZATION OF NONLINEAR COMPONENT OF BLOCK CIPHER: APPLICATIONS TO MULTIMEDIA SECURITY

By

ADIL WAHEED

NATIONAL UNIVERSITY OF MODERN LANGUAGES
ISLAMABAD
July, 2024

Design and Optimization of Nonlinear Component of Block Cipher: Applications to Multimedia Security

By

ADIL WAHEED

MS(CS), National University of Modern Languages, Islamabad, 2024

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR

THE DEGREE OF

DOCTOR OF PHILOSOPHY

In **Computer Science**

To

FACULTY OF ENGINEERING & COMPUTING

NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD

THESIS AND DEFENSE APPROVAL FORM

The undersigned certify that they have read the following thesis, examined the defense, are satisfied with overall exam performance, and recommend the thesis to the Faculty of Engineering and Computing for acceptance.

Thesis Title: Design and Optimization of Nonlinear Component of Block Cipher: Applications to Multimedia Security

Submitted by: Adil Waheed **Registration** #: 5 PhD/CS/F20

Doctor of Philosophy in Computer Science
Degree Name in Full

Computer Science
Name of Discipline

Dr. Fazli Subhan
Research Supervisor

Signature of Research Supervisor

Research Co-Supervisor

Signature of Research Co-Supervisor

Dr. Sajjad Haider
Head of Department (CS)

Signature of HoD (CS)

Dr. M. Noman Malik
Name of Dean (FEC)

Signature of Dean (FEC)

July, 2024

AUTHOR'S DECLARATION

I Adill Waheed

Son of Abdul Waheed

Registration # 5 PhD/CS/F20

Discipline Computer Science

Candidate of **Doctor of Philosophy in Computer Science** at the National University of Modern Languages do hereby declare that the thesis **Design and Optimization of Nonlinear Component of Block Cipher: Applications to Multimedia Security** submitted by me in partial fulfillment of PhD (CS) degree, is my original work, and has not been submitted or published earlier. I also solemnly declare that it shall not, in future, be submitted by me for obtaining any other degree from this or any other university or institution. I also understand that if evidence of plagiarism is found in my thesis/dissertation at any stage, even after the award of a degree, the work may be cancelled and the degree revoked.

_____

Signature of Candidate

_____

Name of Candidate

_____

Date

ABSTRACT

Title: Design and Optimization of Nonlinear Component of Block Cipher: Applications to Multimedia Security

The accessibility and availability of digital content, including images, audio, video, websites, and digital archives, pose significant security challenges due to unrestricted access via the internet and other sources. This thesis addresses these challenges by enhancing cryptographic systems through advanced methods involving artificial neural networks, algebraic structures, coset graphs, chaotic substitution boxes (S-boxes), and image encryption schemes. Key contributions include the development of robust, compact, and bijective S-boxes using an algebraic framework in connection with the neural networks, which enhance security in multimedia applications by obscuring the relationship between the key and the ciphertext, thus ensuring Shannon's property of confusion. Additionally, an image encryption scheme utilizing 2D chaotic maps such as Zaslavsky, Baker, and Henon maps is presented, which ensures high security by employing both confusion and diffusion stages while preserving the maps' inherent mathematical structures characterized by their chaotic behaviour and fractal properties. Furthermore, an innovative image encryption algorithm based on field extension, coset graphs, and logistic chaotic maps is introduced to ensure robust authentication and integrity. This scheme involves extending real numbers to complex numbers, constructing coset graphs with complex numbers as vertices, and circularly shifting these vertices to create edges, thereby uniquely identifying each pixel within an image. To address the security challenges in key distribution and management associated with symmetric key ciphers, an asymmetric image encryption scheme utilizing elliptic curve cryptography (ECC) and a 4D fractional order chaotic map is proposed. This approach not only enhances the security of key management but also ensures that the encryption process is robust against various cyber threats. These advancements collectively aim to significantly improve the security of cryptographic systems, ensuring secure communication and robust protection against a wide range of cyber threats.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AD	-	Absolute Difference
BACI	-	Bitplane Correlation-Based Metric
BIC	-	Bit Independence Criterion
DAP	-	Differential Approximation Probability
ECC	-	Elliptic Curve Cryptography
GF	-	Galois Field
LFT	-	Linear Fractional Transformation
LP	-	Linear Probability
MD	-	Maximum Difference
MI	-	Mutual Information
MLP	-	Multilayer Perceptron
MSE	-	Mean Squared Error
NAE	-	Normalized Absolute Error
NK	-	Normalized Kendall's Tau
NL	-	Nonlinearity
NLC	-	Nonlinear component
NPCR	-	Normalized Pixel Change Rate
PSNR	-	Peak Signal-to-Noise Ratio
RMSE	-	Root Mean Squared Error
SAC	-	Strict Avalanche Criterion
S-box	-	Substitution box
SC	-	Structural Content
SSIM	-	Structural Similarity
UACI	-	Unified Average Changing Intensity

LIST OF SYMBOLS

v	-	Parameter in chaotic map.
μ	-	Variable in mathematical equations.
τ	-	Variable or parameter in mathematical equations.
ε	-	Parameter to represent the behavior of chaotic functions.

LIST OF APPENDICES

ACKNOWLEDGEMENT

In the name of Allah, the most Merciful, the most Compassionate all praise be to Allah, the Lord of the worlds; and prayers and peace be upon Muhammad His messenger. I acknowledge my unlimited gratitude to Allah, the Ever-Magnificent; the Ever-Thankful, for His help and blessing. My special praise for the Holy Prophet Hazrat Muhammad (Peace be upon him), hailed as the supreme instructor, the everlasting source of guidance and wisdom for humanity.

I express my heartfelt appreciation to my honorable supervisor **Dr. Fazli Subhan** for his invaluable guidance, mentorship and encouraging attitude throughout my research work. I am grateful to the respected mentor **Prof. Dr. Tariq Shah** for his valuable support and direction. I am thankful to the Coordinator **Dr. Zia Ur Rehman**, Department Head **Dr. Sajjad Haider** and Dean **Dr. Noman Malik**, for their support and coaching. Special thanks and lot of prayers to my dearest father **Haji Abdul Waheed (Late),** whose love has been my source of strength and inspiration. To my lovely wife **Kishwer Adil,** I am profoundly thankful for her patience and companionship throughout this journey. My sincere appreciation also goes to my sons **Ahmed Adil** and **Muhammad Azaan Adil,** their presence has been a constant reminder of the importance of family and the motivation to strive for excellence.

DEDICATION

This thesis work is dedicated to

My parents,

My beloved brothers and sisters,

My lovely wife,

My sons (Ahmed Adil, Muhammad Azaan Adil).

The great supervisor Dr. Fazli Subhan,

The National University of Modern Languages Islamabad, Pakistan.

CHAPTER 1

INTRODUCTION

1.1 Overview

This study provides a complete examination of multiple facets pertaining to the generation and application of S-boxes inside cryptographic systems. This thesis examines the existing complexities and efficiency challenges that are commonly observed in the fabrication of resilient S-boxes, as recorded in the contemporary cryptographic literature. The study also evaluates the need for secure image encryption using S-boxes, specifically emphasizing the importance of withstanding various statistical and different forms of attacks. This study investigates novel design techniques for the systematic integration of linear fractional transformation into S-boxes, aiming to improve their cryptographic properties. Researchers are currently working on the development of an adaptive algorithm that aims to dynamically modify the level of nonlinearity in S-boxes. This adaptation is intended to ensure that the S-boxes have the ability to meet the diverse cryptographic needs that may arise. This work aims to investigate the impact of various construction approaches based on chaotic maps on the creation of a prominent avalanche effect in S-box design, hence improving diffusion properties. Additionally, a sophisticated image encryption system has been developed, which effectively incorporates the intended S-boxes in order to bolster overall security and fortify resistance against cryptographic attacks.

This study also explores the utilization of coset graphs in the process of permutation shuffling in image encryption, with a particular focus on enhancing the attributes of variety and confusion. Furthermore, this study investigates the utilization of elliptic curve points and 4D fractional order chaotic maps in the context of image encryption. The objective is to improve the permutation shuffling procedure and boost the overall confusion characteristics. The objective of this continuing research is to provide a complete understanding of cryptographic

design paradigms. This research aims to support the development of robust and adaptable systems that are dedicated to assuring the security of data protection. The primary objective of this study is to enhance the comprehension and application of resilient cryptographic methods within the dynamic realm of information security by conducting a methodical examination of S-boxes and image encryption.

In today's world, global discussions revolve around information and its security. The foundation of information security lies in effective communication. This implies that the processes between the sender and receiver are accurately designed to transmit information through seamless, dependable, and precise channels. If the channel lacks reliability, the system must safeguard the information by employing cryptographic techniques before transmitting it over the unreliable channel. Modern cryptography is commonly categorized into two types: symmetric cryptography, which employs a single secret key, and asymmetric cryptography, which utilizes a key pair and is based on the explicit key principle. The Nonlinear component (NLC) [1] servers as a pivotal element in the symmetric key ciphers. Selection of a NLC is a critical stage in assessing the robustness of a cryptosystem against various attacks. Consequently, understanding the design and characteristics of a NLC for encryption purposes is crucial. Therefore, the security level of an encryption algorithm is significantly influenced by the NLC it utilizes. In references [2], [3], [4], [4], [5], the authors examine the characteristics of frequently employed NLCs. These examinations serve the purpose of assessing the encryption potency of a NLC through the application of diverse criteria and methodologies. Included in these are the differential approximation probability method (DP), nonlinearity method, strict avalanche criterion (SAC), bit independence criterion (BIC), and linear approximation probability method (LP). Improving the effectiveness of the nonlinearity method to enhance its capability for inducing confusion in particular applications continues to be a challenge for researchers.

Due to the rapid advancements in information technology, an increasing amount of multimedia data, such as digital images, audio, and video, is being generated and disseminated across diverse networks. Particularly, digital images stand out as one of the extensively utilized data formats. Given that a digital image has the capacity to convey significant information, the unauthorized access to a secret image could lead to significant information security challenges. Consequently, safeguarding the contents of digital images is of great interest. In recent times,

researchers have introduced numerous technologies, including data hiding [6], image encryption [7], [8], [9], and watermarking [10], to facilitate the secure communication of digital images. Among the various technologies ensuring image security, image encryption stands out as one of the most direct and efficient methods [11], [12], [13]. An image encryption algorithm converts a meaningful image into an unrecognizable cipher image. Only with the correct key, ciphered image can be converted into plain image. However, using an incorrect key, it is impossible to retrieve any useful information. Out of all the methods employed for image encryption, the chaos theory stands out as the most extensively utilized and efficient [14], [15], [16]. This is because the chaos theory shares numerous properties with the principles of image encryption [17]. Therefore, when a chaotic system is applied in a digital context, chaos degradation occurs due to precision limitations. This leads to security concerns in image encryption schemes that solely rely on chaotic systems [18]. A viable solution to address this problem involves integrating chaotic systems with other techniques. For instance, the authors presented a successful image scrambling algorithm that works a combination of the 3-cell chaotic map and biological operations [19].

To create NLCs with improved efficiency and performance, this thesis introduces a method for generating NLCs that involves linear fractional transformation, artificial intelligence, chaotic maps, coset graph, and elliptic curve cryptography. Furthermore, an algorithm for encrypting images is put forward, incorporating the NLCs, and security analyses validate its elevated level of security.

1.2 Motivation

This thesis draws inspiration from the rapid creation and extensive examination of nonlinear component and image encryption technologies [20], [21], [22] . There are several ways available in the literature for constructing nonlinear components [23], [24], [25]. However, it is important to note that certain construction methods may not be suited for certain applications due to their high computational complexity and vulnerability to channel noise [26]. Moreover, the literature presents many criteria to assess the robustness of a nonlinear component, but nonlinearity is the most important one that protects the nonlinear component from linear and differential attacks [27]. The size of the nonlinear component is significant

because it can change depending on its purpose. The most important and commonly used size includes an 8-bit nonlinear component, which allows for a larger number of possible combinations, making it more resistant to brute-force attacks [28]. In the majority of instances, image encryption schemes lack comprehensive evaluation in terms of their vulnerability to different attacks, making it challenging to determine the underlying characteristics of these algorithms [29]. One of the fundamental characteristics of a modern image encryption technique or any sophisticated encryption algorithm is its ability to withstand attacks, including cropping. This observation demonstrates that when a portion of information is removed from the cipher image, the decryption algorithm can still successfully decode the altered cipher image. Due to the limitations of single-image encryption schemes, processing multiple images is a difficult job [30]. Hence, in recent times, scholars in the field of multimedia security have shown increased interest in various ways of encrypting multiple images.

1.2.1 Architecture of Nonlinear Component

A nonlinear component (NLC) is a key part of symmetric key algorithms in cryptography that performs substitution (see Fig. 1). They are essential Boolean vectorial functions that are provided as look-up tables, acting as a corner stone in numerous symmetric-key algorithms to secure data security. A NLC accepts input bits and converts them to output bits and substitutes a set number of input bits with an equivalent number of output bits.

NLCs are frequently used in block ciphers to hide the connection between the key and the ciphertext. The design of NLC is based on the Shannon theory of confusion and diffusion, which is used to implement substitution-permutation networks (SPN) and substitutes a set number of input bits with an equivalent number of output bit. NLCs are integral components in symmetric ciphers like AES. NLCs contribute to both the confusion and diffusion aspects of encryption. The nonlinearity inherent in NLCs prevents linear relationships between plaintext and ciphertext, making it more challenging for attackers to exploit patterns. The design principles behind NLCs involve considerations such as bijectiveness, ensuring each input maps uniquely to an output, and resistance against algebraic and statistical attacks. Cryptographers often employ mathematical techniques, such as the properties of finite fields, to craft S-boxes that withstand advanced attacks. The choice of an S-box design greatly influences the

cryptographic strength of an algorithm, making it a subject of continual research and refinement. Some cryptographic algorithms employ multiple rounds of S-box substitutions to enhance security further. Researchers continually explore novel methodologies, including machine learning techniques, to optimize S-box designs and mitigate emerging threats.

Given the importance of NLC in block cipher systems, NLC with high cryptographic performance has been a goal of cryptosystem designers for a long time. There are numerous approaches [17]– [19] presented in literature for designing NLCs.

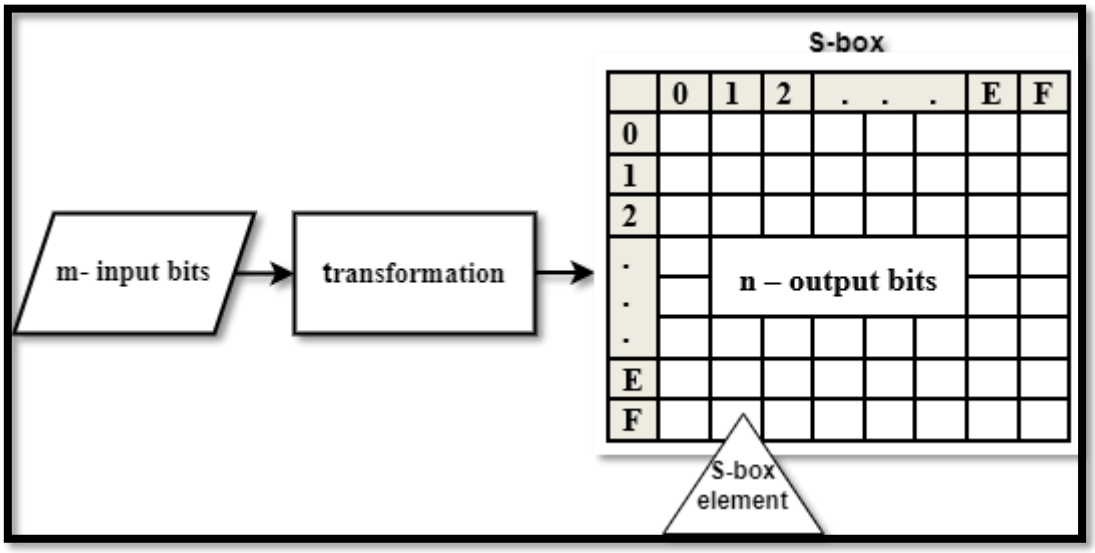


Figure 1.1: Block diagram of the S-box in a block cipher

1.2.2 Applications of Nonlinear Component

The identification of research gaps, formulation of the problem statement, establishment of the aim, determination of the scope, and definition of the objectives jointly provide the groundwork for prospective applications in diverse domains.

1. The research conducted in this study has resulted in the development of novel design approaches and adaptive algorithms. These advancements have the potential to be utilized in the improvement of cryptographic algorithms, hence increasing their resilience and ability to adapt to changing security demands.

2. The proposed image encryption technique, which incorporates custom-designed S-boxes, has potential for utilization in safeguarding confidential image data. This can be especially advantageous in sectors where the preservation of image secrecy is of utmost importance, such as the healthcare, defense, and finance industries.

3. The enhanced cryptographic characteristics of S-boxes, along with the comprehensive encryption scheme, can significantly enhance the security of data transmission.

4. The investigation of various construction approaches based on chaotic maps and the evaluation of proposed design methodology yield valuable information that may be utilized to enhance cybersecurity measures.

5. The results obtained from this study have the potential to exert an influence on the advancement and refinement of the Advanced Encryption Standard (AES).

6. The research findings have the potential to serve as a significant asset for academic institutions and academics involved in the field of cryptography.

7. In conclusion, the research findings have wide-ranging implications across various domains, including enhancements in image data security as well as potential impacts on the advancement of cryptographic algorithms and standards.

1.3 Cryptographic Properties of Nonlinear Component (S-box)

The study of desirable cryptographic properties of a robust nonlinear component is important, as nonlinear components play a critical role in cryptography.

1.3.1 Balanced

If there are an equal number of ones and zeros in the output set of a Boolean function S: $GF(2^n) \rightarrow GF(2)$, the function is said to be balanced. For example, in the truth table below for XOR and AND functions, 3rd column has equal number of ones and zeros which is balanced while 4th column does not have equal zeros and ones which is not balanced.

$$S_1 = XOR : GF(2^2) \rightarrow GF(2) \qquad (1.1)$$

$$S_2 = AND : GF(2^2) \rightarrow GF(2) \qquad (1.2)$$

Table 1.1. Balanced Boolean function

u	v	$u \oplus v$	$u.v$
0	0	0	0
1	0	1	0
0	1	1	0
1	1	0	1

1.3.2 Strict Avalanche Criterion

The evaluation of the efficiency of an S-box is determined by the Strict Avalanche Criterion (SAC), which is considered to be a significant characteristic. The SAC quantifies the degree of sensitivity exhibited by the output of the S-box when subjected to a single-bit alteration in the input. In the context of cryptographic systems, SAC specifies that in the event of a single bit being altered in the input, it is expected that each corresponding output bit will undergo a significant change with a probability that approximates 0.5. Put simply, the S-box should demonstrate a roughly uniform probability of altering each output bit, hence enhancing the diffusion aspect in the encryption procedure. Ensuring compliance with the SAC is of utmost importance in order to guarantee that the S-box provides a substantial level of complexity and confusion, hence augmenting the security of the cryptographic system as a whole. This is achieved by avoiding any localised modification in the input from triggering predictable or biassed changes in the output. The formula for computing the SAC is as follows:

$$SA_i(f) = \sum_{u \in GF(2^n)} f(u) \oplus f(u \oplus d_i) \qquad (1.3)$$

$$SA_i(f) = 2^{n-1} \qquad (1.4)$$

When the dynamic distance (DD) has a value that is a small integer near zero, it is an indication that the S-box satisfies the SAC.

1.3.3 Nonlinearity

Nonlinearity analysis is used to calculate the distance between a known Boolean function and every possible affine function. In other words, nonlinearity refers to the number of bits that must be altered to obtain the closest affine function [34]. An S-box employs a nonlinear mapping between ciphertext and plaintext to prevent attackers from easily understanding the transformation process. Unlike linear mapping, which involves straightforward mathematical operations between inputs and outputs, the nonlinearity of an S-box introduces complexity, making it more challenging for attackers to discern the relationship between plaintext and ciphertext. An optimal nonlinearity value for an S-box is 120, and S-boxes with higher nonlinearity are considered stronger. This is because cryptanalysis methods are less effective against these S-boxes. The following formula is used to determine the nonlinearity of an S-box:

$$NL_f = 2^{n-1} - \frac{1}{2}\max_{\alpha \in F_2^n} |W_{f(\alpha)}| \qquad (1.5)$$

1.3.4 Fixed and Opposite Fixed Point

A fixed point is one of the most basic concepts in the context of an S-box. It is referring to an input value that remains the same under a mathematical S-box operation [35]. In other words, input remains the same as output. Whereas, if an input value transforms into its complement after passing through the S-box transformation, refer to the opposite fixed point [36] [37]. Mathematically, both of these are represented as

Let S-box $S: GF(2^n) \rightarrow GF(2^m),\ u \in GF(2^n)$ (1.6)

1. If $S(u) = u$, a point is referred to as the fixed point of the S-box.
2. If $S(u) = u'$, a point is referred to as the opposite fixed point of the S-box.

Where $u'$is the opposite/complement of u.

1.3.5 Bit Independence Criterion

For creating robust S-boxes, the Bit Independence Criterion (BIC) is another desirable property. It measures the extent of bit-wise independence between plaintext and ciphertext. Additionally, it becomes harder to predict the design of a system as we increase the independence of bits from one another. It also demonstrates the need for all variables to be independent pairwise for a particular set of avalanche vectors generated by a single plaintext bit transpose [38]. The BIC criterion helps identify the role of the confusion function. In the event of any change in the input value of the BIC, the output bits must be changed independently. It is important to understand the correlation between the two for a true understanding of BIC. The change in the input bit affects the output bit independently. Mathematically, this effect is represented as:

$$BIC(a_j, a_k) = \underset{1\le i\le n}{max} |\, corr(a_j^{ei}, a_k^{ei})| \tag{1.7}$$

BIC for a particular S-box is defined as below:

$$BIC(f) = \underset{1\le j,k\le n}{max} \big|\, corr(a_j, a_k)\big|\; for\; j \neq k \tag{1.8}$$

The BIC criterion can have values between 0 and 1, and in the most unfavorable scenario, it can reach a minimum value of 0.

1.3.6 Linear approximation probability analysis (LAP)

Linear approximation probability analysis [39] is used to determine the degree of vulnerability of an encryption scheme to linear cryptanalysis. In other words, this analysis involves evaluating the correlation or imbalance between plaintext and ciphertext of the nonlinear component under linear transformation, and the maximum value of an imbalance is known as the linear approximation probability. By performing experiments, it has been noted that the well-known S-boxes exhibit an average LP value of 0.0625, which is effective in withstanding linear attacks. LP analysis of an S-box can be expressed mathematically in the following form:

$$LP = \underset{\tau x,\tau y\neq 0}{max} \left| \frac{\#\{x\in X | x.\tau x = S(x).\tau y\}}{|x|} - \frac{1}{2} \right| \tag{1.9}$$

1.3.7 Differential approximation probability (DAP) analysis

DAP analysis [39] is utilized to determine the degree of susceptibility of an encryption scheme to differential cryptanalysis. DAP technique is used by invaders to exploit differences in plaintext and ciphertext bit patterns and also makes it possible to identify weaknesses in encryption algorithms and guide design choices to mitigate the impact of differential attacks. Additionally, if each input differential maps to an output differential in a unique way, the S-box exhibits strong resistance to differential attack. Mathematically, DAP analysis for an S-box is calculated using the following formula:

$$DP(\Delta x \rightarrow \Delta y) = \left[\frac{\#\left\{x \in X / S(x) \oplus (x+\Delta x) = \Delta y\right\}}{2^m}\right] \qquad (1.10)$$

1.4. Problem Background

In previous years, several attempts have been made to enhance the static S-box structure of AES by incorporating dynamic characteristics. The authors in [40], introduced a novel approach for generating various S-boxes using key-dependent S-box method. The proposed method utilized constant and additive natured irreducible polynomials. The authors in [41] devised S-boxes through the implementation of several operations on the round key. In the first round of the AES algorithm, a static S-box was employed to construct several S-boxes that possess resistance against differential and linear cryptanalysis. However, the avalanche characteristics of these produced S-boxes were not at an optimal level. In the study of [42], the initial byte of the round key, which is generated by the key scheduling process in AES, was utilized to create a key-dependent substitution function. However, this function exhibited deficiencies in terms of execution time, dynamic characteristics, and the defiance against contemporary assaults. Harpreet and Paramvir [43] developed a key-dependent S-box and introduced a novel key scheduling technique. This approach involved many operations, such as XOR, left rotation, nibble swap, and SHA256, applied to a 128-bit key. The approach employed to establish a relationship of dependence between the key and the S-box was also of a static nature. The utilization of pseudo random numbers in [44] was employed for the purpose of generating dynamic S-box values. However, the presented methodology is ineffective in achieving desired outcomes such as dynamicity and strict avalanche features, when compared

to the proposed S-box scheme. The image encryption algorithm presented in [45] is dependent on the production of chaotic key streams through the utilization of a compound chaotic map. The research discussed the broader spectrum of chaos and improved chaotic features exhibited by the Logistic-Sine system (LSS). However, the efficacy of the encryption process is inherently linked to the robustness of the chaotic map. Nevertheless, in the event that the chaotic map lacks resilience or predictability, it may give rise to possible vulnerabilities. The methodology presented in the study [46], employed the Rössler attractor as a means of generating chaotic behavior in order to construct S-boxes. A potential limitation of the study pertains to the restricted investigation of chaotic maps. Relying only on a singular chaotic map may impose limitations on the range of chaotic phenomena that can be used to augment cryptographic attributes. The 5-bit S-box architecture presented by the authors [47] incorporates the principles of chaotic mapping theory in order to introduce stochastic behavior. The potential weaknesses of the proposed 5-bit S-box architecture may arise due to its reliance on chaotic mapping. The system's capacity to adapt to varied IoT contexts and its resilience to new threats are not well proved. The construction approach of the S-box [48] is based on the use of a two-dimensional exponential quadratic chaotic map (2D-EQCM) and a strong S-box algorithm that incorporates a key. Nevertheless, it is important to acknowledge certain limitations of the method, such as its inherent predictability and the potential introduction of determinism due to the utilization of seed S-boxes.

The researchers, in study [49], presented an innovative approach that is designed to find quotient spaces within an S-box that have the potential to be preserved, with the ultimate goal of detecting any possible backdoors. The vulnerability of S-box designs, such as Kuznyechick, to cryptanalytic attacks is evident when non-trivial subspaces are concealed. The method provided by the authors [35] entails the development of a constructing technique for a robust S-box, utilizing a non-degenerate 3D improved quadratic map (3D-IQM) as the basis. One notable limitation of the proposed methodology is the necessity for the author to carry out supplementary cryptographic examinations in order to comprehensively identify potential vulnerabilities. The image encryption system mentioned in the study [28] is derived from the Advanced Encryption Standard (AES) and incorporates a variable S-box. The plain image is partitioned into uniform-sized blocks (128 bits), with each block being subjected to encryption using a single AES algorithm. In order to conduct a thorough evaluation of the algorithm's robustness, it is crucial to obtain further information regarding the hyperchaotic system's

parameters, its vulnerability to attacks, and any potential constraints it may have in generating really random S-boxes.

The majority of current S-box techniques exhibit a static character and lack robust cryptographic qualities, rendering them ineffective in constructing dynamic S-boxes. Hence, it is imperative to develop a dynamic S-box solution that enhances nonlinearity, adheres to rigorous avalanche criteria, achieves optimal dynamicity, unpredictability, and other essential cryptographic qualities.

1.5 Problem Statement

The AES S-box is fixed in nature, making it vulnerable to certain attacks [50], [51], [52]. This is because the AES S-box is based on a fixed mathematical formula/irreducible polynomial $P(y) = x^8 + x^4 + x^3 + x + 1$ [53], [54] and may not be optimal for specific applications with unique security requirements. While the design prioritizes security, some alternative S-Boxes might offer lower hardware implementation costs, making them more suitable for resource-constrained environments. Furthermore, current S-boxes may not offer the strongest cryptographic qualities, as the nonlinearity of current S-boxes is lower than or equal to that of the older Rijndael AES S-box [55]. This necessitates the development of robust, key-dependent, and dynamic S-boxes using more advanced methods while maintaining a simple construction process [56], [57]. Likewise, S-boxes are very effective in image encryption algorithms [58], [59], [60], but existing literature typically utilizes them in a simple substitution manner. There is a critical need for a secure S-box-based image encryption scheme capable of withstanding statistical and other forms of attacks.

Consequences: If these issues are not addressed, the security of encrypted data, particularly images, will remain vulnerable to various forms of attacks, including statistical and differential attacks. The fixed nature of the current AES S-box and its reliance on a static polynomial make it susceptible to cryptanalysis, potentially compromising sensitive information. Without developing more robust, dynamic, and key-dependent S-boxes, cryptographic systems will continue to face challenges in maintaining high levels of security. This could result in significant data breaches, loss of privacy, and the potential exploitation of

vulnerable encryption systems in critical applications such as secure communications and digital media protection.

1.6 Research Questions

1. How can NLC design methodologies be developed to systematically incorporate linear fractional transformations and multilayer perceptron, and devise an algorithm that enhances the degree of nonlinearity?

2. What contributions do chaotic map-based construction methods make to designing a robust NLC, while also integrating the designed NLC into an innovative image encryption scheme for overall security improvement?

3. How exactly do coset graphs impact the permutation shuffling procedure in the context of image encryption, and how might the incorporation of these graphs enhance the security properties of variability and confusion?

4. How can the integration of elliptic curve points and 4D fractional order chaotic map create a secure and unpredictable permutation shuffling process for image encryption, improving confusion?

1.7 Research Objectives

1. To obtain cryptographically strong S-boxes with high resistance to significantly enhance the security of cryptographic algorithms. In this thesis, algebraic and neural S-boxes are obtained by using the action of the projective general linear group $PGL(2, GF(2^8))$, on a Galois field, $GF(2^8)$ and artificial neural network (multilayer layer perceptron).

2. To achieve high nonlinearity makes it harder for attackers to find patterns and predict the output based on the input. This thesis introduces a novel nonlinearity booster algorithm that can also enhance the nonlinearity of both proposed and existing

algorithms.

3. The objective of the proposed thesis is to develop cryptographic systems that use chaos and random numbers to provide robust encryption approaches for generating ciphered images with exceptional characteristics.

4. This research proposes a novel image encryption algorithm with robust key management that leverages elliptic curve cryptography and coset graphs to create a secure and highly unpredictable permutation-based shuffling procedure.

1.8 Summary of the Proposed Methodologies

The first objective is achieved by proposing a hybrid methodology, which consists of linear fractional transformation (LFT) and multilayer perceptron (MLP). LFT creates a preceding NLC, and MLP produces an initial near to optimal NLC. Additionally, to enhance the nonlinearity of the NLC, a swapping-based algorithm known as nonlinearity booster algorithm (NLB) is proposed. The following is the LFT methodology employed in order to create preceding NLC:

$$f: PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8) \qquad (1.11)$$

$$f(x) = {(ax + b)}\Big/{(cx + d)} \qquad (1.12)$$

Where $a, b, c, and\ d$ are elements of $GF(2^8)$, with specific values assigned: $a = 71, b = 64, c = 16, and\ d = 29$. The justification for choosing these values for the LFT is based on two factors: Firstly, these values yield elements spanning from 0 to 255, leveraging Galois Field $GF(2^8)$ elements generated via the specified polynomial. The chosen irreducible polynomial, $x^8 + x^7 + x^5 + x^3 + 1$, is instrumental in designing the NLC of the block cipher. Secondly, the selected variables adhere to the condition where $ad - bc \neq 0$. Moreover, in order to improve the preceding NLC, we designed an artificial neural network (multilayer perceptron) with input, hidden, and output layers. This machine learning model (multilayer perceptron) is trained by feeding inputs into input layer. In order to train a machine learning model, data is fed into its input layer. These inputs are processed by the input layer before being sent on to the hidden layers, where the model learns to extract features and patterns from the data. Through

repeated iterations, the model's capacity to map inputs to outputs is fine-tuned by adjusting the weights and biases of the connections between neurons in the hidden layers. Finally, an improved NLC is produced by adjusting training parameters, the initial condition, and the activation function. Additionally, a novel nonlinearity booster algorithm (NLB) is presented to boost the nonlinearity of existing and presented NLCs. The NLB algorithm operates based on a swapping mechanism. In this algorithm, the initial step involves selecting one element, exchanging it with another element, and subsequently assessing the nonlinearity (NL) of the resulting NLC. If the NL is greater than or equal to the NL of the previous NLC, the swapping is confirmed; otherwise, the swapping is ignored. This process is repeated for all elements, ensuring that the maximum NL is achieved. Once the swapping of individual elements is completed, the algorithm proceeds to work with pairs of elements. The pairs are swapped with two other elements of the NLC. Following the completion of the swapping of pairs, the group size is increased to 4 and subsequently to 8. It is crucial to maintain that the group size is a power of 2^n $where\, n = \{0,1,2,3,..,n\}$, and swapping occurs only if the NL is greater or equal; otherwise, the swapping is disregarded.

The second objective finds fulfillment through the innovative application of three carefully selected chaotic maps: the Zaslavsky, Baker's, and Hénon maps for the design of NLCs. Crucially, this integration occurs without compromising the integrity of their underlying mathematical structures. The approach strategically unfolds across two distinct stages: confusion and diffusion, collectively engineered to establish a formidable defense against various attacks. Within the confusion stage, chaotic values are accurately linked to sneakily obscure the arrangement of both rows and columns within the image, effectively severing correlations between neighboring pixels. This precisely crafted process seamlessly transitions into the diffusion step, which connects the unique properties of the 2D Baker's and Hénon maps to evoke a potent avalanche effect. To showcase the application of the proposed NLCs, we subsequently design an image encryption algorithm employing the proposed NLCs for nonlinear transformation of the image. The proposed image encryption technique starts with an initial evaluation to determine the color mode of the image, distinguishing between grayscale and RGB. Subsequently, image is divided into various blocks of sizes 16×16, ensuring the dimensions of the image are by 16. In the event that this criterion is not met, image is expanded by appending more pixels to the boundary until both the width and height are divisible by 16.

The third objective is accomplished by employing coset graph in conjunction with the field extension to formulate a new image encryption scheme. In this scheme, an algebraic structure is defined, that is, an extension of the real numbers ($\mathbb{R}$) to complex numbers ($\mathbb{C}$). The generated extension field is subsequently used in the construction of a coset graph based on the chosen field. A coset graph is constructed using complex numbers as vertices. The vertices are shifted circularly to get the desired number of edges. The vertices of the coset graph map to pixels of the image and assign a unique identification to each pixel within the graph.

The fourth objective is achieved by introducing a novel image encryption algorithm that utilizes elliptic curve points and 4D fractional order chaotic maps. The process involves taking advantage of the inherent unpredictability and sensitivity to initial conditions displayed by chaotic maps in four dimensions. Elliptic curve is utilized to discover all elliptic curve points that will serve as the initial values for image encryption with dimensions of rows and columns. The pixel values of the original image are mapped to the elliptic curve points, and a crossover encrypted the mapped points with the use of a public key using ECC encryption. Furthermore, choose the parameters and initial conditions for the 4D fractional order chaotic map to generate the four dimensions, transform them into one matrix equivalent to the size of the image, and then XOR the encrypted points with the chaotic map values to perturb the encrypted points. The combination of chaotic dynamics and elliptic curve cryptography not only introduces a new level of complexity to the proposed scheme but also utilizes the distinct characteristics offered by both techniques.

1.9 Aim of Research

The primary objective of this study is to enhance our comprehension of S-box design by investigating the incorporation of innovative ideas such as coset graphs, 4D chaotic maps, and elliptic curve points, and their potential applications in the field of picture encryption.

1.10 Scope of the Research Work

The scope of this study is to systematically investigate and advance the methodology for designing S-boxes, with a particular emphasis on the use of S-box elements in decimal format. Furthermore, the study expands upon the application of the Portable Network Graphics (PNG) format as a means of processing images, so enabling the inclusion of novel image encryption methods into simulations. The study encompasses the incorporation of linear fractional transformations, dynamic nonlinearity correction, and the use of constructing methods based on chaotic maps in order to enhance cryptographic features. The scope of this study also considers the smooth integration of designed S-boxes into image encryption. It places emphasis on practical issues by ensuring that S-box components are processed in decimal format, and that images are converted to PNG format for the sake of simulation. The objective of this study is to offer a thorough understanding of enhancing S-box design approaches and their practical implementations in image encryption settings.

1.11 Contribution of Thesis

The main contributions of this thesis are summarized as follows:

1. We introduce a method for generating NLCs efficiently, employing a combination of a linear fractional transformation and a multilayer perceptron neuron.

   Our published article related to this contribution: *A. Waheed, F. Subhan, M. Mohd Su'ud, and M. Mansoor Alam, "Molding robust S-box design based on linear fractional transformation and multilayer Perceptron: Applications to multimedia security," Egypt. Informatics J., vol. 26, no. 3, p. 100480, 2024, doi: 10.1016/j.eij.2024.100480.*

2. We conducted a comprehensive literature review, thoroughly examining the proposed research methodologies, including strengths and weaknesses, cryptographic fundamental, research gap and direction, and research challenges.

   Our published article related to this contribution: *A. Waheed, F. Subhan, M. M. Suud, M. Alam, and S. Ahmad, "An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges," Multimed. Tools Appl., vol. 82, no. 19, pp. 29689–29712, 2023, doi: 10.1007/s11042-023-14910-3..*

3. We propose three robust nonlinear components and image encryption scheme connects the topological features of 2-D maps, specifically their chaotic behavior and fractal properties; without altering their underlying mathematical structures. To achieve this, proposed methodology employs the Zaslavsky, Baker, and Hénon maps in a multi-stage process that strategically blends confusion and diffusion for enhanced security against a wide range of attacks. In the initial confusion stage, chaotic values accurately disrupt the arrangement of both rows and columns within the image, effectively reducing correlations between adjacent pixels. This is followed by a precisely designed diffusion step, which controls the 2-D Baker and Hénon maps to induce a potent avalanche effect, ensuring that any minute alterations to the original image propagate extensively throughout the encrypted output.

   Our published article related to this contribution: *A. Waheed, F. Subhan, M. M. Suud, M. Mansoor Alam, and S. Haider, "Design and optimization of nonlinear component of block cipher: Applications to multimedia security," Ain Shams Eng. J., vol. 15, no. 3, p. 102507, 2023, doi: 10.1016/j.asej.2023.102507.*

4. The constructed NLC's performance is evaluated and experimentally compared to numerous NLCs generated by alternative methods in terms of NL, SAC, BIC, DP and LP. The findings demonstrate the superior performance and efficiency of the proposed NLC.

   Our published article related to this contribution: *A. Waheed and F. Subhan, "S-box design based on logistic skewed chaotic map and modified Rabin-Karp algorithm: applications to multimedia security," Phys. Scr., vol. 99, no. 5, p. 055236, 2024, doi: 10.1088/1402-4896/ad3991.*

5. To showcase the application of the proposed nonlinear components, we subsequently design an image encryption algorithm employing the proposed NLCs for nonlinear transformation of the image.

6. Introduce customized image encryption algorithm that can efficiently generate ciphered images using the combination of 4-D fractional order chaotic map, coset graph, and elliptic curve cryptography.

   Our published article realted to this contribution: *A. Waheed, F. Subhan, M. M. Suud,*

Y. H. Malik, and E. Al., "Construction of nonlinear component of block cipher using coset graph," AIMS Math., vol. 8, no. 9, pp. 21644–21667, 2023, doi: 10.3934/math.20231104.

7. Simulation outcomes and security analyses indicate that the proposed image encryption scheme possesses a high level of security, capable of withstanding various security attacks. Comparative results reveal that the scheme outperforms several state-of-the-art image encryption algorithms in terms of both performance and security.

1.12 Thesis Organization

This dissertation is structured into the following seven chapters:

1. Chapter 1 gives an introduction to the proposed work, fundamental concepts, research motivation and objectives, mathematical background for the construction of nonlinear components, and properties of the Boolean function for cryptography. In the end, the cryptographic properties of a nonlinear component are presented.

2. Chapter 2 provides a thorough examination of the current research methodologies, covering important parts that go into the historical development of principles pertaining to S-box design and image encryption. The study conducts a systematic analysis of cryptographic characteristics, providing a comprehensive understanding of their influence on the security and efficiency of a system. Additionally, a thorough study has analyzed and revealed the strengths and weaknesses of the presented approaches, including research background, research gap and directions.

3. Chapter 3 introduces the nonlinear component design based on algebraic structure (linear fractional transoformation) and artificial neural networks. The process of designing nonlinear components relies on utilizing linear fractional transformation over a Galois field and multilayer perceptron. Additionally, a nonlinearity booster algorithm is also presented to boost the nonlinearity of proposed and existing nonlinear components.

4. Chapter 4 proposes novel nonlinear components (S-boxes) and image encryption scheme that connects the topological features of 2-D maps, specifically their chaotic behavior and fractal properties; without altering their underlying mathematical structures. To achieve this, proposed methodology employs the Zaslavsky, Baker, and Hénon maps in a multi-stage process that strategically blends confusion and diffusion for enhanced security against a wide range of attacks. In the initial confusion stage, chaotic values accurately disrupt the arrangement of both rows and columns within the image, effectively reducing correlations between adjacent pixels. This is followed by a precisely designed diffusion step, which controls the 2-D Baker and Hénon maps to induce a potent avalanche effect, ensuring that any minute alterations to the original image propagate extensively throughout the encrypted output. The results of our experiments provide evidence that the suggested approach demonstrates good security and improved effectiveness compared to existing algorithms.

5. In Chapter 5, we introduce a novel image encryption algorithm based on field extension, coset graph, and a known logistic chaotic map. In this algorithm, first we define the algebraic structure, that is, the extension of the real numbers to complex numbers. Subsequently, the extension field is utilized in the construction of the coset graph based on the chosen field. A coset graph is constructed using complex numbers as vertices. The vertices are shifted circularly to get the desired number of edges. The vertices of the coset graph map to pixels of the image and assign a unique identification to each pixel within the graph. Then, in order to generate a secure key sequence, a logistic chaotic map is utilized based on the properties of the coset graph.

6. The symmetric key ciphers face potential security challenges due to key distribution, and a novel asymmetric key image encryption scheme is presented in Chapter 6, which is based on elliptic curve cryptography (ECC) and a 4D fractional order chaotic map. ECC involves generating points on an elliptic curve, which is defined by a specific equation. In order to encrypt the points, the pixel values of the original image are mapped to the elliptic curve points, and encryption is performed on the mapped points using a public key. Additionally, in order to perturb the encrypted points, four dimensions of a 4D fractional order chaotic map are generated, transformed, and XORed with the encrypted points.

7. Chapter 7 concludes this thesis by presenting the contributions and recommendations for further research.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

This chapter provides a thorough examination of the current research environment, covering important parts that go into the historical development of principles pertaining to S-box design and image encryption. The study conducts a systematic analysis of cryptographic characteristics, providing a comprehensive understanding of their influence on the security and efficiency of a system. This study delves into the fundamental principles of Boolean functions and cryptography, emphasizing the thorough exploration of important definitions and the deep link between these two domains. The identification of a research gap involves an examination of areas that require more exploration.

2.2 Related Study

Within the field of cryptography, a substitution box (S-box), also known as a nonlinear component (NLC), holds significant importance as a fundamental element in symmetric key algorithms, including DES and AES [61]. Cryptographic techniques, such as hashing, are used to ensure the integrity of data exchanged between the buyer and the seller. By creating distinct hash values for the data, any modifications or tampering that occur during transmission may be identified, thus guaranteeing the integrity of the shared information [62]. The nonlinear lookup table is designed to accept a predetermined number of input bits and provide a corresponding output of a defined number of bits. The utilization of the NLC in the encryption procedure introduces elements of confusion and diffusion, hence enhancing the security of the encrypted data against potential attacks [63][64]. The NLC is intentionally constructed to possess specific

characteristics, including bijectivity, resistance against linear and differential cryptanalysis, and a substantial degree of nonlinearity. The design and implementation of an S-box play crucial roles in ensuring the security of a cryptographic system. The nonlinearity of the NLC is a critical factor in determining its security, and achieving the appropriate nonlinearity can be accomplished through the use of Boolean functions. The process of designing NLCs utilizing Boolean functions entails the careful selection of appropriate Boolean functions, establishing the correspondence between input and output values, and conducting assessments to ensure the S-box's nonlinearity and other security attributes [65]. The utilization of chaotic functions was employed by the authors [66] to construct a pseudo-random Boolean function. Randomness and unpredictability are frequently attributed to their utilization. The integration of chaotic functions and Boolean functions enables the generation of a pseudo-random Boolean function that exhibits a high degree of unpredictability and resistance to reverse engineering. This characteristic enhances the security level of the cryptographic system [67], [68]. The objective of the authors in reference [69] was to create an S-box with a high degree of nonlinearity by utilizing Boolean functions. Previous research investigations, including those referenced as [70] and [71], have utilized a chaotic map in order to enhance the encryption of images by incorporating it into the S-box. In study [72], authors employed a combination of the Gingerbreadman chaotic map and the S8 permutation technique to effectively encrypt images. In study [73], the authors presented empirical evidence in support of the efficacy of utilizing the chaotic dynamics exhibited by the sine map as a means of creating encryption keys with a high degree of unpredictability. This characteristic contributes to the provision of robust security measures. In study [74], a novel image cryptosystem is formulated and presented. The authors employed the numerical solution of the Lorenz differential equations and a linear descent technique in the second encryption step of the proposed algorithm to construct a resilient and potent S-box. The RGB image encryption system presented in reference [75] integrates the principles of confusion and diffusion as originally introduced by Shannon. The process comprises three distinct stages, with the second stage employing a precisely designed S-box to attain the intended levels of nonlinearity and complexity. Symmetric cyphers are commonly classified into two distinct kinds, namely block cyphers and stream cyphers. The utilization of Boolean functions is a fundamental element in the design of both forms of ciphers.

In recent times, there has been a significant emphasis on chaos theory, which has gathered the interest of numerous S-box designers in their efforts to incorporate this nonlinear

element into modern block ciphers [76], [77]. The construction of resilient S-boxes was achieved by researchers in [78] by the utilisation of a novel approach centred around the Logistic chaotic map. This method involved the incorporation of matrix rotation and affine transformation to produce S-boxes that are dependent on the encryption key. The presented approach for constructing an S-box consists of four steps: calculating the inverse in the Galois Field, generating keys using the Logistic map, computing the rotational matrix, and lastly establishing a new S-box. In study, Alghafis et al. [79] introduced a method for constructing an S-box using a three-dimensional Liu chaotic system. The resulting S-box is employed in conjunction with other chaotic systems for the purpose of picture encryption, and the resulting outcomes demonstrate the strength and effectiveness of the substitution process. In study, Lu et al. [45] introduced a novel compound chaotic map by combining two existing chaotic maps, namely the Sine map and the Logistic map. This compound map was subsequently utilized for the development of a NLC. Tanyildizi et al. [80] developed a technique for generating a NLC utilizing a one-dimensional chaotic map. Liu and colleagues [36] developed an enhanced coupling quadratic map, referred to as the Improved Coupling Quadratic Map (ICQM). Zahid et al. [52] proposed a novel permutation method and a creative polynomial algorithm for the development of resilient NLCs. The permutation-based strategy employed in this study is characterized by its remarkable simplicity and effectiveness. In their study, Riaz et al. [81] proposed the utilization of a compound chaotic map derived from the Tent map and Chebyshev map. This compound chaotic map was employed to produce an efficient NLC, which was subsequently utilized for image encryption purposes.

2.3 Cryptographic Fundamentals

The scientific examination of any kind of regulation necessitates the establishment of precise definitions derived from fundamental ideas. The principles and definitions below include fundamental ideas employed throughout the foundations of cryptography [5] [83][84][85].

Definition 1.1 (Computer Security): The term is often used to refer to the collection of technologies specifically developed to safeguard data and counteract unauthorized access by hackers.

Definition 1.2 (Network Security): Precautions taken to ensure the safety of data during transmission.

Definition 1.3 (Internet Security): Security protocols designed to keep information safe while it travels via a web of interconnected networks

Definition 1.4 (Security Attack): Any activity that undermines the integrity and confidentiality of data possessed by an entity

Definition 1.5 (Security Mechanism): A defense mechanism can help you spot threats, stop them, or get back up and running after an attack.

Definition 1.6 (Security Service): This service aims to boost the security measures used in an organization's data processing systems and information exchanges. The services are designed with the purpose of mitigating security attacks, employing one or several security measures to deliver the desired service.

Definition 1.7 (Cryptography): The discipline that involves the ideas and techniques of converting an intelligible communication into an unintelligible one and afterwards restoring that message to its original form.

Definition 1.8 (plaintext): The term "plaintext" refers to the original message that an individual or party intends to transmit covertly to another individual or party.

Definition 1.9 (ciphertext): When plain text is subjected to an encryption procedure, it results in the production of ciphertext. The encrypted text appears to be a disorganized sequence of information.

Definition 1.10 (Key): A key is a designated word, number, or phrase utilized in the encryption of plaintext. It serves as the controlling factor for both the encryption and decryption processes, dictating the transformation of data between its original and secure forms.

Definition 1.11 (cipher): An algorithm designed to convert an intelligible message into an unintelligible one using techniques such as transposition and/or replacement.

Definition 1.12 (Decryption): The mechanism involves the inverse operation of encryption. The process of decryption involves utilizing both the ciphertext and the secret key in order to generate the original plaintext.

Definition 1.13 (cryptanalysis): A procedure that examines the ideas and methodologies involved in the process of decrypting an unintelligible message and restoring it to an intelligible form, all without possessing any knowledge of the corresponding key. This practice is commonly referred to as code-breaking.

Definition 1.14 (cryptology): It is the combination of cryptography and cryptanalysis. Both cryptography and cryptanalysis are essential components of the field of information security. Cryptography involves the development and implementation of techniques and algorithms to secure data and communications, ensuring confidentiality, integrity, and authenticity.

Definition 1.15 (Block Cipher): A block cipher operates by processing a block of elements at a time from the input, resulting in an output block for each input block.

Definition 1.16 (Stream Cipher): A stream cipher operates by continually processing input components and generating output elements in a sequential manner.

Definition 1.17 (Cipher text only attack): The term "cipher text only" refers to a scenario in which a cryptanalyst possesses just a copy of the cipher text.

Definition 1.18 (Known Plaintext Attack): The cryptanalyst holds a version of the encoded text, while the corresponding plaintext content is denoted as known plaintext.

Definition 1.19 (Chosen Plaintext Attack): The cryptanalysts acquire momentary entry to the encryption process. Although they cannot directly access the key through decryption,

they engage in processing numerous selected plaintexts in an attempt to deduce the key using the resulting ciphertext.

Definition 1.20 (Chosen cipher text attack): The cryptanalyst gains temporary authorization to utilize the decryption machine, employing it to decipher many sequences of symbols. Subsequently, the cryptanalyst tries to deduce the key by analyzing the decrypted texts and attempting to determine the corresponding cipher texts.

Definition 1.21 (Confidentiality): The primary objective is to guarantee that the data stored within a computer system, as well as any information being communicated, may only be accessed for the purpose of reading by those who have been granted authorization.

Definition 1.22 (Authentication): The primary objective is to accurately determine the source of a message or electronic document while also providing a guarantee that the presented identity is authentic and not fraudulent.

Definition 1.23 (Integrity): The primary objective of this measure is to guarantee that only authorized entities possess the capability to alter sent data.

Definition 1.24 (Non-repudiation): It is imperative that both the sender and the recipient of a message lack the ability to deny the act of transmission.

Definition 1.25 (Access control): The regulation of access to information resources can be either imposed by external authorities or implemented internally inside the system in question.

Definition 1.26 (Availability): It is imperative that computer system assets are accessible to authorized entities as and when required.

Definition 1.27 (Interruption): A system's assets become unusable, destroyed, or unavailable. This is an attack on accessibility, such as the deliberate destruction of a hardware

component, the physical cutting of a communication line, or the intentional disabling of a file management system.

Definition 1.28 (Interception): An illegal entity successfully attains entry to a valuable resource. This action is perceived as a violation of confidentiality. An unauthorized party may refer to an individual, a software application, or a computing device. For instance, the act of eavesdropping to intercept data within a network, as well as the unauthorized duplication of information,

Definition 1.29 (Modification): An unauthorized entity not only acquires entry to but also manipulates an asset. This action constitutes an attack on integrity. For instance, the act of editing values in a data file, making changes to software, or adjusting the contents of messages being broadcast inside a network.

Definition 1.30 (Fabrication): The system is vulnerable due to the addition of forged items by an unauthorized person. This attack was inferred as a challenge to the concept of authenticity.

Definition 1.31 (in symmetric key algorithms): Both the sender and recipient have knowledge of the encryption and decryption keys. The encryption key is mutually distributed, whereas the decryption key may be readily derived from it.

Definition 1.32 (in public key cryptography): The encryption key is disclosed to the public, yet it remains computationally impractical to ascertain the decryption key without possessing the specific information exclusively known to the intended recipient.

Definition 1.33 (Linear and differential cryptanalysis) [86]: Linear cryptanalysis is a technique that uses the linear approximation of a cipher to retrieve the secret key. It is designed to locate linear approximation between the input and output of the cryptographic algorithm. Whereas, the behavior of a cipher can be exploited by differential analysis when small changes are made to the plaintext. It involves examining the variations between pairs of plaintexts and their equivalent ciphertexts.

Definition 1.34 (Nonlinearity) [48]: The property of nonlinearity is the fact that the cipher's operations or components do not have a linear relationship between input and output. The high degree of nonlinearity means that small changes in input can result in significant changes in output, making it more challenging for an attacker to analyze the cipher through techniques like linear cryptanalysis.

Definition 1.35 (Visual Cryptography) [87]: Visual cryptography is a cryptographic method that entails encrypting an image or visual data into separate shares or fragments. These shares can be visually combined or overlaid to conduct decryption.

Definition 1.36 (Dynamic Sbox Vs Static Sbox) [88]: A static S-box, sometimes referred to as a pre-computed S-box, is an essential element utilized in block ciphers to perform encryption. Whereas, the dynamic S-box also perform substitution, but the substitution table is not fixed. However, the changing nature of the dynamic S-box enhances the difficulty for attackers to scrutinize the encryption method and capitalize on possible vulnerabilities.

Definition 1.37 (Confusion): Confusion refers to the complex arrangement that exists between the key and cipher text within a cryptographic system.

Definition 1.38 (Diffusion): This process entails distributing the impact of a single bit present in the plaintext message onto numerous bits present in the encrypted message (ciphertext). Dynamic S-box also perform substitution during encryption, but substation table itself is not fixed.

2.3.1 Significance of Nonlinear Component

Nonlinear components (NLCs) are essential for strengthening the security of block ciphers in multiple ways:

1. NLCs introduce complexity in the relationship between plaintext, ciphertext, and encryption key. In simple terms, the nonlinear component is the sole element of confusion that hinders attackers from deducing the key, hence ensuring the Shannon

property of confusion.

2. NLCs are essential components in block ciphers as they introduce nonlinearity, which is necessary because linear operations can be easily reversed.

3. NLCs play a crucial role in maintaining the confidentiality, reliability, and authenticity of digital images when it comes to image encryption. By incorporating NLCs into image encryption techniques, it is possible to securely transmit and retain sensitive image data, effectively protecting it against illegal access and alteration.

4. NLCs diffuse the impact of a single plaintext bit across numerous ciphertext bits. They achieve this by transforming the input bits into an independent set of output bits, hence ensuring the Shannon property of diffusion.

5. NLCs provide the opportunity to customize encryption algorithms according to particular security needs. Cryptographers have the ability to modify encryption schemes by changing the design of S-boxes or employing various S-boxes within the same algorithm. This allows them to effectively handle emerging security risks and meet performance limitations.

2.4 Connection Between Boolean Function and Nonlinear Component

Nonlinear components and Boolean functions must be understood in order to fully comprehend this thesis. It helps in recognizing the significance of this study and the connection between Boolean function and nonlinear component. In this section, fundamental concepts, mathematical formulas, and theorems are provided regarding connection between both of them. In order to comprehend the construction and performance of nonlinear components, it is necessary to first introduce some fundamental concepts of Boolean function. The following are the properties of Boolean function in connection with cryptography:

Let $GF(2^k)$ be a k-dimensional vector space over the binary Galois field $GF(2)$. $GF(2^k)$ comprises of 2^k vectors represented as binary sequences of length k. The vector space $GF(2^k)$ has a scalar product denoted by <. , .>: $GF(2^k)$ x $GF(2^k) \rightarrow GF(2)$.

$$< x, y >= \oplus_{m=1}^{n}(x_m . x_n) \qquad (2.1)$$

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

Definition 1.35 [89] The expression $\hat{\gamma}_h(b)$ represents the autocorrelation function for a shift of b within $GF(2^k)$ which is given as follows:

$$\hat{\gamma}_h(b) = \sum_{z \in GF(2^p)} \hat{h}(z).\hat{h}\,(z \oplus b)` \qquad (2.2)$$

Definition 1.36 [90] The algebraic degree is defined as the count of variables in the highest order monomial without coefficients.

Definition 1.37 [91] A Boolean function "h" with n variables is considered to have a correlation immunity of order m (where $1 \leq m \leq n$) if the values of the function are independent from the statistical analysis of any subset of the input variables.

Definition 1.38 [89] The nonlinearity in a Boolean function is represented by N_h and is defined as follows:

$$N_h = d(h, A_n) = \min_{\beta \in A_n} d(h, \beta) \qquad (2.3)$$

In an affine function, there is no nonlinearity. However, nonlinearity for a non-affine Boolean function “h” is $N_h > 0$. The high level of nonlinearity in a robust cryptosystem provides protection against linear cryptanalysis, as discussed in [92].

Definition 1.39 [93] A Boolean function's algebraic degree and algebraic complexity are directly correlated. Additionally, the higher the degree of a function, the more complex it becomes algebraically.

Definition 1.40 [89] A Boolean function with k variables has the following autocorrelation function:

$$r_h(b) = \sum_{i=0}^{2^k-1} h(z_i) \oplus h(z_i + b) \qquad (2.4)$$

all values of b belong to $GF(2^k)$.

Definition 1.41 [94] When a single input bit is complemented and an output bit changes with a probability of 0.5, the function $h: GF(2^k) \rightarrow GF(2^l)$ holds the strict avalanche criterion.

$$\forall\, x = 1,2,\dots\dots,m\ ,\ y = 1,2,\dots\dots,n, \quad Prob\big(h(z^x)\big)_y \neq Prob\big(h(z)\big)_y.\frac{1}{2} \quad (2.5)$$

The cryptographic transformation is finished when every bit of the ciphertext depends on every bit of the input. Two-way complete cryptographic transformations are those that have complete inverses; if the inverse is incomplete, the transformation is considered as one-way complete.

Definition 1.42 [94] If a single input bit changes the behavior of half of the output bits on average, refers to strict avalanche criterion. In order to observe the avalanche effect, a function h: $GF(2^n) \rightarrow GF(2^n)$is used i.e.

$$\frac{1}{2^n}\sum_{v\in 2^n} wt\left(g\left(z^i\right) - g(z)\right) = \frac{q}{2},\ \ \forall\, i = \{1,2,\dots,p\} \quad (2.6)$$

Definition 1.43 [94] The mapping Ω: $\mathrm{GF}(2^n) \rightarrow \mathbb{R}$ is the Walsh transform of a function "h" on $GF(2^n)$ represented as

$$\Omega(\mathrm{h})(\mathrm{v}) = \sum_{z\in 2^n} h(z)(-1)^{<v,z>} \quad (2.7)$$

Where $< v, z >$ represents the standard scalar product. The Walsh spectrum of h is a collection of 2^n coefficients determined by an equation (1.6).

Definition 1.42 [93] The algebraic normal form (ANF) of the n-variable Boolean function is as follows:

$$h(t) = a_0 \oplus a_0 t_0 \oplus a_0 t_0 t_1 \oplus a_{012\dots n-1} t_0 t_{1\dots.} t_{n-1} \quad (2.8)$$

Where the truth table values for the ANF of h(z) are generated by the coefficients $a \in GF(2^n)$.

Definition 1.43 [93] The total number of variables in the highest product term of the function's ANF that has a non-zero coefficient is the algebraic degree of a Boolean function, expressed as $h(z)$. This is represented as $\deg(h)$.

Definition 1.44 [90] The term "non-degenerate function" (ANF) refers to a function that contains all n variables of a Boolean function h(z). On the other hand, if h(z) does not hold every variable in its ANF, then it is known as degenerate function.

Definition 1.45 [89] The correlation between two Boolean function j and h is defined as following:

$$\text{Correlation} = 1 - \left[\frac{2d(j,h)}{2^{k-1}}\right] \qquad (2.9)$$

Definition 1.46 [93] In the Boolean function h, the imbalance of function is equal to the difference between the number of inputs that map to 0 and the number of inputs that map to 1 divided by 2. The imbalance is between 2^k and 2^{-k}. A Boolean function is said to be balanced if the imbalance parameter is set to zero.

Definition 1.47 (Bent Function): Boolean functions with distinctive characteristics were first introduced by Rothaus [95]. The term "perfect nonlinear" refers to bent functions because of their ideal separation from linear structures. The presence of these structures is found to be contingent on the even-dimensional Boolean function space. The nonlinearity of bent function is defined as $(2^k - 2^{k/2})$. Contrarily, Boolean functions are unable to satisfy the necessary conditions for a bent function in odd-dimensional space, Bent functions don't exhibit any order of correlation immunity. Despite having perfect (minimal) autocorrelation and maximal nonlinearity, bent functions still have a Hamming weight of $(2^{k-1} \pm 2^{k/2-1})$, which is cryptographically optimal. Additionally, n variables bent functions with algebraic degree are not ideal for cryptographic purposes, and thus, not directly applicable in real time applications.

Definition 1.48 [96] A Galois field (GF), also known as a finite field, is a mathematical concept that deals with a finite set of elements. A GF provides a finite set of elements along with well-defined operations of addition and multiplication. If a and b are two elements belonging to $GF(q)$, then a is equivalent to b in $GF(q)$ if and only if a is congruent to b modulo q.

Definition 1.49 A polynomial over $GF(q^n)$ refers to a polynomial that has coefficients which belong to $GF(q)$. It is possible to express all the elements of a finite field as polynomials with degree less than n as given below.

$$a_1 + a_2x + a_3x^2 + \cdots + a_nx^{n-1} \qquad (2.10)$$

Definition 1.50 [97] If a polynomial cannot be broken down into nontrivial polynomials over the same field, then it is considered to be irreducible over $GF(q^n)$. For example, $x^2 + x + 1\ and\ x^3 + x + 1$ are irreducible polynomials over $GF(2)$. Furthermore, Advanced encryption standard (AES), which was developed using a fixed irreducible polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$, uses a finite field $GF(2^8)$ with 256 elements. As a result, each element of $GF(2^8)$ is a polynomial with a degree below 8. These elements can also be represented equivalently by positive integers between 0 and 255 inclusive or by 2-digit hexadecimal numbers or 8-bit binary numbers. Both the polynomial and binary forms of elements in $GF(2^8)$ are presented below:

Table 2.1: The finite field $GF(2^8)$ elements for polynomial $m(x) = x^8 + x^4 + x^3 + x + 1$

Polynomial	**Decimal**	**Hexadecimal**	**Binary**
0	0	00	00000000
1	1	01	00000001
x	2	02	00000010
$x + 1$	3	03	00000011
x^2	4	04	00000100
$x^2 + 1$	5	05	00000101
$x^2 + x$	6	06	00000110
$x^2 + x + 1$	7	07	00000111
.	.	.	.
.	.	.	.
.	.	.	.
$x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	255	FF	11111111

Definition 1.51 [98] If a polynomial $f(x)$ in $GF(q)$ cannot be expressed as the product of lower-degree polynomials in $GF(q)[x]$, then it is considered irreducible.

Definition 1.52 [99] The irreducibility of the polynomial $f(x) = x^p - x + a \in \mathbb{F}_q[x]$, where $q = p^n$ and n ≥ 1 and 'a' is a constant, is equivalent to the absence of its roots in $\mathbb{F}_q$. In other words, $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if it has no zeros in $\mathbb{F}_q$.

2.5 Research Gap and Directions

This section presents a thorough examination of diverse approaches utilized in the design of S-boxes, which serve as essential components of cryptographic algorithms. The critical study involves an investigation of the fundamental techniques employed in various S-box designs, assessing their merits and limitations. Significantly, this study investigates many methodologies including substitution-permutation networks, algebraic structures, and chaotic systems, in order to get insight into their individual strengths and limits.

Table 2.2 Overview of Innovative Approaches

Ref.	Key Features	Strengths	Weaknesses
[100][101]	The Mobius transformation is a configuration involving inversions, rotations, translations, and magnifications. During the execution of a Mobius transformation, symmetry is consistently maintained without any loss. This transformation can be defined as a mathematical operation where, $$f(z) = \frac{az + b}{cz + d}$$ In the given equation, both az+b and cz+d are linear expressions, and the coefficients a, b, c, and d are elements of the Galois Field $GF(2^8)$.	The primary advantage of Mobius transformation lies in its ability to effectively represent linear time-varying systems that depend logically on parameters. The Mobius transformation is a useful tool for representing complicated dynamic systems that have different parameters. It achieves this by decomposing the systems into a linear core and a separate parameter component.	The vulnerability of the Mobius transformation arises from its dependence on an irreducible polynomial of degree 8. Therefore, it is imperative to exercise caution while selecting the degree 8 irreducible polynomial for the purpose of creating the Galois Field $GF(2^8)$. The careful choice of a polynomial is of utmost importance, since it has the potential to greatly influence calculations and potentially disrupt the confusion-generating capabilities of the resulting S-box.
[102]	The mathematical representation of the dynamic linear trigonometric transformation for generating an n×m S-box is provided below: $T(z) = Cos((A + B) * X * z + C)$ Where, $0 \leq z \leq (2^n - 1), n = 8, 0 < X < 1, A, C \in \{1,3, \dots, 2^n - 1\}, B \in z, B = Array\ of\ size\ 256.$	The inherent dynamism of this technique affords an S-box designer a much expanded key space in comparison to that of a variable of float type. Moreover, it produces a significant quantity of key-dependent dynamic S-boxes.	One of the variables, X, is hindered by a deficiency in computing efficiency resulting from the data type selection. The variable is allocated a data type of double, enabling a greater level of precision with the capability to represent up to 15 significant decimal digits. However, the advantage of precision in double precision numbers is accompanied by a trade-off in processing speed, as operations using these

	This implies that the transformation involves a mathematical expression capturing the dynamic and linear trigonometric characteristics utilized in the generation of an S-box with dimensions n×m.		numbers tend to be slower in comparison to those employing float types.
[103]	A Latin square can be defined as a matrix of size n×n, where n represents the number of distinct symbols present in the array. Each symbol is placed in a manner so that it appears only once in each row and column of the matrix. This technology involves the utilization of an improved logistic map to produce chaotic sequences by leveraging the provided initial state. The Latin square is subsequently constructed with a subset of these chaotic sequences. Two orthogonal matrices are constructed using the complete Latin square. In conclusion, an S-box can be generated by introducing perturbations to orthogonal matrices using supplementary chaotic sequences. This methodology delineates a procedure wherein the disorderly dynamics stemming from the logistic map are harnessed to generate Latin squares, which, in turn, serve as a foundation for producing orthogonal matrices used in the development of S-boxes.	The efficacy of this S-box creation procedure is in its ability to avoid intricate matrix row, column, or transformation procedures. The lack of these complex procedures leads to a reduced temporal complexity, hence improving the overall efficiency of the generation process. The efficiency of the technique is enhanced by its simplicity, resulting in quicker computations. This characteristic is particularly helpful in situations when the rapid generation of S-boxes is of utmost importance.	This approach is subject to a limitation that arises when attempting to attain a more homogeneous distribution of components inside a matrix through the random reordering of their places. The introduction of randomness in this context serves to improve uniformity, but it also poses a challenge throughout the decryption process due to the inability to accurately determine the original placements of the pieces. The absence of a deterministic correlation between the initial and encrypted places may hinder the decryption procedure.
[68]	The generation of the components of the S-boxes in this approach involves the coupling of the logistic chaotic map with Bent functions. The method effectively utilizes the	The efficacy of this methodology resides in its utilization of a balancing procedure that proficiently eliminates redundant outputs. During this procedure, all elements that yield the same output are substituted with the	The problem in this particular instance pertains to the employment of the threshold quantization method for the purpose of picking the value quantization method of the chaotic sequence. The resultant

	characteristics of chaotic processes. In the field of cryptography, the logistic mapping approach is commonly employed to construct Bent functions that exhibit high nonlinear values. This study focuses on the use of chaos theory and Bent functions in the construction of S-box components, with a particular emphasis on leveraging chaotic dynamics to improve the cryptographic characteristics of the resulting S-boxes. The integration of chaotic maps and Bent functions is a fundamental element of this generation strategy.	numerical value of 256. This phase guarantees the bijective characteristic of an S-box, wherein every distinct input is mapped to a distinct output, and vice versa. Through the implementation of a systematic replacement approach and the resolution of duplicate outputs, this technique effectively strengthens the injective properties of the S-box. As a result, the cryptographic strength and reliability of the S-box are significantly improved, making it suitable for a wide range of applications.	quantized binary sequence, meanwhile, exhibits a consistent pattern and lacks variability. The absence of variety or dynamism in the quantized binary sequence can be considered a vulnerability due to the fact that cryptographic applications typically benefit from dynamic fluctuations seen in chaotic sequences.
[104]	Cuckoos adopt unique behavior during the period of egg deposition. The majority of cuckoos exhibit a reproductive strategy known as brood parasitism, when they lay their eggs in the nests of conspecifics. This behavior is believed to enhance the likelihood of successful hatching, and in rare cases, cuckoos may even remove the eggs of the host bird to optimize their own breeding success. This technique utilizes a combination of a chaotic map and the cuckoo search algorithm to produce S-boxes that possess strong cryptographic properties. The integration of Cuckoo search optimization into the pre-existing S-boxes yielded a highly efficient S-box, aimed at achieving maximum nonlinearity.	The main objective of integrating the chaotic map is to enhance the search process, guaranteeing that it begins from favorable places and reduces the likelihood of becoming stuck in local optima. The utilization of the chaotic map introduces a degree of stochasticity and indeterminacy, hence facilitating the systematic examination of a solution space in order to identify optimal places throughout the search process. This methodology is especially advantageous in the context of optimization problems, as it increases the likelihood of discovering global optima instead of accepting suboptimal solutions that are frequently associated with local optima.	One notable drawback is the significant time investment necessary for the computation of fitness functions. This suggests that the technique may require significant computational resources, which could potentially affect its efficiency in situations when rapid computations are essential. One of the identified limitations pertains to the comparatively lower rate of convergence. A low convergence rate implies that the method may exhibit a prolonged duration in reaching an optimal solution or converging towards a desirable state.
[105]	The method describes a methodology for	The efficacy of the method is derived from its design, which	The limitation of this design methodology is rooted in the

	constructing an S-box with the objective of achieving high nonlinearity. The approach involves multiplying multiple separate affine transformations with multiple distinct overlapping vectors of 8 bits. This technique introduces complexity and nonlinearity to the S-box by combining the effects of multiple affine transformations applied to overlapping bit vectors. The use of multiple distinct vectors and the multiplication operation contribute to a higher degree of nonlinearity in the resulting S-box.	incorporates supplementary constraints on the nonlinear layer inside a sub-byte step. The deliberate introduction of conditions aims to optimize the avalanche effect and boost the comprehensiveness of the planned S-box. The phenomenon known as the avalanche effect pertains to the advantageous characteristic whereby a minor alteration in the input yields a substantially distinct outcome, hence augmenting the level of security and responsiveness to variations.	requirement for a greater number of constant vectors in order to enhance the intricacy of the S-box. The primary objective of incorporating computational complexity is to bolster security measures. However, it is important to acknowledge that the heightened necessity for constant vectors can be perceived as a disadvantage.
[106]	The approach is characterized as a lightweight encryption method based exclusively on the Advanced Encryption Standard (AES), specifically tailored for Internet of Things (IoT) devices. In order to demonstrate the efficacy of the proposed methodology, the system is employed for the encryption of a grayscale image utilizing an XM1000 sensor. The practicality and applicability of the approach in encrypting images and enabling safe transmission across networked smart devices is evidenced by its successful deployment in IoT contexts.	The algorithm's efficacy is derived from its iterative methodology, which systematically assesses and enhances the creation of the S-box. In particular, the process involves the preservation of S-boxes if a high nonlinearity value is obtained. The prioritization of capturing large nonlinearity values is aimed at guaranteeing that the produced S-boxes exhibit robust cryptographic characteristics, hence rendering the technique a potentially effective means for producing secure S-boxes in cryptographic contexts.	The limitation of this S-box generation method is its narrow focus, as it is specifically tailored to mitigate the vulnerabilities found in Internet of Things (IoT) devices. A potential limitation arises from the proposal to expand the algorithm's reach to incorporate a broader perspective, rather than restricting its usage exclusively to IoT devices.
[107]	In contrast to traditional methodologies that utilize a Galois field, this approach proposes a novel structure for the nonlinear component. The structure is obtained from the elements	The primary advantage of this method lies in its reliance on Boolean functions over the maximal cyclic subgroup that includes zero, along with the extension 0→0. The selection of this fundamental option results in	The mapping of the S-box, which states that it is one-to-one from $G_n \cup \{0\}\ to\ GF(2^8)$, yet is not bijective, reveals the flaw in this designing approach.. A bijective mapping guarantees a one-to-one

	of the largest cyclic subgroup within the multiplicative group of invertible elements in a finite Galois ring. The decision to deviate from employing a Galois field represents a fresh and potentially groundbreaking strategy for constructing S-boxes.	a scheme that exhibits a high level of efficiency and is capable of readily fulfilling the majority logic requirement. This design approach ensures efficiency, logical consistency, and suitability for watermarking, hence showcasing its adaptability and effectiveness across several cryptographic scenarios.	connection between members in the two sets, a property that is crucial for cryptographic applications. The identified flaw implies a possible deficiency or insufficiency in the mapping.
[108]	The construction approach is referred to as "Symmetric group composition." This implies that the construction incorporates elements or concepts derived from symmetric groups, which are mathematical entities linked to permutations.	The process of creating an S-box is designed to guarantee a balanced distribution of its elements, hence enhancing its overall cryptographic strength.	Using a high number of irreducible polynomials can improve complexity and variety, but because it requires more computing power, it may also bring a vulnerability. The symmetric composition process may become more difficult if a big set is used, since this might result in increased computing expenses in terms of time and resources.
[109]	The design of the S-box involves the integration of the tangent delay technique with an elliptic cavity chaotic sequence and a particular permutation derived from the symmetric group of permutations. The utilization of chaotic dynamics and permutations in a methodical manner is proposed as a means to alter the cryptographic features of the S-box, potentially resulting in improved security and nonlinearity. The design methodology revolves around a criterion for selecting clones.	The efficacy of this strategy resides in its assertion that the S-box, which is constructed using this approach, effectively mitigates linear and differential attacks. Linear and differential attacks are prevalent cryptographic flaws. The statement implies that the technique utilized in the construction of the S-box serves as a protective measure against these particular forms of attacks.	The algorithm indicates that the nonlinearity attained using the approach given is not up to the AES S-box's standards. A key cryptographic feature is nonlinearity, and in this instance, the flaw is that it doesn't fulfil the standard imposed by the well-known AES S-box. This suggests that the S-box produced by this method could not provide the required amount of nonlinearity, which could affect how resistant it is to some cryptographic assaults.
[110]	The design of the S-box involves the integration of the tangent delay technique with an elliptic cavity chaotic sequence and a particular permutation derived from the symmetric group of permutations. The utilization of chaotic dynamics and permutations in a methodical manner is	The efficacy of this approach resides in the computational efficiency of the algorithm or methodology employed for the generation of S-boxes. This suggests that the S-boxes generated have a low level of differential homogeneity within a feasible search duration. The concept of differential uniformity pertains to the cryptographic	The problem discovered in this methodology pertains to the strategy of developing a substantial collection of S-boxes, rather than prioritizing the creation of one that optimally aligns with the Advanced Encryption Standard (AES). Although the generation of a substantial dataset may provide a wide

	proposed as a means to alter the cryptographic features of the S-box,	domain and serves as a metric for evaluating the level of resilience exhibited by an S-box when subjected to differential attacks. The proposed methodology indicates that the algorithm effectively identifies or generates S-boxes that possess desirable properties in terms of differential uniformity.	range of options, it might be perceived as a drawback due to its deviation from the primary objective of identifying an effective S-box that is especially designed for the Advanced Encryption Standard (AES).
[111]	The construction technique entails the composition of S-boxes, which is initiated from a singular reference point. This suggests that a composite structure is formed by systematically combining several S-boxes, beginning from a designated initial configuration or reference S-box. The methodology presumably encompasses a sequential procedure for integrating and constructing these S-boxes, offering a logical framework for constructing a sophisticated cryptographic component.	Chaotic maps are utilized in order to generate a sequence of initial S-boxes. The S-boxes that are produced demonstrate a low level of complexity, rendering them challenging to analyze. Additionally, they possess a bigger key space, hence augmenting their resilience against prospective assaults.	The method's recognized shortcoming is found in its restriction to key-dependent S-boxes. Although it demonstrates proficiency in managing one particular kind, its adaptability and efficacy are limited when confronted with different variations of S-boxes.
[48]	The design methodology employed in this study is founded upon the utilization of a two-dimensional hyper chaotic map in conjunction with algebraic procedures. Hyper chaotic maps are mathematical systems that demonstrate intricate and unpredictable dynamics. In the present context, a two-dimensional hyperchaotic map is utilized. The incorporation of chaos theory and algebraic operations into the design process has the potential to yield cryptographic primitives that possess desirable attributes, like confusion and dissemination	The efficacy of this approach is in its capacity to produce S-boxes characterized by a high degree of nonlinearity. The attribute of nonlinearity holds significant importance in the field of cryptography as it measures the extent to which alterations in the input of the S-box affect its output. The desirability of high nonlinearity lies in its ability to strengthen the resistance of the S-box against a range of cryptographic assaults, including linear and differential cryptanalysis. The proposed methodology indicates that it is capable of generating S-boxes that exhibit a robust nonlinear correlation between input and output, hence enhancing the overall security and cryptographic potency of the constructed primitives.	The observed vulnerability pertains to the method's exclusive focus on building keyed S-boxes, rather than constructing generic ones. The imposed constraint has the potential to hinder the flexibility and practicality of the created S-boxes, as they are designed only for use in conjunction with cryptographic keys. The identified vulnerability indicates a possible constraint in the method's range of applicability, underscoring the need of including generic S-box construction for a broader range of cryptographic applications.

[112]	The research utilizes two specific dimensions, namely the Lorenz and Henon maps, as a foundation for the development of resilient S-boxes. The Lorenz and Henon maps are mathematical models that demonstrate chaotic dynamics. The incorporation of dynamic qualities extracted from the Lorenz and Henon maps is likely to be involved in the utilization of these two dimensions for the creation of the S-box. The utilization of various dimensions implies an all-encompassing methodology, which may result in the advancement of cryptographic primitives with enhanced security.	The efficacy of this approach resides in its specificity, as the S-box is purposefully created for the encryption of images. The prioritization of favorable statistical qualities indicates that the constructed S-box is proficient in facilitating a well-balanced and secure conversion of pixel values within an image. Moreover, the reference to a substantial key space signifies that the S-box plays a significant role in enhancing the cryptographic robustness of the picture encryption system.	A problem observed in this approach is its exclusive reliance on a single sort of chaotic map for constructing S-boxes, without including other chaotic maps for the sake of comparison. The absence of a comparison study against S-boxes generated from various chaotic maps hinders the comprehensive evaluation of the method's resilience. The use of diverse chaotic maps for comparative analysis can yield valuable insights into the relative merits and limitations of the approach, hence facilitating a more thorough assessment of its efficacy in the production of S-boxes.

The algorithms for design and optimization of S-box discussed in the Table 2.2 showcase a variety of approaches, each with its strengths and weaknesses. Mobius transformation utilizes translation, rotations, inversions, and magnifications to maintain symmetry. However, it is essential to accurately choose the degree 8 irreducible polynomial in order to prevent any computational complications. Linear Trigonometric Transformation constructs $m \times n$ dynamic S-boxes with large key space but suffers from slower computation due to the use of double data types. The complete Latin Square method generates chaotic sequences to create Latin squares and orthogonal matrices with low time complexity, but decryption becomes more complicated by randomly scrambling element positons.

The combination of Bent Functions and Logistic Chaotic Systems remove the duplicate output to ensure the bijective properties and high nonlinearity, but lacks dynamism in the quantized binary sequence. While the Discrete Chaotic Maps and Cuckoo Search Algorithm (DC-CSA) effectively avoids local optima during S-box generation, its performance is

hampered by slow fitness function calculations and low convergence rates. Affine Transformation improves avalanche and completeness properties by employing multiple transformations and overlapping vectors. However, this complexity comes at the cost of requiring additional constant vectors.

Lightweight 8-bit S-box design utilizes circuit design to minimize delay and area using 2- input NAND gates. However, its applicability is limited to field inversion within F_{24}, , and it lacks adaptability for broader use. Special S-boxes designed for IoT devices, the Lightweight S-box approach leverages chaotic Boolean functions and the Hilbert curve to achieve high nonlinearity. However, its application is limited to addressing vulnerabilities specific to IoT devices. In summary, these methodologies showcase the diverse approaches to S-box construction, highlighting the inherent trade-offs between complexity, efficiency, and security in cryptographic systems.

2.5.1 Research Directions

Based on the above-mentioned research background, cryptographic properties, and rigorous literature review, several potential directions for future research emerge:

1. Future study might potentially prioritize the enhancement of S-boxes that are constructed using algebraic structure by utilizing the possibilities offered by neural network approaches.

2. There exists a necessity to create algorithms that are especially tailored to boost the cryptographic properties (NL, SAC, BIC, LAP, DAP) of S-boxes as documented in existing research. Further investigation in this area may investigate into innovative computational methodologies and optimization tactics to methodically modify and enhance cryptographic properties.
3. Potential avenues for future study might encompass investigating the use of several chaotic maps (2D, 3D, 4D), as opposed to a singular chaotic map, in the development of S-boxes.

4. The focus of research can be focused on the development of image encryption systems utilizing Galois field, ring structures, group theory, lattice-based structures, Boolean algebra, and elliptic curve cryptography, as well as the investigation of alternative algebraic structures.

5. Hybrid methods that draw on cryptography, machine learning, and algebraic structures are potentially promising avenues for further study.

6. There must be a comprehensive cryptographic testing tool capable of testing all types of S-box and encrypted image properties. Therefore, this advancement will assist scientists in conducting more thorough examinations.

2.6 Research Challenges in S-box construction

The S-box, functioning as the heart of the cryptosystem, aims to create confusion between the key and ciphertext. This section of the thesis contains challenges facing S-boxes:

1. The AES nonlinear component in use today is static [113], making the development of dynamic nonlinear components to replace it a difficult task. The fixed mapping of AES makes it easy job for an intruder to decipher the ciphertex back into its original plaintext. As a result, there will always be a need to design and construct S-boxes with a higher number of input bits that can withstand a variety of linear and differential attacks.

2. The literature discusses a wide range of strategies for designing stable S-boxes, including linear and trigonometric approaches, heuristic evolution, spatiotemporal chaotic dynamics, and chaotic map-based approaches [114](see Table 2.2). However, the most difficult part is thinking about crucial qualities that are considered essential for the analysis and strength of S-boxes. This difficulty occurs because some algebraic features contribute very little to the development of a strong S-box [115], while others play a far more substantial role. Fibonacci sequences and prime numbers are also used to increase the safety of S-boxes, as explained in [116]. In order to construct S-boxes

that are secure against attacks, researchers need constantly investigate these nonlinear transformations.

3. Because present tools lack adequate capabilities to analyses cryptographic aspects fully, designing and selecting tools for analyzing the cryptographic properties of S-boxes is another important challenge. Therefore, we think that cryptographers will benefit from the creation of new tools for cryptographic property analysis if they are able to investigate the behavior of S-boxes more thoroughly.

4. Numerous approaches for constructing S-boxes, including several that rely on randomness, have undergone extensive examination. Because of the many approaches taken throughout creation, random S-boxes are quite secure and resistant to significant cryptanalysis attacks. The absence of fixed locations in the reconstruction technique and the high computing complexity of randomization are, however, drawbacks [117], [118]. Adopting complicated mathematical structures that are more resistant to algebraic attacks is superior than depending exclusively on random creation.

5. In certain cases, S-boxes may be constructed using manual processes or by employing basic mathematical operations. However, it is important to note that this construction approach is mostly applicable to smaller S-boxes. Nevertheless, when it comes to the constructing of extensive S-boxes, this methodology may exhibit lossiness and lack compactness. So, the construction setup must be improved by implementing innovative and complex mathematical models.

2.7 Summary

The chapter presents a comprehensive analysis of the existing research landscape, specifically emphasizing the areas of S-box design and image encryption. A thought examination has been conducted in order to identify specific areas that require more exploration. Additionally, a thorough study has analyzed and revealed the strengths and weaknesses of the presented approaches, including research background, research gap and directions.

CHAPTER 3

NONLINEAR COMPONENT DESIGN BASED ON ARTIFICIAL NEURAL NETWORK AND ALGEBRAIC STRUCTURE

3.1 Overview

This chapter of the thesis introduces a comprehensive approach for designing robust, compact, and bijective S-boxes to enhance the security of multimedia applications and improve information security methods. The process of designing an S-box relies on utilizing an artificial neural network architecture, that is, a multilayer perceptron and linear fractional transformation over a Galois field. The proposed algorithm yields an S-box with a very high strength to muddle the data, despite being very straightforward. With the help of various analyses (nonlinearity, strict avalanche, bit independence, linear approximation probability, and differential approximation probability), the strength of an S-box and its capacity to cause confusion are critically evaluated. We also use a comprehensive evaluation strategy, along with other relevant cryptographic tests, to measure how well our proposed S-box works in image encryption applications. Additionally, this newly constructed optimized S-box is equated with widely recognized S-boxes such as AES [82], Dimitrov [119], Zhu [120], Zahid [121], Javeed [122], Gray [123], APA [124], Skipjack [125], Residue Prime [5], and Xyi [126]. The comparative study yields promising results regarding the quality of the proposed S-box.

3.2 Background

In the field of symmetric key cryptography, the strength of the S-box heavily influences the working of the block ciphers. The S-box is solely responsible for creating confusion and

concealing it within the encrypted data. The ability of the S-box to distort the data determines how strong the encryption will be; as a result, the process of finding new and potent S-boxes is of great interest in the field of cryptography. In the literature, Shannon begins the construction of the S-box in the Shannon theory [127],and Fiestal continued the process during the Fiestal cipher [128]. Currently, Abd-El-Atty et al. [129] have proposed a novel S-box construction scheme that is based on quantum-inspired quantum walks and the Hénon map. In order to construct an optimized S-box, Zamli et al. [130] proposed a novel S-box design based on the naked mole rat (NMR) algorithm. In contrast to the majority of challenging works, which typically combine one chaotic map with a specific metaheuristic algorithm, NMR uses multiple chaotic maps as part of the presented algorithm. Si et al. [48] created a 2D chaotic map to address the issues with some 1D chaotic maps, such as poor randomness and a lack of ergodicity, and they examined the dynamic behavior of the chaotic map using a phase diagram, Lyapunov exponent, Kolmogorov entropy, correlation dimension, and randomness testing. The outcomes showed that the 2D chaotic map can function as a PRNG because of its ergodicity and improved randomness. In [60], a new system model with improved chaotic properties was obtained using a polynomial-based chaotic map. The presented system performs dynamically more effectively than some existing 1D chaotic systems. For the purpose of creating the nonlinear component of block cipher, Sani et al. [131] present a piecewise nonlinear chaotic map. An approach for encrypting color and medical images of various sizes is presented in [132]. With this encryption method, chaotic maps and genetic operators are combined. Abughazalah et al. [133] proposed an innovative nonlinear component of block cipher by using recurrent neural networks. Sun et al. [134] introduced a complex two-dimensional chaotic map as a pseudorandom number generator and also proposed an image compression algorithm by combining a multilayer perceptron and a median edge detector. In this study [135], a cryptographic key generation algorithm is proposed by using the chaotic sequence and time series forecasting models. A permutation box and key-based data substitution are combined to design the AES substitution-permutation network. When multiple keys are applied in each round of AES, a number of layers of substitution-permutation combinations lead to the generation of ciphertext. Chao-based S-box [119] has higher encryption security and algebraic complexity. AES [82] and Gray S-boxes [136] have higher nonlinearity and robustness against cryptographic attacks.

The Gray S-box and AES S-box are both influenced by binary Gray codes and the symmetric group. Additionally, Xyi S-boxes [126], Skipjack S-boxes [137], and Prime S-boxes [5] are utilized in generic encryption techniques and are best suited for data hiding methods. Finite field theory and its extensions serve as the foundation for S-boxes, as is clear from the APA S-box, AES S-box, S8 S-box, Residue Prime S-box, Skipjack S-box, Gray S-box, and Xyi S-box. Galois field was used to build S-box in the literature [31], [138], [139], [140], [141]. Modular arithmetic, or exponentiation modulo polynomials in extended Galois fields, is the foundation of this approach [142]. In this chapter, we propose an algorithm to construct an S-box using a fractional linear transformation applied to the Galois field, which results in a very high nonlinearity measure, as inspiration for some recently presented designs. A number of well-known tests are used to look more closely at the novel S-box's properties. These include tests for nonlinearity, strict avalanche criterion, bit independent criterion, linear approximation probability tests, and both linear and differential approximation probability tests. Experiential results prove its effectiveness and security against different attacks. In this study, researchers proposed S-boxes based on a chaotic map and jellyfish optimization algorithm [143]. Zhou et al. [144] presented very robust chaotic S-boxes based on a two-dimensional hyperchaotic map. The authors in this paper [145] utilize three-way intelligent decision-making to propose S-boxes for secure communication. Likewise, the researchers in [66] investigated secure and improved S-boxes based on quantum crossover and chaotic functions. In the analysis of nonlinear components, the majority logic criterion (MLC) is a fundamental method to assess whether a nonlinear component resists various cryptographic attacks [4]. The MLC includes several analyses to evaluate the behavior of the nonlinear component. Here are key analyses associated with the MLC: balancedness, nonlinearity, strict avalanche criterion, bit independence criterion, linear approximation probability, differential probability, and correlation immunity. The following is a list of irreducible polynomials for construction of an S-box.

Table 3.1: List of Irreducible Polynomial

Sr. No	Irreducible Polynomial
1	$x^8 + x^7 + x^5 + x^3 + 1$
2	$x^7 + x^6 + x^5 + x^4 + x^2 + 1$
3	$x^8 + x^7 + x^6 + x^5 + x^2 + \mathrm{x} + 1$
4	$x^8 + x^7 + x^6 + x^4 + x^2 + \mathrm{x} + 1$
5	$x^8 + x^7 + x^6 + \mathrm{x} + 1$
6	$x^8 + x^7 + x^5 + x^4 + 1$
7	$x^8 + x^7 + x^5 + \mathrm{x} + 1$
8	$x^8 + x^7 + x^3 + x^2 + 1$

9	$x^8 + x^7 + x^2 + \mathrm{x} + 1$
10	$x^8 + x^6 + x^5 + x^4 + x^2 + \mathrm{x} + 1$
11	$x^8 + x^6 + x^5 + x^3 + 1$
12	$x^8 + x^6 + x^5 + \mathrm{x} + 1$
13	$x^8 + x^6 + x^3 + x^2 + 1$
14	$x^8 + x^5 + x^4 + x^3 + 1$
15	$x^8 + x^5 + x^3 + x^2 + 1$
16	$x^8 + x^5 + x^4 + x^3 + x^2 + \mathrm{x} + 1$
17	$x^8 + x^4 + x^3 + x^2 + 1$

Perceptron is a fundamental concept in artificial neural networks [146]. It is a straightforward and powerful unit that takes inspiration from biological neurons and functions as a binary classifier in supervised learning problems. They are specifically developed to handle input-based binary classification problems. The inputs are multiplied by their respective weights and then summed. This sum is then sent through an activation function, which is typically a threshold function. The output of this function is a binary value, either 0 or 1. The red circle depicted in Figure 3.1 [147] symbolizes the magnitude of influence that each input has on the neuron. The perceptron updates its weights by making adjustments according on the inaccuracies in its predictions.

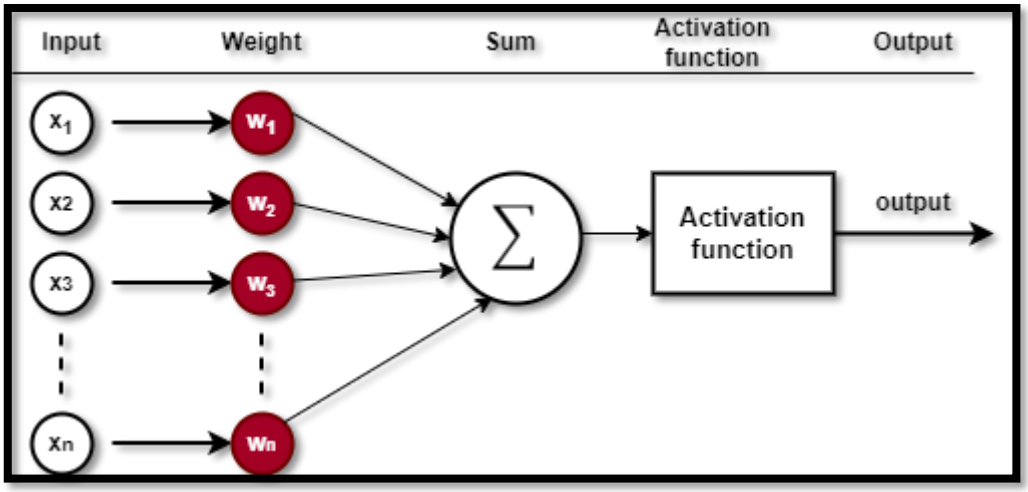


Figure 3.1. Neuron Structure

3.3 Algebraic Structure of the Proposed NLC (S-box)

In academic works, neural networks and algebraic structure are being employed within the Galois field over irreducible polynomials encompassing elements ranging from 0 to 255. In this novel technique, the sequence is permuted with the help of a linear fractional transformation to obtain the preceding output, and then a multilayer perceptron (MLP) is designed to get the optimized proposed S-box. Further, we also introduced an efficient nonlinearity booster algorithm in order to increase the nonlinearity of the proposed nonlinear component.

3.3.1 Preceding Nonlinear Component Design

In order to design a nonlinear component, we applied an algebraic property of linear fractional transformation to $GF(2^n)$ with elements ranging from 0 to 255. The properties of $GF(2^8)$ are used in the designing of 8×8 nonlinear components. AES nonlinear component is based on fixed 8-degree irreducible polynomial$x^8 + x^4 + x^3 + x + 1$. Nizam Chew et al. [100] used another degree 8 irreducible polynomial $x^8 + x^4 + x^3 + x^2 + x + 1$. In Farwa et al. [148], an irreducible polynomial $x^8 + x^6 + x^5 + x^4 + x + 1$ is utilized as a generating polynomial. In Hussain et al.[149], $x^8 + x^4 + x^3 + x^2 + x$ is employed as a generator polynomial. Our chosen irreducible polynomial for design of nonlinear component of block cipher is $x^8 + x^7 + x^5 + x^3 + 1$. For $GF(2^8)$ we can choose any irreducible 8-degree polynomial (see Table 3.1), however the choice of the polynomial has a significant impact on the calculation procedure because it sets the properties and behavior of the transformation. The design of the proposed S-box is based on projective linear group and implemented to $GF(2^8)$. The linear fractional transformation used in the design of proposed nonlinear component of block cipher is given as,

$$f: PGL(2, GF(2^8)) \times GF(2^8) \rightarrow GF(2^8) \tag{3.1}$$

$$f(x) = {(ax + b)}\Big/{(cx + d)} \tag{3.2}$$

Where, $a, b, c, and\ d$ belongs to $GF(2^8)$ and in our case $a, b, c, and\ d$ are $71, 64, 16, and\ 29$ respectively. As long as the condition $ad - bc \neq 0$ is met, any parameter can be used for the variables a, b, d, and d and x varies from 0 to 255. The idea to use this map

for byte substitution is motivated by the better nonlinearity and algebraic complexity of the fractional linear transformation. Calculations are made here in form of byte substitution, $a = 01000111$, $b = 01000000$, $c = 00010000$, and $d = 00011101$.

The procedure starts by utilizing $GF(2^8)$, and the action of $PGL(2, GF(2^8))$ on $GF(2^8)$ produces the function $f(x)$. In order to design the preceding S-box, the function $f(x)$ is utilized. The numerator and denominator are calculated separately after converting them into binary form. The numbers within $f(x)$ are swapped with their corresponding binary values and binary values are represented by some power of ω, Where ω is referred to as the root of the primitive irreducible polynomial. In Table 3.2, elements of $GF(2^8)$are represented by column 4, consisting of elements ranging from 0 to 255. The analytical particulars of linear fractional transformation are enumerated in 2nd column, correspond to the $GF(2^8)$. The outcomes of $f(x)$ are listed in 3rd column of Table 3.2 by utilizing Table 3.3. For example:

$$\mathrm{GF}(2^8) = \mathrm{x} = 0$$

$$\mathrm{f(x)} = \frac{71(\mathrm{x}) + 64}{16(\mathrm{x}) + 29}$$

$$\mathrm{f}(0) = \frac{71(0) + 64}{16(0) + 29}$$

$$\mathrm{f}(0) = \frac{64}{29}$$

Converting 64 and 29 into binary numbers:

$$\mathrm{f}(0) = \frac{1000000}{11101}$$

Now, search 1000000 and 11101into Table 3.3 and take their corresponding ω values as represented in 3rd column of Table 3.2:

$$\mathrm{f}(0) = \frac{\omega^{\,6}}{\omega^{\,158}}$$

Perform subtraction operation: $GF_{Value} = numerator - denominator = 6 - 158 = -152$

If GF_Value value less than zero then add 256 with it as given below:

$$GFValue = -152 + 256$$

$$GFValue = 104$$

$$f(0) = \omega^{104}$$

Search ω^{104} in Table 3.3, take its corresponding GF value in binary format.

$$f(0) = 10101000$$

Next, simply convert 10101000 into decimal format which is equivalent to 168

$$f(0) = 168$$

Finally, 168 is the first value of our preceding nonlinear component which is also presented in 4th column of Table 3.2. Here are key rules to follow when dealing with the numerator and denominator for LFT:

1. If numerator is greater than 255, then take its mod with 256:
$$numerator = mod(numerator, 256)$$
2. If denominator is greater than 255, then take its mod with 256
$$denominator = mod(denominator, 256)$$
3. Perform subtraction operation for calculation of GF value, as given below:
$$GF\_Value = numerator - denominator$$
4. If GF_Value less than zero, then add 256 with it to keep values within range of 0 to 255.

Complexity:

Step 1: Galois Field multiplication and addition: $O(n^2)$ $\therefore$ n represents degree of polynomial, in our case degree of polynomial is 8.

Step 2: Inversion in the Galois field: $O(\log(q)^2)$ $\therefore$ q represents size of the field which is 256

Step 3: Conversion from $f(z)$ to binary: $O(\log(q))$

Step 4: Calculation: $O(256 \times 8^8 \times \log(256)^2)$

Step 5: Overall complexity: $O(256 \times n^2 \times \log(q)^2)$

Computational Cost:

Input size: $GF(2^8)$, $n = 256$

n^2= 65536

$\log_2 n^2$=16

Total Cost:

65536×16= 1048576 operations

Table 3.2: Calculation of $f(x)$ using irreducible polynomial $x^8 + x^7 + x^5 + x^3 + 1$ including balancing factor using Table 3.3

$\boldsymbol{f(x)}$ $\boldsymbol{= GF(2^8)}$	$\boldsymbol{f(x) = \frac{71(x)+64}{16(x)+29}}$	**Here we are using ω from Table-2.**	**Proposed Nonlinear elements.**
0	(71(0)+64/16(0)+29)	f(x)=ω^6/ω^158	168
1	(71(1)+64/16(1)+29)	f(x)=ω^247/ω^217	80
2	(71(2)+64/16(2)+29)	f(x)=ω^251/ω^124	65
3	(71(3)+64/16(3)+29)	f(x)=ω^101/ω^164	36
4	(71(4)+64/16(4)+29)	f(x)=ω^201/ω^236	43
5	(71(5)+64/16(5)+29)	f(x)=ω^228/ω^156	66
6	(71(6)+64/16(6)+29)	f(x)=ω^233/ω^234	1
7	(71(7)+64/16(7)+29)	f(x)=ω^68/ω^46	164
8	(71(8)+64/16(8)+29)	f(x)=ω^42/ω^166	158
9	(71(9)+64/16(9)+29)	f(x)=ω^176/ω^129	179
10	(71(10)+64/16(10)+29)	f(x)=ω^14/ω^37	234
11	(71(11)+64/16(11)+29)	f(x)=ω^164/ω^64	222
12	(71(12)+64/16(12)+29)	f(x)=ω^88/ω^238	91
13	(71(13)+64/16(13)+29)	f(x)=ω^57/ω^119	72
14	(71(14)+64/16(14)+29)	f(x)=ω^53/ω^80	239
15	(71(15)+64/16(15)+29)	f(x)=ω^184/ω^186	212
16	(71(16)+64/16(16)+29)	f(x)=ω^149/ω^158	135
17	(71(17)+64/16(17)+29)	f(x)=ω^136/ω^217	139
18	(71(18)+64/16(18)+29)	f(x)=ω^59/ω^124	9
19	(71(19)+64/16(19)+29)	f(x)=ω^227/ω^164	178
20	(71(20)+64/16(20)+29)	f(x)=ω^67/ω^236	74
21	(71(21)+64/16(21)+29)	f(x)=ω^239/ω^156	229
22	(71(22)+64/16(22)+29)	f(x)=ω^218/ω^234	38
23	(71(23)+64/16(23)+29)	f(x)=ω^74/ω^46	20
24	(71(24)+64/16(24)+29)	f(x)=ω^161/ω^166	206
.	.	.	.
.	.	.	.
.	.	.	.
249	(71(249)+64/16(249)+29)	f(x)=ω^131/ω^129	4
250	(71(250)+64/16(250)+29)	f(x)=ω^226/ω^37	250
251	(71(251)+64/16(251)+29)	f(x)=ω^238/ω^64	251
252	(71(252)+64/16(252)+29)	f(x)=ω^193/ω^238	200
253	(71(253)+64/16(253)+29)	f(x)=ω^24/ω^119	232
254	(71(254)+64/16(254)+29)	f(x)=ω^63/ω^80	19
255	(71(255)+64/16(255)+29)	f(x)=ω^105/ω^186	254

3.3.2 Proposed Galois Field Generation Algorithm

The following algorithm outlines the procedure for calculating the Galois field. Interestingly, this algorithm can generically produce Galois fields by updating the fundamental conditions. Thus, it is capable of working for $GF(2^n)$. See Table 3.3, for binary Galois field for $GF(2^8)$.

1. To represent the chosen irreducible $x^8 + x^7 + x^5 + x^3 + 1$ in binary format, first convert it to [110101001].

$$orgPolynom \leftarrow 110101001$$
$$startingPoint \leftarrow 8$$

2. Calculate 2 raised to the power of 8 and subtracts 2 from the resulting value.

$$endingPoint \leftarrow 2^8 - 2$$
$$endingPoint \leftarrow 254$$

3. Start iterating from starting point to ending point.
4. **Repeat** 8 to 254
    a. Store the copy of chosen irreducible polynomial
    b. Calculate the value of 2 raised to the power of 8 and stores the result in variable 'e'

$$e \leftarrow 256$$

    c. Convert ‘e’ into its equivalent binary $m1 \leftarrow 100000000$
    d. Perform XOR operation between both of the polynomials

$$010101001 \leftarrow 110101001\ XOR\ 100000000$$

    Binary GF for ω^8 (see Table 3.3) = 10101001

    e. If the length of the resultant polynomial exceeds 9, add the necessary number of zeros to the original polynomial (right side) to equalize their lengths.
5. **End**

Table 3.3: Galois Field $GF\ (2^8)$ representation for polynomial $x^8 + x^7 + x^5 + x^3 + 1$

Binary GF	No.	Binary GF	No.	Binary GF	GF		Binary GF	No.	Binary GF	No.
0	00	1	ω^{255}	10	ω^{1}	…	10000	ω^{4}	100000	ω^{5}
1000000	ω^{6}	10000000	ω^{7}	10101001	ω^{8}	…	10111110	ω^{11}	11010101	ω^{12}
11	ω^{13}	110	ω^{14}	1100	ω^{15}	…	1100000	ω^{18}	11000000	ω^{19}
101001	ω^{20}	1010010	ω^{21}	10100100	ω^{22}	…	11010110	ω^{25}	101	ω^{26}
1010	ω^{27}	10100	ω^{28}	101000	ω^{29}	…	11101001	ω^{32}	1111011	ω^{33}
11110110	ω^{34}	1000101	ω^{35}	10001010	ω^{36}	…	1111	ω^{39}	11110	ω^{40}
111100	ω^{41}	1111000	ω^{42}	11110000	ω^{43}	…	10001101	ω^{46}	10110011	ω^{47}
11001111	ω^{48}	110111	ω^{49}	1101110	ω^{50}	…	100010	ω^{53}	1000100	ω^{54}
10001000	ω^{55}	10111001	ω^{56}	11011011	ω^{57}	…	1111100	ω^{60}	11111000	ω^{61}
1011001	ω^{62}	10110010	ω^{63}	11001101	ω^{64}	…	11001100	ω^{67}	110001	ω^{68}
1100010	ω^{69}	11000100	ω^{70}	100001	ω^{71}	…	10100001	ω^{74}	11101011	ω^{75}
1111111	ω^{76}	11111110	ω^{77}	1010101	ω^{78}	…	1010011	ω^{81}	10100110	ω^{82}
11100101	ω^{83}	1100011	ω^{84}	11000110	ω^{85}	…	10010100	ω^{88}	10000001	ω^{89}
10101011	ω^{90}	11111111	ω^{91}	1010111	ω^{92}	…	1000011	ω^{95}	10000110	ω^{96}
10100101	ω^{97}	11100011	ω^{98}	1101111	ω^{99}	…	101010	ω^{102}	1010100	ω^{103}
10101000	ω^{104}	11111001	ω^{105}	1011011	ω^{106}	…	100011	ω^{109}	1000110	ω^{110}
10001100	ω^{111}	10110001	ω^{112}	11001011	ω^{113}	…	11111100	ω^{116}	1010001	ω^{117}
10100010	ω^{118}	11101101	ω^{119}	1110011	ω^{120}	…	11001010	ω^{123}	111101	ω^{124}
1111010	ω^{125}	11110100	ω^{126}	1000001	ω^{127}	…	11110011	ω^{130}	1001111	ω^{131}
10011110	ω^{132}	10010101	ω^{133}	10000011	ω^{134}	…	1000111	ω^{137}	10001110	ω^{138}
10110101	ω^{139}	11000011	ω^{140}	101111	ω^{141}	…	11010001	ω^{144}	1011	ω^{145}
10110	ω^{146}	101100	ω^{147}	1011000	ω^{148}	…	111011	ω^{151}	1110110	ω^{152}
. . .	. . .	. . .	. . .	. . .	. . .	…	. . .	. . .	. . .	. . .
10010000	ω^{195}	10001001	ω^{196}	10111011	ω^{197}	…	101110	ω^{200}	1011100	ω^{201}
10111000	ω^{202}	11011001	ω^{203}	11011	ω^{204}	…	11011000	ω^{207}	11001	ω^{208}
110010	ω^{209}	1100100	ω^{210}	11001000	ω^{211}	…	11100100	ω^{214}	1100001	ω^{215}
11000010	ω^{216}	101101	ω^{217}	1011010	ω^{218}	…	101011	ω^{221}	1010110	ω^{222}
10101100	ω^{223}	11110001	ω^{224}	1001011	ω^{225}	…	10100011	ω^{228}	11101111	ω^{229}
1110111	ω^{230}	11101110	ω^{231}	1110101	ω^{232}	…	11111010	ω^{235}	1011101	ω^{236}
10111010	ω^{237}	11011101	ω^{238}	10011	ω^{239}	…	10011000	ω^{242}	10011001	ω^{243}
10011011	ω^{244}	10011111	ω^{245}	10010111	ω^{246}	…	11100111	ω^{249}	1100111	ω^{250}
11001110	ω^{251}	110101	ω^{252}	1101010	ω^{253}	…				

Table 3.4: Rectified Initial Preceding S-box based on LFT

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

3.3.3 Construction of an Initial NLC Design based on Multilayer Perceptron using Preceding NLC

Artificial intelligence (AI) introduces innovative methods in order to secure communication over the network. AI techniques, including neural networks, contribute to the construction of robust S-boxes, the analysis of patterns, and the development of image encryption schemes. In the proposed method, an artificial neural network is employed for the construction of S-boxes due to their inherent characteristics and training factors. By employing a neural network (multilayer perceptron), the proposed S-box becomes more resistant to various cryptographic attacks. The applications of AI facilitate the creation of refined and optimized nonlinear components and also address the challenges posed by cyber threats. In order to improve the preceding nonlinear component, we designed an artificial neural network (multilayer perceptron) with input, hidden, and output layers. Trained the multilayer perceptron (MLP) using the preceding S-box. Finally, an improved S-box is produced by adjusting training parameters, the initial condition, and the activation function (see Fig. 3.1).

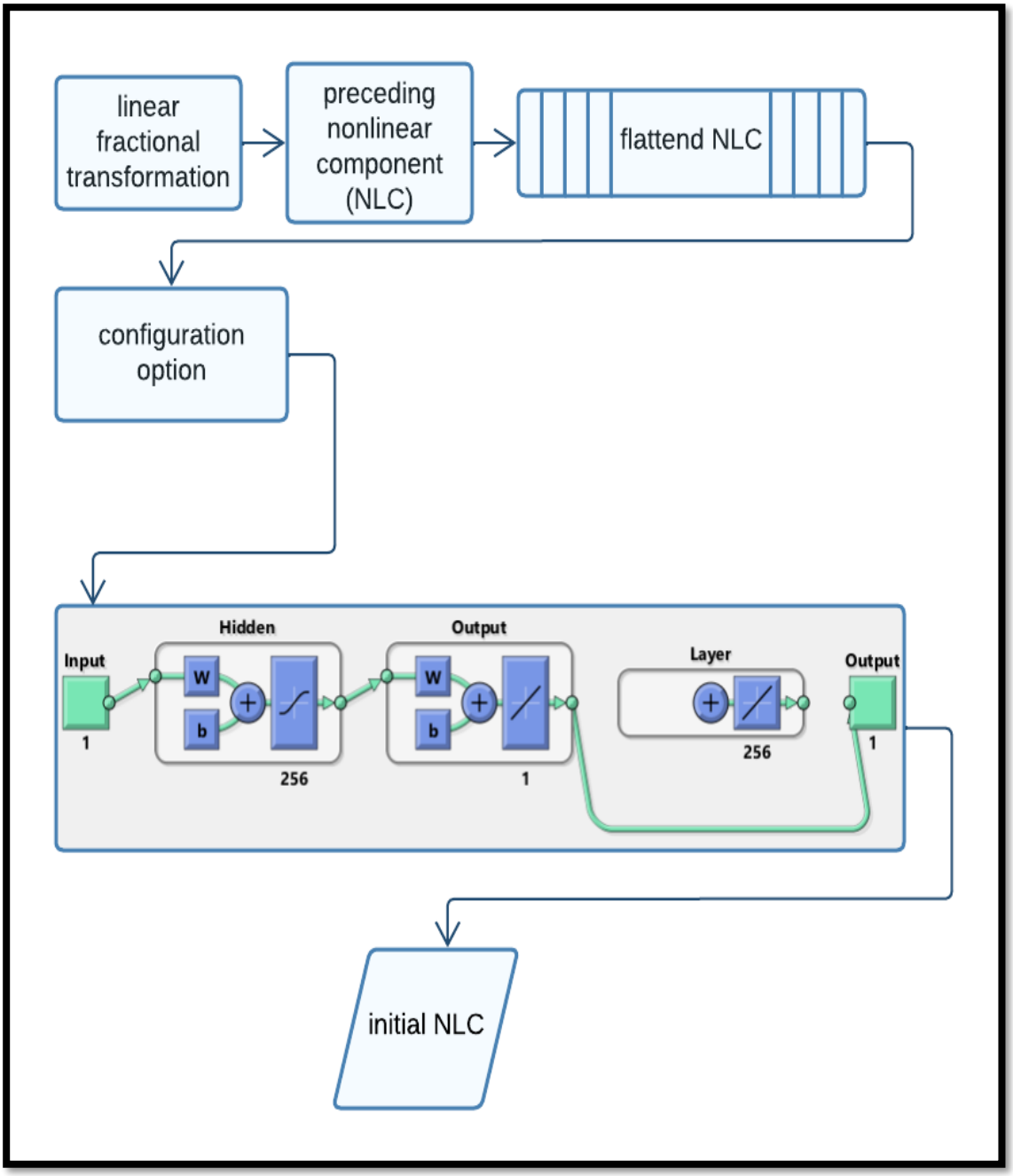


Figure 3.2: S-box design based on LFT and MLP

Figure 3.2 depicts a state-of-the-art method in which the initial S-box is constructed using a preceding S-box. The preceding S-box is designed based on linear fractional transformation to create a complex, secure nonlinear transformation by selecting appropriate parameters $a, b, c, and\ d$ from the Galois field $GF(2^8)$. The preceding S-box is then converted into a row vector for use in a multilayer perceptron (MLP). Configure the MLP by setting options such as the number of input, hidden, and output layers, learning rate, number of epochs,

and activation function. Train the MLP and subsequently apply the trained MLP to the preceding S-box to produce the initial S-box.

The detailed steps of the proposed S-box construction scheme are listed below:

1. Load and convert the preceding nonlinear component into a row vector for MLP.
2. Construct the architecture and set the following control parameters for MLP: the number of input, hidden, and output layers, including hidden units, that is, the number of hidden neurons in each hidden layer. The proposed design includes an input layer with 256 neurons, a hidden layer with 512 neurons, and an output layer with 256 neurons.
3. Selecting the appropriate sizes for input, hidden, and output layers. In our case, the input layer size is equivalent to the size of the nonlinear component or flattened nonlinear component, that is, 256, and the same is true for the size of the output layer, but the size of the hidden layer is one.
4. Set up the configuration for learning rate and training epochs. We adjusted the learning rate to 0.02 and the number of epochs to 1000.
5. Train the MLP using the preceding S-box obtained from linear fractional transformation as inputs and set the parameters for the desired initial nonlinear component as target outputs.
6. Apply the trained MLP to the LFT-based flattened nonlinear component.
7. Rearrange the MLP output to the required size of the nonlinear component.
8. Perform the experimental analysis with different LFT and MLP coefficients and training parameters that result in a robust, efficient, and secure component.

Complexity

Step 1: Input size: n

Step 2: Number of hidden units: h

Step 3: Number of epochs: e

Step 4: Number of samples: N

Step 5: Total Complexity: $O(e \times N \times n \times h)$

```
data = load('precedingSbox.txt'); %data = load('inputSbox.txt');
sBox=reshape(data,16,16);
disp('Original S-box:');
disp(sBox);
sBoxInput = sBox(:)';
inputSize = numel(sBoxInput);
hiddenLayers = 1;       % Number of hidden layers
hiddenUnits = 256;      % Number of neurons in each hidden layer
outputSize = inputSize;  % Size of MLP output is the same as input
net = feedforwardnet(hiddenUnits);
net.numLayers = 2 + hiddenLayers;    % Set the number of hidden layers
net.layers{1}.size = inputSize;      % Set input layer size
net.layers{end}.size = outputSize;   % Set output layer size
net.trainParam.epochs = 1000;         % Number of training epochs
net.trainParam.lr = 0.02;             % Learning rate
net = train(net, sBoxInput, sBoxInput);
mlpOutput = net(sBoxInput);
modifiedSBox = reshape(mlpOutput, size(sBox));
modifiedSBox = mod(round(modifiedSBox), 256);
nl=nonLinearity(modifiedSBox)
if(nl>104)
    disp('Modified S-box:');
    disp(modifiedSBox);
end
```

Figure 2.3. Code snippet for MLP based S-box design

Table 3.5. MLP based initial S-box

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

3.4 Proposed Nonlinearity Booster Algorithms (NLB)

The NLB algorithm operates based on a swapping mechanism. In this algorithm, the initial step involves selecting one element, exchanging it with another element, and subsequently assessing the nonlinearity (NL) of the resulting NLC. If the NL is greater than or equal to the NL of the previous NLC, the swapping is confirmed; otherwise, the swapping is ignored. This process is repeated for all elements, ensuring that the maximum NL is achieved. Once the swapping of individual elements is completed, the algorithm proceeds to work with pairs of elements. The pairs are swapped with two other elements of the NLC. Following the completion of the swapping of pairs, the group size is increased to 4 and subsequently to 8. It is crucial to maintain that the group size is a power of 2^n $where\ n = \{0,1,2,3,4,5,6,7\}$, and swapping occurs only if the NL is greater or equal; otherwise, the swapping is disregarded. Additionally, it is important to specify that the algorithm has the capacity to work on any size of S-box, subject to minor modifications such as adjusting the size of the swapping window.

The following is the algorithm for boosting nonlinearity of a NLC. This algorithm is not limited to boost up the nonlinearity of proposed S-box only, but it is also effective for both existing and proposed S-boxes.

1: $Sbox \leftarrow$ the function LFT(irreduciblePolynomial) generates bijective Sbox(m, n)

2: $convertedSbox \leftarrow$ the function $reshape(Sbox, 16,16)$ converts $Sbox$ into size of 16×16

3: $NL \leftarrow$ the function $nonLinearity(Sbox)$ calculates nonlinearity of current $Sbox$

4: $While(targetedNonlinearity)$

5: $cloneSbox = Sbox$

6: $[cloneSbox(r2, c2), cloneSbox(r1, c1)] = deal(Sbox(r1, c1), Sbox(r2, c2))$

7: $newNL = nonLinearity(Sbox)$

8: $if(newNL > NL \;\&\&\; (cloneSbox(r1, c1)\ not\ equal\ to\ cloneSbox(r2, c2)))$

9: $ArrayStorage \leftarrow cloneSbox$

10: $[cloneSbox(r2, c2), cloneSbox(r1, c1)] = deal(cloneSbox(r1, c1), cloneSbox(r2, c2))$

11: $end\ if$

12: $maxNonlinearity = Scan(ArrayStorage)$

13: $End\ for\ while$

14: $maxNonlinearity = Scan(ArrayStorage)$

15: $Stop$

3.4.1 Objectives of the Proposed Nonlinearity Booster Algorithm

The primary objectives of the proposed NLB algorithm are as follows:

1. Enhance the overall security of the cryptographic system.
2. Enhance resilience by minimizing susceptibility to conventional attacks.
3. Ensure that the S-box enables a more intricate correspondence between input and output bits.
4. Improve the confusion and diffusion characteristics of the encryption algorithm.
5. This algorithm is designed to prevent statistical attacks by reducing the correlation between input and output bits to a minimum.

Best Case Analysis	Average Case Analysis
Step 1: Shaping of an array into matrix: $O(n)$ **Step 2:** Walsh-Hadamard transformation: $O(n\log(n))$ **Step 3:** Swapping operations: $O(1)$ **Step 4:** Window size: 2^k, dimensions of an S-box: $m \times m$ **Step 5:** For each window size k, total number of swaps: $(m-2^k+1)(n-2^k+1)$ **Step 6:** Assuming varying window size and average swaps: $O(m.n.\log(\min(m,n)$ **Step 7:** Scanning for max nonlinearity: $O(n)$ **Step 8:** Overall complexity: $O(m.n.\log(\min(m,n)$	**Step 1:** Shaping of an array into matrix: $O(n)$ **Step 2:** Walsh-Hadamard transformation: $O(n\log(n))$ **Step 3:** Swapping operations: $O(n)$ **Step 4:** Window size: 2^k, dimensions of an S-box: $m \times m$ **Step 5:** For each window size k, total number of swaps: $(m-2^k+1)(n-2^k+1)$ **Step 6:** Maximum number of swaps for each windows: $O(m.n.\log(\min(m,n)$ **Step 7:** Scanning for max nonlinearity: $O(n)$ **Step 8:** Overall complexity: $O(m.n.\log(\min(m,n)$

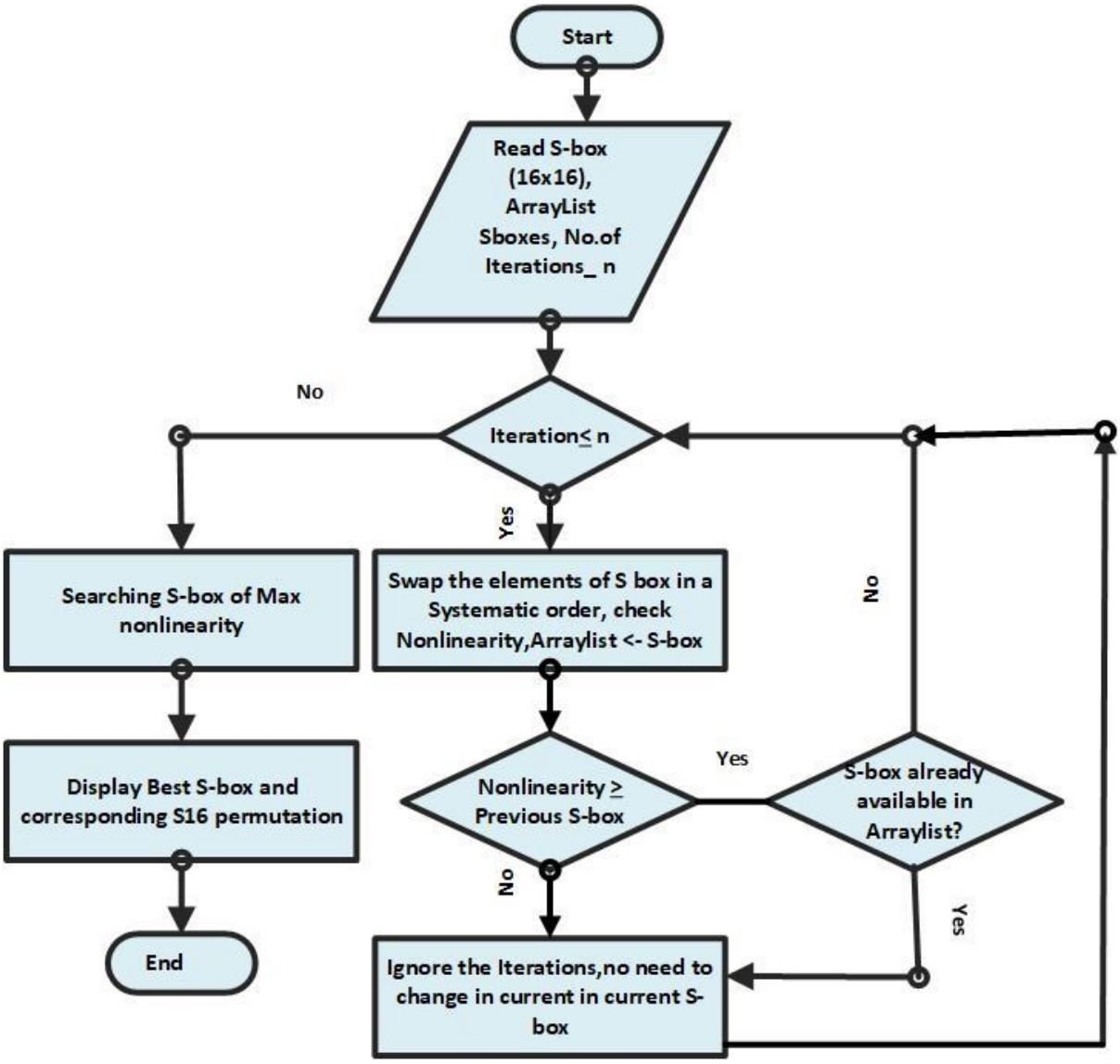


Figure 3.4: Flowchart for nonlinearity booster algorithm

Worst Case Analysis for NLB
Step 1: Shaping of an array into matrix: $O(n)$
Step 2: Walsh-Hadamard transformation: $O(n\log(n))$
Step 3: Swapping operations: $O(n)$
Step 4: Window size: 2^k, dimensions of an S-box: $m \times m$
Step 5: For each window size k, total number of swaps: $(m - 2^k + 1)(n - 2^k + 1)$
Maximum number of swaps for each windows: $O(m.n.\log(\min(m,n)$
Step 6: Scanning for max nonlinearity: $O(n)$
Step 7: Overall complexity: $O(m.n.\log(\min(m,n)$

Table 3.6: Proposed optimized NLC after applying NLB algorithm

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

Table 3.7: Improved nonlinearity results with proposed NLB algorithm

Method	**Existing Average Nonlinearity**	**Improved Nonlinearity using Proposed Algorithm (this work)**
Alghafis [150]	102.875	**110.625**
Zhu [120]	105.75	**111.75**
Zahid-1 [121]	111.75	**112.00**
Zahid-2 [151]	107.00	**111.25**
Artuğer [152]	111.75	**112.00**
Hematpour [153]	105.125	**111.875**
AES [82]	112.00	**113.25**
Javeed [122]	107.50	**109.50**
Skipjack [137]	105.75	**112.00**
Xyi [126]	105.00	**112.00**

3.5 Experimental Work and Security Analyses

This section deals with the experimental analysis to evaluate the cryptographic strength of the proposed S-box construction algorithm. In this regard, the constructed S-box is tested with widely used analysis techniques such as fixed point analysis, reverse fixed point analysis,

strict avalanche criterion, bit independence criterion, linear approximation probability, differential approximation probability, and nonlinearity. All security metrics are implemented in MATLAB R2020a on a laptop having Windows 10 operating system, Intel(R) Core(TM) i5-6300U, CPU @ 2.40GHz 2.50 GHz and RAM of 8.00 GB. The analysis demonstrates that the constructed S-boxes exhibit exceptional performance and can withstand a variety of security attacks, such as linear and differential attacks.

3.5.1 Nonlinearity

Nonlinearity refers to the calculation of the number of bits that must be changed in the truth table of a Boolean function to make it more similar to the nearest affine function. Table 3.8 shows the nonlinearity results for the newly proposed nonlinear component, and Table 3.9 demonstrates the comparison of the proposed nonlinear component with other well-known nonlinear components. It is clearly observed that the nonlinearity of the proposed nonlinear component is higher than that of the AES, APA, Residue Prime, Skipjack, Xyi, etc.

Table 3.8: Nonlinearity of Proposed S-boxes

Proposed S-boxes	**Nonlinearity:**							
	0	1	2	3	4	5	6	7
Proposed Initial S-box-1	110	112	110	110	112	110	110	110
	Average Nonlinearity: 110.50							
Proposed S-box-2 after applying NLB	112	114	114	114	114	116	114	116
	Average Nonlinearity: 114.50							

Table 3.9 contains nonlinearity comparison of our proposed S-box with others well-known S-boxes.

Table 3.9: Nonlinearity Comparison with well-known S-boxes

S-box	1	2	3	4	5	6	7	8	Nonlinearity
Zhu [120]	108	108	106	102	108	102	108	104	105.75
Shahzad [154]	110	112	108	110	110	112	110	112	110.50
Zahid-1 [121]	110	112	112	112	112	112	112	112	111.75
Jiang [68]	108	106	104	106	108	108	108	106	106.75
Hematpour [153]	109	106	104	104	104	106	102	106	105.13
Zahid-2[151]	106	108	108	108	108	106	106	106	107.00
Alghafis[150]	105	103	97	105	105	102	103	103	102.88
Abuelyamam[155]	94	98	100	102	104	104	100	94	99.50
Artuğer[152]	112	112	112	110	112	112	112	112	111.75
Zahid-3[156]	108	108	110	106	110	104	108	106	107.50
Ramzan [157]	107	108	107	108	101	107	110	106	106.75
Hua [103]	105	106	108	106	102	102	108	104	105.13
Javeed[122]	108	106	106	110	106	108	108	108	107.50
Chew [100]	112	112	112	112	112	112	112	112	112.00
Kim [137]	106	104	104	108	108	108	104	104	105.75
AES [158]	112	112	112	112	112	112	112	112	112.00
APA [124]	112	112	112	112	112	112	112	112	112.00
Gray [123]	112	112	112	112	112	112	112	112	112.00
Xyi [159]	106	104	106	104	106	104	104	106	105.00
Proposed optimized S-box (this work)	**114**	**114**	**114**	**114**	**114**	**116**	**114**	**116**	**114.50**

3.5.2 Bit Independent Criterion

The bit-independent criterion implies that output bits are not dependent on each other while alterations of input bits occur in any sequence. This means that there should be no statistical dependence or pattern in the output bits or avalanche output vector. Table 3.10 contains the numerical results of BIC, which are compared in Table 3.17. It can be noticed that our nonlinear component is quite better than renowned nonlinear components.

Table 3.10: BIC Results for Initial S-box

BIC Results of Initial S-box	0	1	2	3	4	5	6	7
	----	0.517578	0.517578	0.533203	0.537109	0.496094	0.513672	0.513672
	0.517578	----	0.515625	0.511719	0.494141	0.519531	0.498047	0.494141
	0.517578	0.515625	----	0.458984	0.501953	0.496094	0.486328	0.521484
	0.533203	0.511719	0.458984	----	0.490234	0.515625	0.505859	0.511719
	0.537109	0.494141	0.501953	0.490234	----	0.484375	0.523438	0.521484
	0.496094	0.519531	0.496094	0.515625	0.484375	----	0.507812	0.535156
	0.513672	0.498047	0.486328	0.505859	0.523438	0.507812	----	0.507812
	0.513672	0.494141	0.521484	0.511719	0.521484	0.535156	0.507812	----
	Average BIC: 0.508							

Table 3.11: BIC Results for optimized S-box

BIC Result After NLB	0	1	2	3	4	5	6	7
	----	0.517578	0.517578	0.482422	0.498047	0.498047	0.509766	0.492188
	0.517578	----	0.494141	0.505859	0.500000	0.531250	0.513672	0.509766
	0.517578	0.494141	----	0.525391	0.505859	0.511719	0.490234	0.513672
	0.482422	0.505859	0.525391	----	0.500000	0.488281	0.511719	0.490234
	0.498047	0.500000	0.505859	0.500000	----	0.501953	0.507812	0.492188
	0.498047	0.531250	0.511719	0.488281	0.501953	----	0.500000	0.500000
	0.509766	0.513672	0.490234	0.511719	0.507812	0.500000	----	0.533203
	0.492188	0.509766	0.513672	0.490234	0.492188	0.500000	0.533203	----
	Average BIC: 0.50							

3.5.3 Strict Avalanche Criterion

This criterion is used to assess the performance of the output bits when the input bit is altered for every cryptographic procedure. It is required that changing a single input bit result in altering half of the output bits. The numerical results of SAC are presented in Tables 3.12 and 3.13 and are compared in Table 3.17. It can be observed that SAC results for our proposed S-box are near the ideal value of SAC, which is 0.5.

Table 3.12: SAC Results for Initial S-box

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
SAC Results of initial S-box	0.51563	0.50000	0.50000	0.46875	0.43750	0.54688	0.46875	0.45313
	0.53125	0.50000	0.48438	0.51563	0.56250	0.46875	0.48438	0.50000
	0.48438	0.50000	0.53125	0.51563	0.48438	0.48438	0.50000	0.50000
	0.53125	0.48438	0.53125	0.53125	0.54688	0.48438	0.51563	0.53125
	0.48438	0.48438	0.57813	0.54688	0.54688	0.51563	0.48438	0.56250
	0.53125	0.48438	0.45313	0.46875	0.54688	0.50000	0.45313	0.45313
	0.46875	0.56250	0.57813	0.50000	0.53125	0.48438	0.53125	0.50000
	0.45313	0.53125	0.48438	0.51563	0.56250	0.46875	0.48438	0.53125
	Average SAC: 0.50							

Table 3.13: SAC Results for optimized S-box

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
SAC Results of optimized S-box	0.54688	0.46875	0.48438	0.51563	0.53125	0.48438	0.51563	0.48438
	0.48438	0.54688	0.43750	0.56250	0.56250	0.53125	0.48438	0.48438
	0.50000	0.48438	0.45313	0.42188	0.43750	0.50000	0.46875	0.48438
	0.46875	0.46875	0.50000	0.54688	0.46875	0.54688	0.45313	0.51563
	0.50000	0.50000	0.53125	0.53125	0.51563	0.50000	0.45313	0.53125
	0.46875	0.50000	0.46875	0.53125	0.48438	0.45313	0.48438	0.53125
	0.53125	0.42188	0.51563	0.50000	0.54688	0.53125	0.46875	0.48438
	0.50000	0.50000	0.46875	0.51563	0.50000	0.50000	0.53125	0.50000
	SAC Results: 0.4975							

3.5.4 Linear Approximation Probability

The event's highest imbalance value is determined by the linear approximation probability. In other words, there is an imbalance in the output bits as a result of input changes. The numerical results of LP are shown in Table 3.14, which are compared in Table 3.17. It is evident that the LP results for our S-box are very close to the ideal value of LP.

Table 3.14: Results for initial and optimized S-boxes

Linear Approximation Probability:		
	Max Count	**Max Value**
LP for Initial S-box-1	164	0.140625
LP for Enhanced S-box-2	162	0.132812

3.5.5 Differential Approximation Probability

To design robust S-boxes, it is preferred that nonlinear transformations demonstrate measurable differential approximation probability analysis. The numerical results of DP are presented in Table 3.15 and compared in Table 3.17. It can be observed that DP results for our S-box are quite better than strong proposed S-boxes.

Table 3.15: DP Results for initial and optimized S-boxes

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	6	8	8	6	8	6	6	6	8	6	8	6	6	6	8
6	8	6	6	6	8	6	10	10	6	6	6	6	6	6	8
6	6	6	6	8	6	10	6	6	6	6	6	6	10	6	8
8	8	6	6	8	6	6	4	6	6	8	6	8	6	6	6
8	6	8	8	10	8	8	6	8	6	6	6	6	6	6	8
6	6	6	6	6	10	8	6	6	6	8	8	6	8	6	6
8	8	8	6	6	6	6	8	8	6	8	8	6	6	6	6
6	4	6	6	6	6	8	8	6	8	8	8	8	6	6	8
6	6	8	6	6	6	6	6	8	8	6	6	6	6	6	6
6	8	8	6	8	8	6	6	8	6	6	10	6	6	6	6
6	6	6	6	8	6	6	6	6	6	6	6	6	6	4	8
4	6	6	8	6	8	8	6	6	6	8	6	6	8	8	6
8	6	8	6	6	8	8	8	6	8	6	6	8	8	6	8
8	8	6	6	6	6	6	8	6	4	6	8	6	6	8	6
6	6	6	8	10	6	6	8	6	8	8	8	6	6	8	6
6	8	8	8	8	8	6	8	4	6	8	8	6	6	8	6
Max DP Value for Initial S-box-1=10															
Max DP Value for Initial S-box-2=10															

3.5.6 Correlation Immunity

Correlation immunity for a nonlinear component refers to the correlation between the input and output bits in relation to linear and differential cryptanalysis. It is measured using the correlation coefficient, which ranges from 0 to 1. A correlation coefficient close to 0 indicates low correlation, whereas one close to 1 indicates high correlation. It can be expressed mathematically using the following equation:

$$CI_i = max_{\Delta x \neq 0, \triangle y \neq 0} |corr(NLC(x), NLC(x \oplus \Delta x) \oplus \Delta y)| \qquad (3.3)$$

Where,

$NLC(x)$ is the output of the nonlinear component for the input x.

Δx a change in the input.

Δy a change in the output.

Table 3.16 contains correlation immunity results for initial and optimized S-box.

Table 3.16: Correlation coefficient for initial and optimized S-box

Correlation vector for initial S-box	0.0217	0.0477	0.0004	0.0781	0.0781	0.0004	0.0477	0.0217
Correlation vector for optimized S-box	0.0171	0.0422	0.0625	0.0554	0.0554	0.0625	0.0422	0.0171

In order to assess the several properties of nonlinear component a comparative analysis is presented in detail (see Table 3.17).

Table 3.17: Majority Logic Criterion comparison

S-box	Nonlinearity			SAC	BIC-NL	BIC-SAC	DP	LP
	MaxVal	MinVal	AvrVal	AvrVal	AvrVal	AvrVal	MaxVal	MaxVal
Razaq [160]	116	112	113.75	0.5017	104.00	.5018	12	0.1328
Razaq [161]	112	110	111.25	0.5029	110.78	0.5007	6	0.0781
Zhu [120]	108	102	105.75	0.5021	104.14	0.5050	10	0.1328
Zahid [121]	112	110	111.75	0.5029	103.74	0.5005	10	0.125
Zahid [151]	108	106	107.00	0.4968	103.50	0.5039	10	0.1562
Razaq [162]	108	104	106.75	0.5031	103.64	0.5073	12	0.1328
Razaq [163]	110	106	108.25	0.4985	103.00	0.5057	10	0.1406
Razaq [164]	112	112	112.00	0.5014	112.00	0.5030	4	0.0625
Zahid [156]	110	104	107.5	0.4980	103.50	0.5005	10	0.125
Razaq [165]	112	112	112.00	0.5056	112.00	0.5192	4	0.625
Alghafis [150]	105	97	102.87	0.5192	102.67	0.4787	54	0.1679
Zahid [166]	108	104	106.75	0.5070	103.92	0.4997	14	0.125
Jiang [68]	108	104	106.75	0.4975	103.57	0.5022	10	0.1328
Shahzad [154]	112	108	110.50	0.5031	109.21	0.5018	6	0.0859
Razaq[157]	110	101	106.75	0.5031	103.57	0.5005	10	0.1289
Hua [103]	108	102	105.25	0.5351	103.25	0.5087	-	0.1406
Javeed [122]	110	106	107.50	0.4997	104.64	0.5048	12	0.1406
Hematpour [153]	109	102	105.25	0.4960	104.53	0.5045	-	0.1328
Nizam Chew [100]	112	112	112.00	0.4980	112.00	0.4981	4	0.0625
Artuğer [152]	112	110	111.75	0.4968	104.00	0.5016	12	0.125
Proposed Optimized S-box	**116**	**114**	**114.50**	**0.4975**	**103.28**	**0.5050**	**10**	**0.1328**

3.5.7 Fixed Point and Reverse Fixed Point

A fixed point is an unchanging value under a given transformation [35]. In other words, a fixed point is an input value that remains unchanged while passed through the function.

Whereas, opposite fixed point are specific to function dealing binary values. An opposing fixed point is present when the function applied on the opposite (flipped) version of the input value yields the original input value [36] [37]. Mathematically, both of these are represented as

Let S-box $S: GF(2^n) \rightarrow GF(2^m),\ u \in GF(2^n)$ (1.6)

3. If $S(u) = u$, a point is referred to as the fixed point of the S-box.

4. If $S(u) = u'$, a point is referred to as the opposite fixed point of the S-box. Where $u'$is the opposite/complement of u.

Table 3. 18. Fixed point and reverse fixed point

S-box	Fixed Point(s)	Reverse Fixed Point(s)
Proposed Optimized S-box	**None**	**None**
Ref [167]	3	1
Ref [168]	18	None
Ref [169]	1	1

3.6 Summary

This chapter presents a two-step methodology for designing secure S-boxes. The first step involves constructing the S-box using Linear Fractional Transformation (LFT). Following this, an artificial neural network, specifically a multilayer perceptron, is employed to refine the initial S-box design, potentially enhancing its cryptographic properties. To rigorously assess the effectiveness of these S-boxes, the chapter utilizes established testing methodologies. Furthermore, the study introduces a novel adaptive method specifically focused on improving the S-box's nonlinearity, a crucial aspect for cryptographic strength.

CHAPTER 4

CHAOTIC NONLINEAR COMPONENT DESIGN FOR ROBUST IMAGE ENCRYPTION SCHEME

4.1 Overview

Chaos refers to unpredictable behavior that can emerge from relatively simple deterministic systems. However, chaos itself does not refer to determinism. Additionally, chaos does not follow a regular pattern and does not converge to a value, despite being constrained. Chaotic systems' reliance on their initial conditions and control parameters is their key characteristic. The proposed image encryption scheme connects the topological features of 2-D maps, specifically their chaotic behavior and fractal properties; without altering their underlying mathematical structures. To achieve this, proposed methodology employs the Zaslavsky, Baker, and Hénon maps in a multi-stage process that strategically blends confusion and diffusion for enhanced security against a wide range of attacks. In the initial confusion stage, chaotic values accurately disrupt the arrangement of both rows and columns within the image, effectively reducing correlations between adjacent pixels. This is followed by a precisely designed diffusion step, which controls the 2-D Baker and Hénon maps to induce a potent avalanche effect, ensuring that any minute alterations to the original image propagate extensively throughout the encrypted output. Moreover, we also presented three nonlinear components for the purpose of utilizing them in proposed image encryption. To assess the security and computational efficiency of the proposed image encryption method, various analyses such as correlation, contrast, entropy, energy, homogeneity, and performance are conducted. Additionally, the effectiveness of the three proposed nonlinear components is evaluated through cryptographic analysis tests, including nonlinearity, strict avalanche criterion, differential probability, linear probability, and bit independence criterion.

4.2 Introduction

Chaotic behavior is not an uncommon occurrence. This behavior is seen across a very broad spectrum, from computer science to mathematics, economics to electronic circuits, engineering to social sciences, and from human body behavior to wild population distribution. The design of cryptographic chaotic maps and their application to image encryption using chaotic system dynamics is one of the most popular applications of chaotic systems in electrical engineering and computer science [144]. Nonlinear component structures based on chaos are one of the most effective examples of this relationship [170]. Image encryption methods differ significantly from those used for textual data due to the distinct structural properties of visual information. Textual data exhibits a higher degree of redundancy, allowing encryption algorithms to leverage patterns and repetitions. However, images present unique challenges due to their inherent complexity and visual patterns. The authors [171], presented is a novel image encryption algorithm that leverages modern diffusion techniques to achieve rapid transmission while preserving the compact statistical characteristics of the original image.. In their research, [172] explored a multi-layered color image cryptosystem that integrates fractional-order hyper-chaotic maps with pseudo-random number generators (PRNGs). Reference [114] provides a comprehensive analytical review of the construction of nonlinear components. Reference [173] explored a remarkably efficient image encryption algorithm that achieves robust confusion by intertwining pixel shuffling with grayscale value alterations. The widespread and successful employment of PRNGs within image cryptosystems is extensively reported throughout a rich tapestry of literature examples. In a groundbreaking development, [174] unveiled a novel image encryption paradigm secured in True Random Number Generation (TRNG).

Recently, researchers [175] have shown enthusiasm for employing "chaotic maps" to conceal images. These maps are like crazy jumbles of numbers that are hard to guess, making them good for scrambling secret images. Chaotic maps are scientific methods that are highly sensitive to initial conditions and parameters. They are beneficial for producing random numbers and establishing nonlinear transformations [176]. The presented method by researchers [177] utilized Arnold's cat map to shuffle images and also utilized cyclic chaos and PRNG as additional security measures. We built our understanding of these algorithms as foundational concepts, drawing inspiration from this source [88]–[180]. In the encryption of chaotic images, the usual practice involves interchanging the positions or values of pixels in the

original image through the utilization of a chaotic stream cipher. Similarly, the researchers [13] introduced an innovative framework for encrypting images by employing two hyperchaotic maps and the single neuron model (SNM). The authors [167] utilized a coset graph, a mathematical tool for representing group structures, to design an S-box with improved cryptographic characteristics. The researchers [181] presented a big data architecture and general framework with the ability to process, analyze, and ensure the performance and security of data for big data applications. In [182], a thorough analysis of applications based on blockchain in the context of security and privacy is provided. The technique presented by researchers [183] is effective for feature extraction in image analysis and pattern recognition tasks and often used in applications like image classification, object detection, and texture analysis. The Zaslavsky map [179] is a two-dimensional chaotic map that has found applications in cryptography. It's defined by a set of nonlinear equations and exhibits complex, unpredictable behavior even in response to slight changes in its initial conditions. Researchers have explored the Zaslavsky map in various domains, including its use in generating pseudorandom numbers and constructing cryptographic algorithms such as S-boxes [184]. The Hénon map [180] is a two-dimensional map known for its chaotic behavior. This characteristic has led to its extensive use as a foundational element for cryptographic primitives, including the construction of nonlinear components in block ciphers and stream ciphers [185], [186]. Like the Hénon map, Baker's map [178] is also a two-dimensional map with diverse applications in cryptography, signal processing, and image processing.

The study in [187] presented a new one-dimensional chaotic system (1-DFCS) and a dynamic mutual image encryption technique (SDME) utilizing 1-DFCS. The approach improves security and time efficiency by using dynamic diffusion and confusion, together with a newly developed plain image sensitivity function. Gao [188]constructed a 2D hyperchaotic map from two one-dimensional chaotic maps and subsequently proposed a method for image encryption using this 2D map. Liu et al. [189] introduced a new n-dimensional conservative chaos system derived from the generalized Hamiltonian system. This system addresses security weaknesses in chaos-based encryption by exhibiting exceptional chaotic properties, real-time communication capability, and resilience against various attacks. The authors [190] proposed a new method for encrypting images by using a chaotic sequence and a modified AES algorithm. In a similar manner, Liu et al. [191] proposed an image encryption algorithm that combines conservative hyperchaotic systems with biological gene algorithms in order to mitigate

weaknesses found in existing techniques. The authors in [192] enhanced a chaotic map by using fuzzy numbers and introducing an additional layer of randomization via the use of a bifurcation diagram. The experimental results confirm that the suggested cryptosystem is highly resistant to well-known security and statistical studies. The study in [48], [193], presented a key-dependent S-box generation technique using a novel non-degenerate two-dimensional enhanced quadratic map (2D-EQM) exhibiting both ergodicity and unpredictability.

Shah et al. [194] introduced a technique using extended Galois rings. This approach led to significantly increased confusion levels in S-boxes. They further applied these S-boxes to achieve high encryption quality for RGB images. Researchers in [195] proposed an image encryption scheme based on a newly developed hyper-chaotic system with a high Lyapunov exponent. This system generates keystreams for image pixel rearrangement and substitution, enhancing the encryption process's security. Wang et al. [196] proposed an image encryption approach based on a spatiotemporal chaotic system with dynamic S-boxes and randomized blocks. Simulations showed its effectiveness in transforming images into unreadable encrypted data. Genetic algorithms, like the one presented in [55], have been used to create S-boxes with desired characteristics. A crucial aspect for strong cryptography is high nonlinearity, which these algorithms can help achieve. Combining chaotic and Boolean functions offers resilience. Chaotic maps of various dimensions (1D, 2D, 3D, and 4D) have been used for S-box creation, as seen in [197], [198]. Liu et al. [199] investigated a third-order nonlinear digital filter and its behavior with discrete sine inputs. Based on the filter's characteristics, they proposed an S-box generation method that results in bijective S-boxes. Hyper-chaos offers additional complexity and unpredictability in encryption. Tong et al. [200] proposed a method to enhance block cipher security through S-boxes constructed using mixed chaotic systems. Their approach combines different techniques like index-based chaotic systems, pseudo-random number generators, and Henon mapping to achieve increased nonlinearity. A novel approach using the Choquet Fuzzy Integral and DNA techniques proposed in [201] to improve S-box security. This work also developed an image encryption system specifically designed to secure digital photographs. Security assessments demonstrated its resistance against various attacks. While multi-dimensional chaotic S-boxes offer increased security, their complexity can lead to longer processing times and potentially hinder real-time applications.

4.3 Overview of Different Chaotic Map

In the study of chaotic maps, dynamic systems create a state that appears random and entirely disordered but is intricately controlled by the initial conditions. The study of the relationship between completely random chaotic outputs and the underlying patterns that give rise to them is explained by chaos theory. When the interconnection of a generator is known, these patterns can be scrutinized in great detail. Such generators typically rely on the system's capacity to demonstrate a feedback loop, repeat patterns, showcase self-similarity, and manifest fractal behavior. Chaotic maps come in two varieties: continuous and discrete, and they can be based on either complex or real numbers. Some chaotic maps even extend into four dimensions. However, the majority of chaotic maps discussed in the literature are one or two dimensional. The following is a brief explanation of chaotic maps

4.3.1 Zig Zag Chaotic Map

Zigzag maps exhibit excellent chaotic behaviors and are used to generate true random numbers. Nejati et al. [202] investigate this map in depth and look into its essential chaotic properties and parameters. The generalized zigzag map is a mapping function that can be described as

$$x_{n+1} = -m(x_n + 2/|m|) \quad (4.1)$$

$$x_{n+1} = mx_n \quad (4.2)$$

$$x_{n+1} = -m(x_n - 2/|m|) \quad (4.3)$$

Where x_n varying from -1 to 1 and m is a real number.

4.3.2 Logistic Chaotic Map

In spite of its formal simplicity, the logistic map is a one-dimensional discrete-time map that demonstrates a surprising level of complexity [203]. During the early stages of research on deterministic chaos, it was one of the most significant and paradigmatic systems. Mathematically, the map is given by the equation:

$$x_{n+1} = rx_n(1 - x_n) \quad (4.4)$$

Where x_n represents the initial condition at generation n, r is the controlling parameter for growth rate ($3.5 < r \leq 4$), and x_{n+1} represents the population at next generation. Moreover, the chaotic characteristics of the logistic map render it valuable for creating pseudo-random numbers. This use is essential in simulations, cryptography, and many techniques that need randomization.

4.3.3 Lorenz System

The following three ordinary differential equations made up Lornez's atmospheric convection model.

$$\frac{dx}{dt} = \sigma(y - x) \quad (4.5)$$

$$\frac{dy}{dt} = rx - y - xz \quad (4.6)$$

$$\frac{dz}{dt} = xy - bz \quad (4.7)$$

Where, $x, y, and\ z$ indicate the convection flow, horizontal temperature distribution, and vertical temperature distribution, respectively. Whereas sigma (σ), rho (ρ), and beta (β) represents the ration of viscosity to thermal conductivity, temperature difference, and ration of the width to the height, respectively.

4.3.4 Zaslavasky Map

The Zaslavasky Map stands as a 2D classical instance demonstrates chaotic behavior. This map includes four controlled parameters that regulate it i.e., $Nu\ (\nu)$, $Tau\ (\tau)$, $Mu\ (\mu)$, and $Epsilon\ (\varepsilon)$ that influence the map behavior. The Zaslavasky map applies a mapping to a point (x_n, y_n) on the plane, resulting in a new point. It is particularly known to produce chaotic numbers despite its simple mathematical structure.

4.2.5 Henon Map

The Henon map functions in two dimensions, discrete-time, nonlinear chaotic scheme that exhibits chaotic behavior. This map is notably acclaimed for its capacity to generate complex numbers and unpredictable behavior, even with its simple formulation. With the help of this map, two sets of values can be generated. One can be used for the confusion process and

the other for the diffusion process. The control parameters of this map are two, i.e., Depending on the values of and, regular behavior can be generated.

4.3.6 Baker's Map

It is possible to think of the Baker's map as a chaotic, dynamic system that operates inside the unit square. Its title originates from the kneading technique utilized by bakers to make dough. The dough is split into two equal pieces, stacked on top of one another, and compressed. Baker's map can be utilized to achieve the following objectives:

1. Generate chaotic values
2. Generate keys in the range $\{0,1,2,\dots,2255\}$
3. Generate prime numbers with Baker's map

4.3.7 Four Dimensional Hyperchaotic System

A 4D hyperchaotic system is a nonlinear dynamic system that exhibits chaotic behavior in four-dimensional space, meaning that it has at least two positive Lyapunov exponents. Which represents that the system is sensitive to initial conditions and unpredictable behavior. Which means a small change in the initial condition can lead to an entirely different state. In this chaotic system, four dimensions are involved. These dimensions can generate complex and irregular patterns, which can be useful in image encryption, secure communication, and different computations. Due to the large dimensionality of hyperchaotic systems, hyperchaotic theory focuses on 4D hyperchaotic systems. In our proposed image encryption technique, the following 4-D hyperchaotic system is utilized, which was proposed by Ishkakova [204].

$$D_{0,t}^{\delta}x(t) = a.y.z \qquad (4.8)$$

$$D_{0,t}^{\&}y(t) = bx - xz - cx \qquad (4.9)$$

$$D_{0,t}^{\delta}z(t) = d.x.y - xw \qquad (4.10)$$

$$D_{0,t}^{\delta}w(t) = x - ew + y \qquad (4.11)$$

In this work, we investigate some dynamical features and the paramount values for a, b, c, d and delta for getting best results regarding image encryption.

4.4 Proposed NLC design and optimization algorithm with chaotic maps

The Zaslavsky map algorithm's proposed scheme encompasses a sequence of precisely defined procedures aimed at producing pseudorandom numbers (PRNs). The procedure starts by assigning starting values to the variables, which are then used in the computation of the parameter. After determining the value of μ, a loop is initiated to perform two million (2,000,000) iterations.. The Zaslavsky map equations find application inside this iterative process to compute the updated values of x and y. Subsequently, these updated values are utilized to determine two pseudorandom numbers (PRNs). The PRNs are shown in both decimal and binary formats, and the variables x and y are reassigned with their updated values for the subsequent iteration of the loop. The technique has the capability to be iteratively executed with modifications in order to produce extended sequences of PRNs. The algorithm's efficacy stems from its inherent chaotic properties, rendering it challenging for a potential adversary to predict the sequence of PRNs. produced. Here is a procedure to generate customized nonlinear component with Zaslavasky map without modifying its mathematical structure.

Step 1. Assign values to the variables $x, y, v, e, and\ \tau$ to specific values during initialization. The proposed construction scheme includes $x = 0.19, y = 0.21, v = 7, \tau = 5, \epsilon = 2.7$

Step 2- The numerical value of μ is determined by the following equation

$$\mu = \frac{1-e^{-\tau}}{\tau} \qquad (4.12)$$

Step 3- Repeat (size<=200000)

Step 3.1- Compute updated values for x_1 and y_1 using following equations

$$x_1 = mod(y_n + v(1 + \mu z_n) + \epsilon v \mu z_n \cos(2\pi y_n), 1) \qquad (4.13)$$

$$y_1 = e^{-\tau}(z_n + \cos(2\pi y_n)) \qquad (4.14)$$

Step 3.2- Generate initial pseudo random number using x_1 through the utilization of the provided equation:

$$updated\_X = floor[\, mod\big(floor\big(x_1 \times (2^{275-1})\big), 256\big)] \qquad (4.15)$$

Step 3.3- Converting $updated\_X$ into its binary equivalent

Step 3.4- Determine the first complement of binary number-1

Step 3.5- Produce second pseudo random number using $y_1$by employing the given equation:

$$updated\_Y = floor[\, mod\big(floor\big(y_1 \times (2^{275-1})\big), 256\big)] \qquad (4.16)$$

Step 3.6- Converting $updated\_X$ into its binary equivalent

Step 3.7- Determine the first complement of binary number-2

Step 3.8- Perform XORing between both of the binary numbers to get the values of desired nonlinear component

Step 4- End of repetition/loop

Step 5- To designa trustworthy nonlinear component (S-box), implement a permutation on the newly generated pseudo-random numbers.

Table 4.1: Proposed chaotic S-box derived from modified Zaslavsky map

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

In connection with the Henon map, the method shown below begins by assigning starting values to variables x and y, as well as to parameters. Additionally, the algorithm specifies the total number of iterations to be executed. The Henon map undergoes 1.5 million iterations (1,500,000) to create a series of values for the variables. These values are then used to compute a new value for x. The aforementioned value is thereafter multiplied by a designated value and truncated to get a pseudorandom number. The given number is restricted to a range of values from 0 to 255 by the process of calculating its modulus with 256. The aforementioned

procedure is repeatedly performed until the attainment of the necessary bijective values, which are thereafter arranged into a 16×16 S-box. The subsequent algorithm outlines the process of creating a secure S-box utilizing the Henon Map:

Step 1. Initialize the variables $x\ and\ y$ by assigning the value of 2.33 and 1.91, respectively.

Step 2. Specify the values of parameters $a, b, and\ size,$ a=1.7, b=0.5

Step 3. Repeat 1 to size=1500000

Step 3.1. $x_{n+1} = 1 + y_n - ax_n^2$

Step 3.2. $y_{n+1} = bx_n$

Step 3.3. Both of the above equations (Steps: 3.1 and 3.2) will produce next values x_{n+1} and y_{n+1}

Step 3.4. Utilize newly produced value x_{n+1}, multiply it by (2^{275-1}) and after that round down it using the floor function through given equation

$$newNo = \left(floor\left(x_{n+1} \times (2^{275-1})\right)\right) \qquad (4.17)$$

Step 3.5. Compute the modulo operation of the newly generated number with 256 to obtain a value within the range of 0 to 255.

Step 3.6. Perform following bit shuffling permutation on newly generated number

Step 3.6.1. Transform new number into its equivalent binary number

Step 3.6.2. Execute flip operation on binary number

Step 3.6.3. Reverse the flipped binary number and transform it into its equivalent decimal number.

Step 3.6.4. Store the flipped number into an arrayList

Step 3.7. End of loop

Step 3.8. Arrange the newly generated flipped numbers into nonlinear component.

Step 3.9. – **end**

Table 4.2. Proposed S-box obtained from the modified Henon map

41	59	187	201	10	221	147	193	163	154	36	38	191	114	246	141
74	243	98	121	58	153	53	178	228	19	245	215	255	92	203	78
222	250	34	152	249	133	179	165	168	186	240	69	86	229	97	12
167	51	83	173	199	218	254	182	55	113	60	16	80	224	183	65
22	81	110	176	115	91	251	211	26	219	45	161	140	57	162	238
137	207	210	216	71	117	101	61	31	24	205	151	73	190	47	66
202	135	46	50	148	119	40	177	170	122	233	100	2	84	33	105
39	129	220	4	127	52	169	208	252	14	164	54	144	62	21	64
76	209	37	17	150	241	189	13	156	108	149	239	118	204	155	213

235	244	206	67	226	212	116	126	146	192	124	0	42	1	232	188
128	35	175	227	120	111	225	43	3	56	25	194	214	109	236	130
15	248	94	185	72	231	70	20	230	145	157	132	196	88	63	123
103	77	49	99	89	28	85	112	7	87	75	198	242	44	160	181
79	142	139	174	159	90	166	106	107	18	11	247	95	200	172	27
68	180	93	234	32	5	143	48	138	171	30	195	217	158	253	136
184	104	134	237	102	125	223	96	82	131	8	9	29	23	197	6

The Baker's map constructs an S-box by specifying the parameters and the desired arrangement. The two distinct branches of this map alter the variables. The adjusted values are kept in the xSboxkey and ySboxkey arrays, respectively. The values of the S-box exhibit chaotic behavior, characterized by their representation as floating-point numbers. Multiplying the provided floating numbers by a specified factor or key and then performing a modulo operation with a divisor of 256 keeps the resultant value within the range of 0–255.How to make an S-box using Baker's map is shown below.

Step 1. Initialize the coordinates $x \; and \; y$ by assigning the value between 0 and 1 and between 0.5 to 1

Step 2. Define the control parameter a and set its values in the range of $0 \; to \; 0.5$

Step 3. Set the variable size that represents number of chaotic values to be generated

Step 4. $\boldsymbol{Repeat}$ $1 \; to \; specific \; size$, that is, 2000000

Step 4.1. Execute the provided equations for $0 \leq x \leq 0.5$

$$x \leftarrow 2 * x$$

$$y \leftarrow a * y$$

Step 4.2. Execute the following equations when $0.5 < x \leq 1$

$$x \leftarrow 2x - 1 \qquad y \leftarrow a * y + 0.5$$

Step 4.3. Store the results of step x and y into two different arrays (xSboxKey, ySboxKey)

Step 4.4. Perform multiplication for each value of xSboxKey with a specific number, that is 49 and then take its mod with 256 to keep the values in the range of 0 to 255.

Step 4.5. Transform each value of xSboxkey into its equivalent binary number

Step 4.6. Select the key for addition based hash permutation between transformed number and key

Step 4.7. Organize the values into an S-box of size 16 by 16

Step 5. End

Table 4.3: Proposed S-box based on modified Baker's Map.

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

Table 4.4. Experimental Results and Comparison with known S-boxes

S-box	**LP**	**SAC**	**Nonlinearity**			**BIC-NL**	**BIC-SAC**	**DP**
	MaxVal	AvrVal	MaxVal	MinVal	AvrVal	AvrVal	AvrVal	MaxVal
Ref [129]	0.125	0.5043	106	98	101.50	104.28	0.5071	12
Ref [120]	0.1328	0.5021	108	102	105.75	104.14	0.5050	10
Ref [121]	0.125	0.5029	112	110	111.75	103.74	0.5005	10
Ref [150]	0.1679	0.5192	105	97	102.87	102.67	0.4787	54
Ref [68]	0.1328	0.4975	108	104	106.75	103.57	0.5022	10
Ref [154]	0.0859	0.5031	112	108	110.50	109.21	0.5018	6
Ref [103]	0.1406	0.5351	108	102	105.25	103.25	0.5087	-
Ref [122]	0.1406	0.4997	110	106	107.50	104.64	0.5048	12
Ref [153]	0.1328	0.4960	109	102	105.25	104.53	0.5045	-
Ref [100]	0.0625	0.4980	112	112	112.00	112.00	0.4981	4
Ref [152]	0.125	0.4968	112	110	111.75	104.00	0.5016	12
Proposed S-box-1	**0.1406**	**0.4956**	**116**	**112**	**113.75**	**103.42**	**0.4992**	**10**
Proposed S-box-2	**0.125**	**0.4978**	**116**	**112**	**114.25**	**103.41**	**0.5044**	**10**
Proposed	**0.1328**	**0.5063**	**112**	**112**	**112**	**103.86**	**0.4987**	**10**

S-box-3								

4.5 Novel Image Encryption Algorithm Based on Multiple S-boxes

In the field of cryptography, both one-dimensional (1-D) and two-dimensional (2-D) maps find use. In general, one-dimensional (1-D) maps are often used for the purpose of generating encryption keys or digital signatures. However, a notable concern arises from the fact that the keys created using 1-D maps tend to possess limited size, as well as a reduced level of complexity and unpredictability. Nevertheless, 2-D maps are deemed to be more secure as a result of their greater key size, parameters, spatial characteristics, and complexity. That's the reason we employed 2-D maps (Zaslavasky, Henon, Bakers). The maps attained a state of chaos in order to exhibit nonlinear and dynamic characteristics.

The proposed image encryption technique starts with an initial evaluation to determine the color mode of the image, distinguishing between grayscale and RGB. Subsequently, a validation process is conducted to determine if the dimensions of the image possess divisibility by 16. In the event that this criterion is not met, image is expanded by appending more pixels to the boundary until both the width and height are divisible by 16. The following section presents a method designed to address the problem of perfect division.

1. Analyze and compute the precise measurements of the image's height and width.

2. Determine the nearest or equal multiples of 16 that correspond to the current height and width. The new values must be assigned the identifiers 'new_height' and 'new_width'.

3. Calculate the difference between the current height and width values and the values assigned to the variables 'new height' and 'new_width'.

4. Construct the empty canvas using the dimensions of new height and new_width.

5. Replicate the original image and position it in the middle of the canvas. The remaining region is filled with white pixels. The image used for padding exhibits a property of being evenly divisible by 16.

Following the partitioning of the image into 16×16 blocks, a swapping step is executed. This process entails interchanging the upper diagonal elements of the first block with the lower diagonal elements of the final block, and vice versa. Additionally, it requires swapping the lower diagonal elements of the initial block with the higher diagonal elements of the last block. The technique described above is systematically performed for each individual block included in the image. After the completion of the swapping method, a row-wise substitution is performed on each value of every block using the proposed chaotic S-box to encrypt the image. A detail process of encryption and decryption are thoroughly discussed below:

4.5.1 Image Encryption Steps

In order to encrypt the image, the following steps need to be executed in a sequential fashion:

1. Read the original image to be encrypted.
2. Count the number of channels in order to determine whether the image is grayscale or RGB.
3. Ensure that the image is divisible by 16 using the proposed algorithm regarding the problem of perfect division.
4. Divide the image into various blocks of different sizes. In this way, separate blocks disclose nothing about the original image.
5. Perform a systematic swapping mechanism that includes interchanging the upper diagonal elements of the first block with the lower diagonal elements of the final block, and vice versa. Additionally, it requires swapping the lower diagonal elements of the initial block with the higher diagonal elements of the last block.
6. Substitute each block of input image with chaotic S-boxes in the given sequence, such as replacing the first block with the Zaslavasky-based S-box, the second with the Henon-based S-box, and the third with the Bakers-based S-box.
7. XORing updated blocks with proposed chaotic S-boxes ensures that, during addition, both blocks are not the same.
8. Image is encrypted (see Figure 4.1).

However, if the dimensions of the image are not evenly divisible by 16, a padding approach is used. Add additional pixels to the image on the sides until both the width and height are evenly divisible by 16.

Complexity

Step 1: Read an image: $O(n)$

Step 2: Access time: $O(1)$

Step 3: Calculate dimensions: $O(1)$

Step 4: Pixels padding: $O(n)$

Step 5: Partition operation/divisions: $O(n)$

Step 6: Substitution operation: $O(n)$

Step 7: XORing operation: $O(n \times m)$ $\therefore n$ represents number blocks and m represents size of each block

Step 7: Overall complexity: $O(n^2)$

Overall Space Complexity:

Overall Space complexity: $O(n)$

Moreover, newly designed nonlinear components in block ciphers offer practical recommendations for enhancing multimedia security. They play a crucial role in applications like Virtual Private Networks (VPN) and Transport Layer Security (TLS), ensuring secure communication. These components are also integral to guaranteeing message integrity and authentication through digital signatures. Additionally, when transmitting data embedded in images, nonlinear components effectively scramble image pixels, facilitating secure transmission over communication channels.

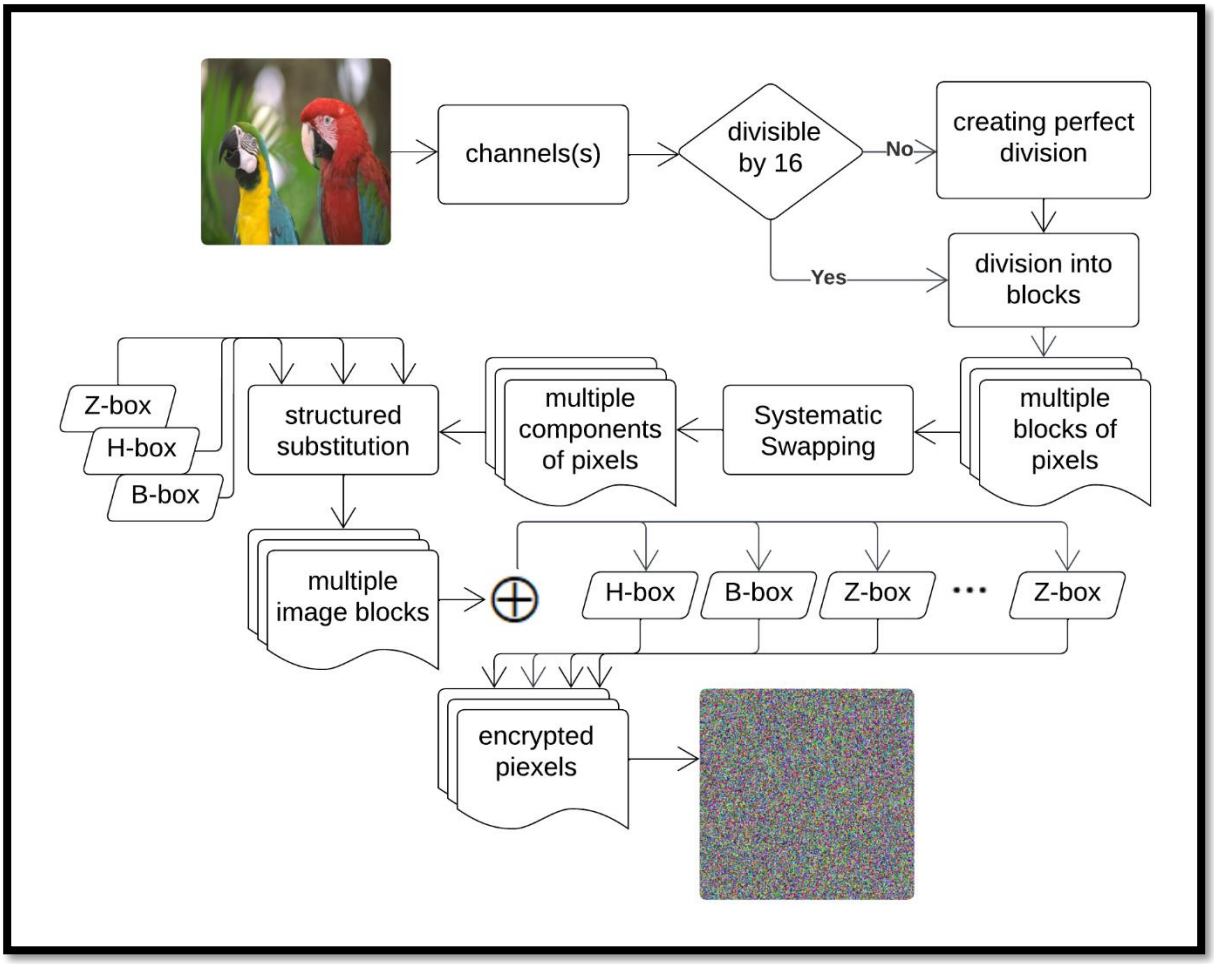


Figure 4.1: Chaotic S-boxes based Image Encryption Scheme

In addition, we chose an image block with dimensions of 16x16 for the following reasons:

1. Our image encryption algorithm utilizes a 16x16 S-box, which is a well-recognized and standardized size.
2. The 16×16 image block offers an optimal trade-off between cryptographic robustness and computational efficiency. This size ensures strong nonlinearity, immunity to linear and differential cryptanalysis, and compatibility with contemporary cryptographic techniques.

A MATLAB program has also been developed to conduct experiments by varying parameters within a defined range and observing the resulting chaotic behavior. Simultaneously, the performance of the encryption scheme is assessed using different parameter combinations. Based on the evaluation results, the parameter selection is refined to

optimize encryption performance. This fine-tuning of the parameters aims to find the best combination for optimal results. After performing millions of iterations, the optimized parameters are selected.

To decrypt encrypted image, simply execute the encryption steps in reverse order. This involves systematically reversing the sequence of encryption operations that were originally applied during the encryption process. By following the reverse sequence accurately, the encrypted image can be effectively deciphered, restoring it to its original, unencrypted state.

4.6 Experimental Setup and Security Analyses

This section deals with the experimental analysis to evaluate the cryptographic strength of the proposed S-box construction algorithm. In this regard, the constructed S-box is tested with widely used analysis techniques such as fixed point analysis, reverse fixed point analysis, strict avalanche criterion, bit independence criterion, linear approximation probability, differential approximation probability, and nonlinearity. All security metrics are implemented in MATLAB R2020a on a laptop having Windows 10 operating system, Intel(R) Core(TM) i5-6300U, CPU @ 2.40GHz 2.50 GHz and RAM of 8.00 GB. The analysis demonstrates that the constructed S-boxes exhibit exceptional performance and can withstand a variety of security attacks, such as linear and differential attacks. Moreover, several experimental tests are also carried out for the proposed image encryption algorithm on the same machine with the same configuration using MATLAB 2020a to examine its performance and security properties. The experimental images are standard RGB and grey images from the UEF—SIPU and USC—SIPI image collections. Statistical analyses, Visual analyses, and differential analyses reveal the strength of the proposed method. Tables 5.7 (greyscale images), 4.5- 4.11 (RGB images), and 6.5 to 6.8 list several image quality measures to compare the proposed encryption process's results with those of the standard known encryption schemes. Furthermore, RGB images are selected over other modes due to several reasons:

1. RGB images contain color data, which is essential for various image processing tasks like object detection, segmentation, and classification.

2. RGB images provide enhanced versatility for manipulation and processing.
3. RGB images are aesthetically pleasing and more closely approximate the perception of the world by humans.

4.6.1 Histogram Analysis

Image processing requires image histogram analysis, which involves examining and interpreting the distribution of pixel intensities within an image. The frequency of intensity values, ranging from dark to bright, across the entire image is depicted in a histogram. The presence of peaks, valleys, or gaps can be identified by analyzing the histogram. These key characteristic provide clues about the image's tonal range and potential issues such as overexposure or underexposure. The distribution of the plain images histogram and their equivalent encrypted images are illustrated in Figure 4.2, 4.3, and 4.4. Figure 4.4 shows the obvious peaks and changes in the original image's grey value distribution, which is not uniform. The histogram distributions, on the other hand, are more consistent and lean toward being horizontal for the corresponding encrypted image in Figure 4.5. The results demonstrate that our proposed encryption algorithm can produce an encrypted image that is statistically secure.

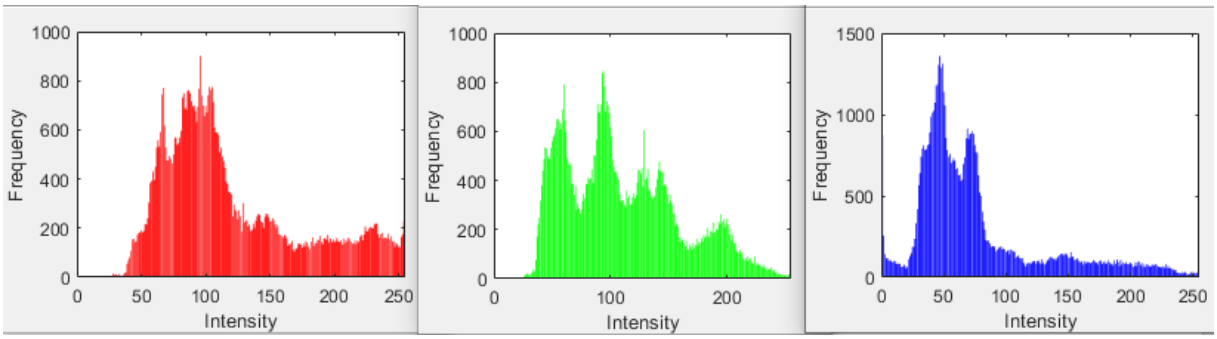


Figure 4.2: The Histogram of a plain image of parrots

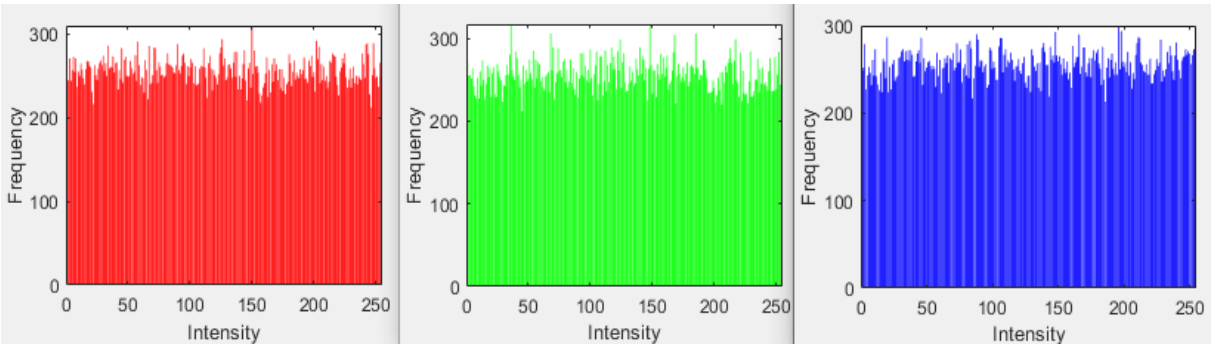


Figure 4.3: The Histogram of an encrypted image of parrots

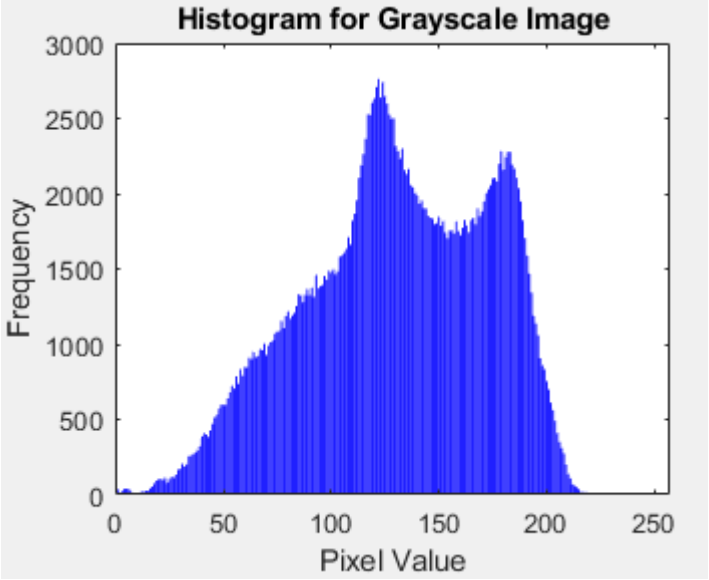


Figure 4.4: The Histogram of a plain grayscale image of a baboon

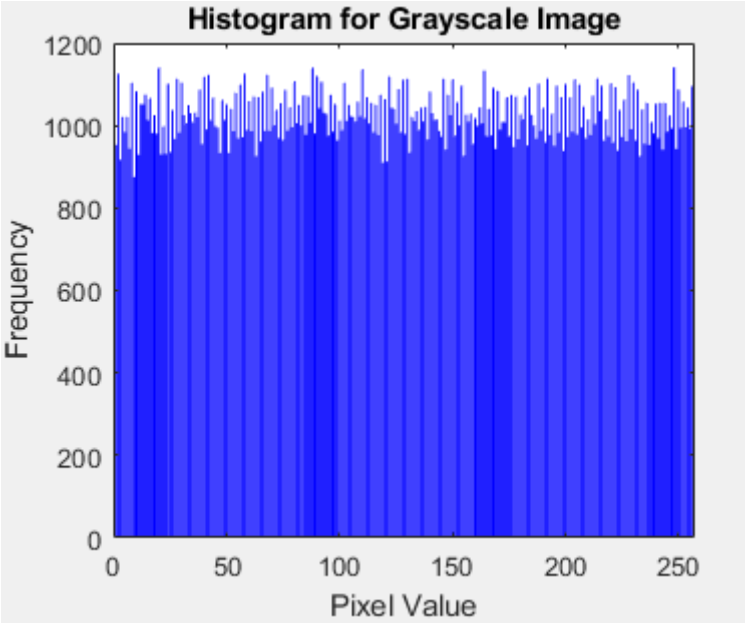


Figure 4.5: The Histogram of an encrypted grayscale image of baboon

4.6.2 Image Entropy Analysis

Image entropy analysis is a technique for calculating the degree of randomness or uncertainty in an image. The amount of disorder or randomness in a system is measured mathematically using the concept of entropy. Entropy can be used to calculate an image's complexity or level of detail in image analysis. Analyzing the distribution of pixel values within an image allows one to determine its entropy. Each pixel in a digital image has a numerical value that corresponds to its color or brightness. An image's entropy rises when a wide range of pixel values are present, indicating a more intricate or detailed image. On the other hand, an image with a constrained range of pixel values will have a lower entropy and seem more simple (see Table 4.1). The mathematical formula for calculating entropy analysis is given as follows:

$$H = \sum p(i) log_2 p(i) \qquad (4.18)$$

Where H is the image's entropy, p(i) is a pixel's chance of having a certain value, and log2 is the binary logarithm. A high entropy is preferable for encrypted images, as it signifies randomness and resistance to analysis. However, specific entropy value for images is typically close to 8 bits per pixel/byte.

Table 4.5: Entropy Analysis

Images	Size	Plain Image Entropy	Encrypted Image Entropy
Parrots	256×256	R 7.4754 G 7.4519 B 7.1752	R 7.9973 G 7.9963 B 7.9973
Lena	256×256	R 7.2778 G 7.5788 B 7.0300	R 7.9973 G 7.9970 B 7.9972
Pepper	256×256	Gray 7.5769	Gray 7.9973
Airplane	256×256	Gray 6.7542	Gray 7.9225
Baboon	256×256	Gray 7.2595	Gray 7.9973
House	256×256	R 6.4311 G 6.5389 B 6.2320	R 7.9971 G 7.9972 B 7.9972

4.6.3. Image Energy Analysis

Energy is a term used in digital image processing to describe the amount of information in an image. Image energy analysis is especially helpful for locating areas of interest or significant information in an image. The squared values of each pixel in an image are added to determine the energy of the image. According to mathematics, an image's energy is determined by:

$$E = \sum m \sum n \; I(m,n)^2 \qquad (4.19)$$

Where $I(m,n)$ denotes the value of the pixel located at (m,n) in the image. High-energy images have a wider range of pixel values, which denotes a more intricate and complex image. The overall brightness and contrast of an image are related to its energy. A limited range of pixel values and simpler appearance characterize low-energy images (see Table 4.2). Image segmentation, object detection, and feature extraction are just a few of the uses for energy analysis that can be beneficial. For instance, energy analysis can be used to pinpoint areas of an image that contain important object features when performing object detection.

Table 4.6: Energy analysis

Images	Size	Plain Image Energy	Encrypted Image Energy
Parrots	256×256	0.17466	0.029776
Lena	256×256	0.12177	0.029823
Pepper	256×256	0.11082	0.015645
Airplane	256×256	0.35137	0.016221

Baboon	256×256	0.092992	0.015643
House	256×256	0.19522	0.02959

4.6.4 Image Homogeneity Analysis

The measurement of the uniformity or similarity of pixels within an image is known as image homogeneity analysis. It is a crucial technique for image processing and analysis because it can be used to find areas of an image that share common traits or to spot changes and anomalies in an image. There are several methods for performing image homogeneity analysis, including statistical measures such as variance or standard deviation, texture analysis techniques, and image segmentation algorithms. The gray-level co-occurrence matrix (GLCM) method is one frequently employed technique for assessing image homogeneity. Utilizing this technique, the homogeneity of the image is determined by computing a matrix that represents the distribution of pixel values in an image and then examining its characteristics. It is calculated by using the following formula:

$$H = \sum_{i,j=0}^{k-1} \frac{P(i,j)}{1+(i-j)^2} \qquad (4.20)$$

Where $\sum(i,j)$ refers to adding up all possible combinations of the GLCM matrix's pixel values i and j and $P(i,j)$ is the probability of the occurrence of the combination of pixel values (see Table 3.3).

Table 4.7: Image homogeneity analysis

	Homogeneity		
Images	**Direction**	**Plain Image**	**Encrypted Image**
Parrots	256×256	0.9182	0.4715
Lena	256×256	0.8797	0.4705
Pepper	256×256	0.8954	0.3899
Airplane	256×256	0.8981	0.3958
Baboon	256×256	0.7781	0.3878
House	256×256	0.9221	0.4709

4.6.5 Image Correlation Analysis

A method for comparing two or more images to see how closely they resemble one

another is called image correlation analysis. It entails figuring out the correlation between two images, which expresses how linearly pixel values are correlated in the images (see Table 4.4). In this analysis, the images are typically aligned before calculating the correlation coefficient to ensure that the corresponding pixels are compared. Applications for image correlation analysis can be found in pattern recognition, computer vision, and image processing. In addition to image compression, it is used in motion tracking, object recognition, and image registration. Mathematically,

$$Correlation = \sum i \sum j \, (1 - \mu i)(j - \mu j) * G(i, j) \qquad (4.21)$$

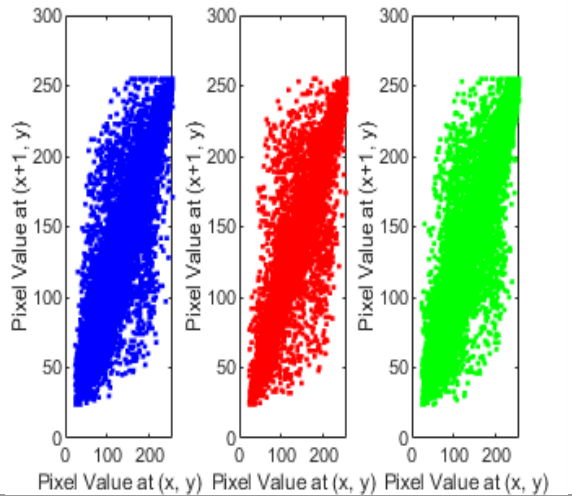
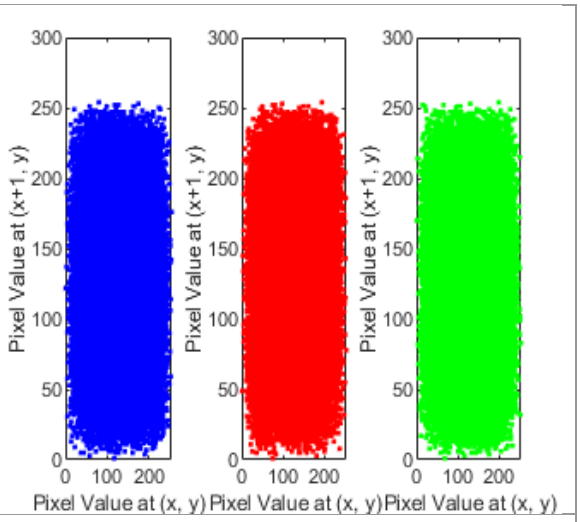
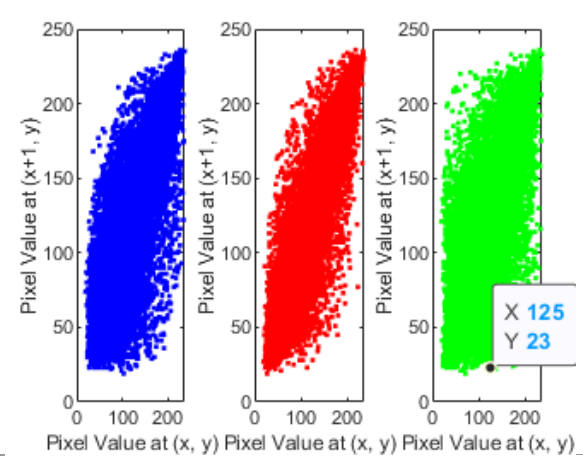
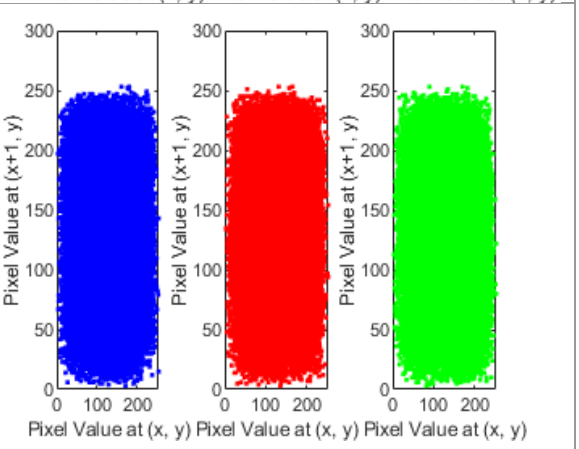
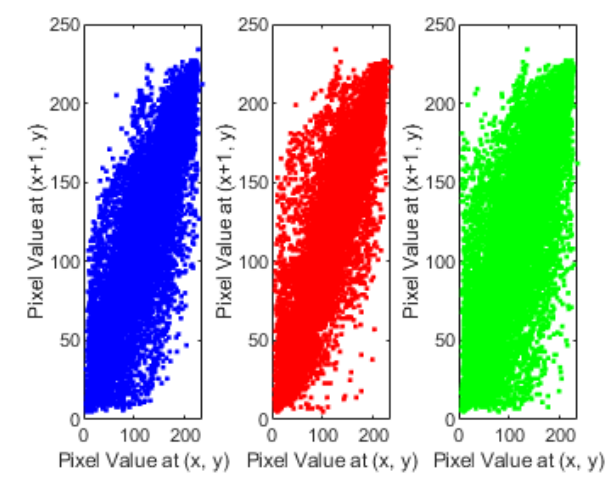
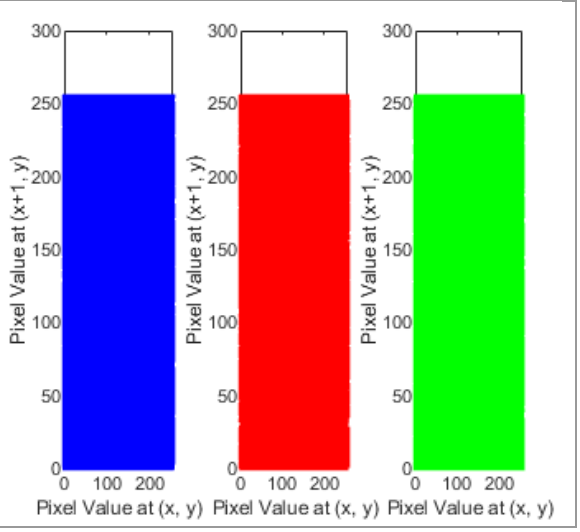
Where i and j are the means of the respective rows and columns of the GLCM matrix G. Additionally, Table 4.5 contains correlation coefficient graph.

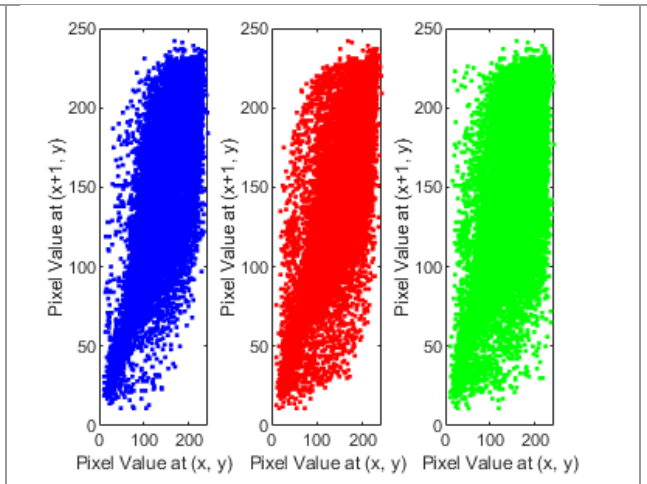
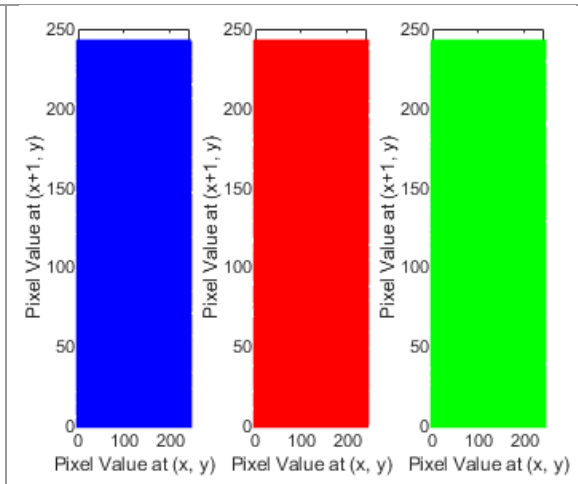
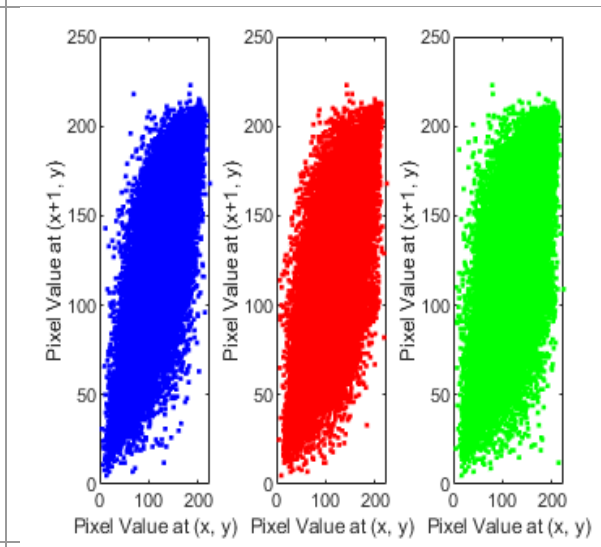
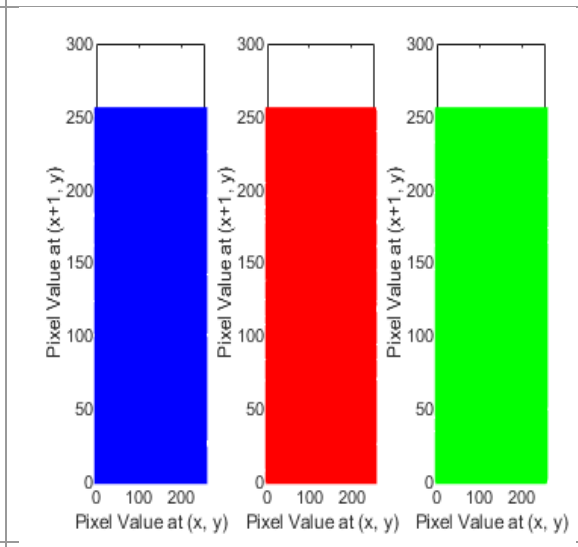
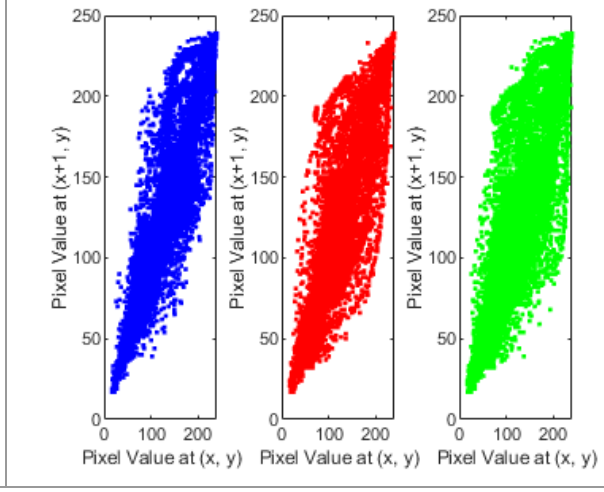
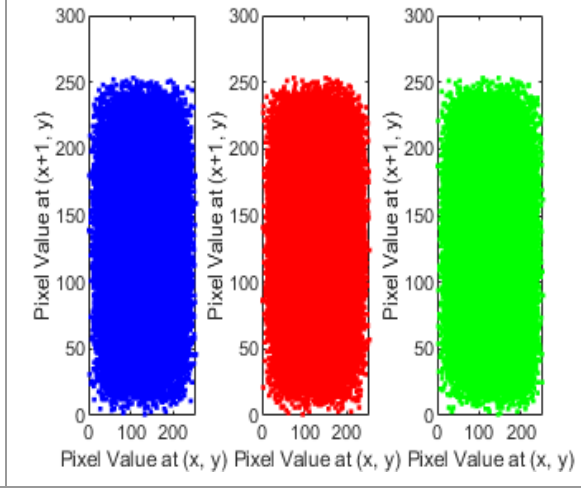
Table 4.8: Correlation analysis

		Correlation	
Images	**Direction**	**Plain Image**	**Encrypted Image**
Parrots	Horizontal	0.9707	-0.0042
	Vertical	0.9767	0.0227
	Diagonal	0.9597	-0.0027
Lena	Horizontal	0.9238	-0.0003
	Vertical	0.9598	0.0243
	Diagonal	0.8938	-0.0022
Pepper	Horizontal	0.9578	-0.0068
	Vertical	0.9652	0.0674
	Diagonal	0.9276	-0.0049
Airplane	Horizontal	0.9245	-0.0041
	Vertical	0.9207	0.0072
	Diagonal	0.8665	0.0040
Baboon	Horizontal	0.8409	-0.0057
	Vertical	0.7862	-0.1283
	Diagonal	0.7447	0.0015
House	Horizontal	0.9727	0.0049
	Vertical	0.9467	0.0030
	Diagonal	0.9263	-0.0051

Table 4.9: Coefficient correlation graphs for plain and encrypted images

Image	Plain Image coefficient correlation	Encrypted Image coefficient correlation

Parrots		
Lena		
Pepper		

Airplane		
Baboon		
House		

4.6.6 Image Contrast Analysis

Image contrast analysis is a method for determining how brightly different areas of an image are from one another. Contrast affects the visibility and clarity of details in an image,

making it a crucial component of image quality. Images with high contrast typically have more visual impact and are simpler to interpret (see Table 4.6). Application areas for image contrast analysis include computer vision, remote sensing, and medical imaging. One can learn useful details about an image's composition and contrast by measuring its contrast. Mathematically,

$$Contrast = \sum_i \sum_j G(i,j) * (i-j)^2 \qquad (4.21)$$

Where $(i-j)^2$is the difference in squared pixel values between the two images, and $G(i,j)$ is the normalized GLCM element at position (i,j).

Table 4.10: Contrast Analysis

Contrast			
Images	**Size**	**Plain Image Entropy**	**Encrypted Image Contrast**
Parrots	256×256	R 0.2699 G 0.2531 B 0.2735	R 10.4373 G 10.4702 B 10.5470
Lena	256×256	R 0.3833 G 0.4060 B 0.3563	R 10.5707 G 10.3348 B 10.4828
Pepper	256×256	0.3206	10.6010
Airplane	256×256	0.3684	9.7719
Baboon	256×256	0.6243	10.5514
House	256×256	R 0.2042 G 0.1918 B 0.2867	R 10.5169 G 10.4295 B 10.3673

4.6.7 Comparison

In this section, the proposed analysis is explained and shown in Table 4.7 and Table 4.8. Alongside other schemes presented in literature. The proposed image encryption scheme entropy, contrast, correlation, energy, and homogeneity are with other well know algorithms. According to results, the proposed scheme analysis is better than others which demonstrates that the proposed scheme the proposed scheme is highly resistant to attacks.

Table 4.11: Texture comparison analysis

Analysis Method	Entropy	Contrast	Correlation	Energy	Homogeneity

Proposed (Lena Image)	7.9971	10.4828	0.0087	0.02982	0.4705
Gray [4]	7.9299	7.7961	0.1014	0.0198	0.4567
AES [205]	7.84018	7.423085	0.088914	0.035476	0.389521
Xyi[4]	7.9127	7.8942	0.1413	0.0188	.4605
Prime [206]	7.669541	6.477377	0.098544	0.037190	0.48858

Table 4.13: Comparison of entropy analysis for baboon and Lena image

Method	**Entropy**
Proposed (Baboon)	**7.9973**
Proposed (Lena)	**7.9972**
Idrees [196]	7.9969
Faragallah [207]	7.6238
Ahmad [208]	7.9966
Wang [209]	7.9971
Wu [210]	7.9909

4.7 Summary

This chapter investigates the application of three chaotic maps, specifically the Zaslavasky, Henon, and Baker's maps, in the development of S-boxes. The structures of these maps are modified to suit the design requirements of the S-boxes. The cryptographic characteristics of these altered S-boxes have been comprehensively assessed. Furthermore, the study showcases the practical utilization of these S-boxes by implementing them inside the framework of image encryption. This thesis endeavors to provide valuable insights into the efficacy of employing modified chaotic maps without disturbing their mathematics structures for the creation of S-boxes, as well as their potential application in enhancing the security of image data.

CHAPTER 5

OPTIMIZING IMAGE SECURITY WITH COSET GRAPH

5.1 Overview

A coset graph is a graph that represents the cosets of a subgroup in a group. Let H be a subgroup of G, the group. The coset graph of G with respect to H is represented by the notation $\tau(G, H)$. The security of some cryptographic systems, especially those based on group actions, can be examined using coset graphs. In some circumstances, coset graphs can be used to assess the computational difficulty of the discrete logarithm problem. The coset graph $\tau(G, H)$ is a random graph with a high probability if the group G is a cyclic group of prime order and the subgroup H is also cyclic and generated by a random element. The coset graph, on the other hand, may not be random and may contain useful information for tackling the discrete logarithm problem if the subgroup H is not chosen at random but instead has some unique structure. Overall, coset graphs offer a practical approach for evaluating the security of cryptographic systems based on collective actions and can help in the discovery of flaws in these systems. A field extension in mathematics and computer science is the creation of a larger field through the addition of components to an already existing field. It is commonly used in cryptography. A field extension is indicated as $F(a)$, where F is the basic field and "a" is an addition to F. In this chapter, we introduce an innovative image encryption algorithm based on coset graphs and field extensions. In the first stage, an algebraic structure is defined, that is, an extension of the real numbers ($\mathbb{R}$) to complex numbers ($\mathbb{C}$). The generated extension field is subsequently used in the construction of a coset graph based on the chosen field. A coset graph is constructed using complex numbers as vertices. The vertices are shifted circularly to get the desired number of edges. The vertices of the coset graph map to pixels of the image and assign a unique identification to each pixel within the graph.

5.2 Introduction

Nonlinear components, also known as S-boxes, are key for modern cryptography because they help to keep cryptographic algorithms secure. In order to achieve desirable properties like nonlinearity and diffusion, nonlinear components are typically designed using algebraic structures like Galois fields and finite rings. Coset graph-based S-box design and optimization have shown promising results in terms of efficiency and security for a wide range of algebraic structures, including finite fields, field extensions, rings, and groups. As a result, the construction of S-boxes using coset graphs is a subject of growing interest in the cryptography community and is likely to be a focus of active research for years to come. Coset graphs [211] offer a graph-theoretic representation of an algebraic structure that can be used to create S-boxes with desirable properties. In particular, the coset graph approach allows for efficient implementation and analysis and is used to design S-boxes with desirable cryptographic strength. In [162], the authors employed the coset diagram as a foundation for their novel nonlinear component proposal. In order to determine how well this new nonlinear component would protect cryptographic algorithms, they thoroughly analyzed its strength through extensive cryptanalysis. With the use of chaotic maps or algebraic operations, some researchers have created S-boxes that exhibit significant nonlinearity. The modular group by $PSL\ (2\ ,Z)$, initiated by $l: s \to -1/s$ and $m: s \to s-1/s$., represents a group of linear fractional mappings. The $PSL\ (2\ ,Z)$, finite display is $< l, m: l^2 = m^3 = 1 >$. Modular groups are the only infinite discrete groups that are used extensively in number theory, advanced group theory, geometry, and topology. Coset diagrams [212] are derived from $PSL\ (2\ ,Z)$ actions on a projective line over the finite field $GF(p^n)$, denoted by $PL(F_{p^n}) = GF(p^n) \cup \{\infty\}$, where p is a prime.

Singh [213] represented how codes and ciphers have shaped wars, nations, and lives. Through fascinating storytelling and intelligent research, the book examines encryption's significance in historical events from wartime espionage to present cybersecurity issues. The authors [214] focused on communicating the essentials and minimizing mathematics, moving quickly from foundations to practical implementations, including recent topics like lightweight ciphers for RFIDs and mobile devices and key-length recommendations. Cryptanalysis, sometimes referred to as code breaking, is an interesting discipline that utilized diverse methods to decipher the concealed information contained in encrypted messages [215]. In cryptography

and image encryption schemes, field extensions are frequently utilized to introduce additional mathematical structures and operations that enhance the security and complexity of the encryption process by adding more mathematical structures and operations. It is possible to do numerous algebraic operations and transformations on the image data by expanding the base field. The cryptographic system requirements and desired extended field properties will determine which field extension is selected. Field extensions are commonly employed to expand real numbers to complex numbers, extend rational numbers to algebraic numbers, and create finite fields (Galois fields). The research [216] aims to construct S-boxes on the elements of the multiplicative subgroup of the Galois field rather than the entire Galois field. Asif et al. [217] presented powerful and robust S-boxes based on the Galois field with powerful confusion capability and applications in image encryption. These are several common fields that can be extended [218].

1- The field of real numbers (R) can be broadened to encompass complex numbers (ℂ), which have a real and an imaginary part. Complex numbers are given as $a + b\acute{\imath}$, where a and b are real numbers and ί is the imaginary unit (√(-1)). When real numbers are extended to complex numbers, new mathematical structures and operations are introduced, including complex conjugation, multiplication, and division of complex numbers.

2- Algebraic numbers can be added to the field of rational numbers (ℚ). Algebraic numbers are those that have solutions to polynomial equations with rational coefficients. This extension is widely used in algebraic geometry and number theory.

3- Finite fields or Galois fields $GF(p^n)$ can be created by extending prime fields, such as the field of integers modulo a prime number (Z_p). Finite fields are used extensively in cryptography, error correction codes, and coding theory due to their finite number of elements. The extension of prime fields to finite fields necessitates the introduction of additional operations like field addition, field multiplication, and modular arithmetic. In the case that a complex number lacks an imaginary part or if the imaginary part is zero, it is equivalent to a real number. This is a straightforward mapping from the complex number to the real number in this case. For instance, a complex number $z = a + 0\acute{\imath}$, where z is the same as real number and a is a real number. The mapping between z and a is represented as $z \rightarrow a$. In other words, a real number is the only kind of number that can be created by a complex number when its

imaginary part becomes zero. Based on elements like the nature of the image data, the required cryptographic features, and the computing effectiveness of the encryption algorithm, a suitable field extension can be chosen in the context of image encryption. This research [219] introduces a digital encryption technique that is based on finite fields and has two primary stages of diffusion and permutation. The overlapping rows and columns of image pixels are mixing during the Diffusion stage when matrix multiplication operations in the GF (256) are used, resulting in the mixing of the pixels. The 2D chaotic map in $GF(2^n)$ or the 3D chaotic map in the GF field 2^k are used during the permutation stage to alter the position of image pixels. Chen et al. [220] proposed improved image encryption algorithm with better efficiency based on 2D chaotic map derived from Sine map.

5.3 Proposed Image Encryption Scheme with Coset Graph

In this chapter, we designed a novel image encryption algorithm based on field extension, coset graph, and a known chaotic map. The main objective of this scheme is to create a robust algorithm that guarantees authentication and integrity. First, we define the algebraic structure, that is, the extension of the real numbers to complex numbers. The generated extension field is subsequently used in the construction of a coset graph based on the chosen field. A coset graph is constructed using complex numbers as vertices. The vertices are shifted circularly to get the desired number of edges. The vertices of the coset graph map to pixels of the image and assign a unique identification to each pixel within the graph. Then, in order to generate a secure key sequence, a logistic chaotic map is utilized based on the properties of the coset graph. Next, we proceed to apply the rotation transformation to the coset graph. Afterward, the image is encrypted by performing the mod operation on the mapped vertices. Additionally, security keys are also used to further enhance the security of the encryption process. For experimental purposes, here we have selected a greyscale image of moon surface from SIPI database. The detailed step-by-step image encryption algorithm with coset graph is given below:

Step 1: Read image and convert it into pixels. The following are the pixels of grayscale image of moon surface (see Table 5.1).

Table 5.1: Representation of the image pixels based on the size of the image

0	**1**	**2**	**3**	**4**	**5**	**6**	**…**	**…**	**250**	**251**	**252**	**253**	**254**	**255**
1	144	160	144	146	153	155	**…**	**…**	58	73	69	73	71	76
2	144	160	144	146	153	155	**…**	**…**	58	73	69	73	71	76
3	142	151	144	146	153	151	**…**	**…**	69	69	67	67	66	78
4	160	158	148	144	140	129	**…**	**…**	75	69	66	73	69	84
5	162	148	140	155	138	144	**…**	**…**	80	73	66	64	76	71
6	164	168	155	148	148	155	**…**	**…**	69	62	64	55	73	80
7	164	162	157	158	148	155	**…**	**…**	75	56	44	42	58	84
8	162	149	160	158	149	144	**…**	**…**	86	104	88	49	69	78
9	155	149	146	146	155	153	**…**	**…**	86	144	155	70	64	86
10	153	155	144	149	138	153	**…**	**…**	84	177	175	114	75	111
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .		. . .	. . .	. . .	. . .	. . .	. . .
246	135	127	148	137	118	127	**…**	**…**	135	148	146	144	151	142
247	131	124	126	129	124	127	**…**	**…**	140	138	146	137	151	140
248	140	124	131	129	126	129	**…**	**…**	144	142	140	142	142	142
249	133	131	124	133	126	133	**…**	**…**	138	140	129	144	149	144
250	137	131	131	118	131	126	**…**	**…**	142	148	127	142	142	146
251	131	117	133	133	124	120	**…**	**…**	138	148	135	149	133	146
252	133	122	126	127	126	118	**…**	**…**	146	140	131	144	142	146
253	129	127	133	126	127	129	**…**	**…**	142	140	137	131	146	135
254	111	127	127	124	133	129	**…**	**…**	138	148	148	137	146	142
255	133	131	133	127	129	129	**…**	**…**	151	138	142	138	149	149

Step 2: Compute the algebraic structure for the field extension, that is, extension of real numbers to complex numbers using following mathematical equation:

$$z = a + b\acute{\imath} \qquad (4.1)$$

In our case, complex numbers don't have imaginary part or it is equivalent to zero. So, $'z'$ is the same as real number $'a'$ and the mapping is redefined as

$$z \rightarrow a \qquad (4.2)$$

Table 5.2: Field extension for a specific image

0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**…**	**248**	**249**	**250**	**251**	**252**	**253**	**254**	**255**
1	144	160	144	146	153	155	149	151	**…**	56	62	58	73	69	73	71	76
2	144	160	144	146	153	155	149	151	**…**	56	62	58	73	69	73	71	76
3	142	151	144	146	153	151	148	148	**…**	73	76	69	69	67	67	66	78
4	160	158	148	144	140	129	140	153	**…**	73	82	75	69	66	73	69	84
5	162	148	140	155	138	144	132	155	**…**	76	69	80	73	66	64	76	71
6	164	168	155	148	148	155	155	158	**…**	89	66	69	62	64	55	73	80
7	164	162	157	158	148	155	149	146	**…**	67	64	75	56	44	42	58	84
8	162	149	160	158	149	144	142	144	**…**	56	55	86	104	88	49	69	78
9	155	149	146	146	155	153	151	160	**…**	42	57	86	144	155	70	64	86
10	153	155	144	149	138	153	157	149		18	46	84	177	175	114	75	111
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .
246	135	127	148	137	118	127	131	124	**…**	140	146	135	148	146	144	151	142
247	131	124	126	129	124	127	129	122	**…**	150	148	140	138	146	137	151	140
248	140	124	131	129	126	129	131	122	**…**	155	146	144	142	140	142	142	142
249	133	131	124	133	126	133	126	123	**…**	144	148	138	140	129	144	149	144
250	137	131	131	118	131	126	117	115	**…**	144	144	142	148	127	142	142	146
251	131	117	133	133	124	120	109	107	**…**	146	140	138	148	135	149	133	146
252	133	122	126	127	126	118	124	113	**…**	142	142	146	140	131	144	142	146
253	129	127	133	126	127	129	124	126	**…**	144	144	142	140	137	131	146	135
254	111	127	127	124	133	129	131	126	**…**	146	142	138	148	148	137	146	142
255	133	131	133	127	129	129	127	127	**…**	144	149	151	138	142	138	149	149

Step 3: Our chosen Field Extension consist of $256 \times 256 \rightarrow 65536$ elements and significant number of elements are repeated. In order to proceed further, we need to find out unique value from Table 5.2. Table 5.3 contains distinct values that are extracted from Table 5.2.

Table 5.3: Distinct elements as vertices for coset graph

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

Step 4: The Table 5.3 contains 249 distinct elements are utilized as vertices in the construction of coset graph. Edges are determined to apply circular shift on the distinct elements/vertices of coset graph. In Table 4.4, we apply one hundred circular shifts on sorted vertices to precisely identify the edges of the coset graph.

Table 5.4: Edges after application of circular shift

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

Step 5: Next, we are required to map pixels of the image to the vertices of the coset graph and assign a unique identifier to each pixel. For the unique identification of pixels, the proposed algorithm is used to calculate channels (the image is either grayscale or RGB) and the total number of rows and columns. For a grayscale image, the channel value is 1, while for an RGB image, the channel value is 3. In our scenario, the number of rows and columns is 256, and the channel is 1. In order to find the mapped vertices, the matrix of the field extension is updated using the vertices of coset graph elements through row-wise mapping. If the length of the vertices is not equal to 256, missing numbers are added to complete them. Row mapping involves performing XOR operations between the rows of the field extension and the vertices of the coset. This process updates all rows of the extension field after each XOR operation. The mapping continues until all rows of the field extension are scrambled. When the pixels are mapped to the vertices of a coset graph, encryption keys are generated using a logistical chaotic map to transform the pixels of an image. The map shows chaotic behavior, which means that small changes in its initial conditions may lead to significant variations in its output. This property is suitable for producing unpredictable encryption keys for unpredictable purposes. In our proposed encryption scheme, this map is used in combination with field extensions to

increase the security of the encrypted image. The chaotic nature of this map ensures that the encrypted picture shows a high sensitivity to the encryption key. It's challenging for the attacker to decrypt the image if they don't know the exact key used to decrypt it. By utilizing this map, we achieve a high level of confusion and diffusion, thereby ensuring the confidentiality and integrity of the encrypted image. One of its important parameters, that is, sequence length, is calculated as follows:

$$sequenceLength = row \times columns \qquad (4.3)$$

By adjusting other parameters as well. Total 65536 key sequences are generated. The problem is that key sequences are in form of vector. In order to arrange the values in form of matrix, these values are reshaped into 256×256 matrix.

Table 5.5: Key Sequences generated from Logistic Map

0	**1**	**2**	**3**	**4**	**5**	**6**	**…**	**251**	**252**	**253**	**254**	**255**
1	3	23484	43975	23950	32802	62554	**…**	35287	51165	44313	27283	48421
2	25203	34840	48406	54729	22285	30967	**…**	3746	28649	25943	6281	18742
3	6796	19336	37409	20196	13837	26590	**…**	16121	46736	57094	55319	31315
4	54983	48166	39860	58337	12502	14146	**…**	53338	44813	65461	38232	63652
5	17592	14863	2451	17575	60892	32491	**…**	24992	15701	46153	1376	17810
6	12818	23524	3319	42104	33361	31350	**…**	60024	36296	56706	53681	58361
7	35601	48346	49488	60408	3042	23857	**…**	28535	51842	1775	38248	13782
8	20569	58855	49555	56033	64197	57284	**…**	38787	53133	42635	55499	11741
9	55413	51058	18154	48630	8672	54706	**…**	3777	61713	30508	11880	40737
10	33832	10220	13299	18865	44703	5010		53246	63873	43313	33662	17988
. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	. . .	
246	35385	39786	2927	46992	15365	47182	**…**	40075	5838	12582	22168	27807
247	17989	33663	43314	63874	53247	24049	**…**	44702	18864	13298	10219	33831
248	40738	11881	30509	61714	3778	35051	**…**	8671	48629	18153	51057	55412
249	11742	55500	42636	53134	38788	2159	**…**	64196	56032	49554	58854	20568
250	13783	38249	1776	51843	28536	42727	**…**	3041	60407	49487	48345	35600
251	58362	53682	56707	36297	60025	38500	**…**	33360	42103	3318	23523	12817
252	17811	1377	46154	15702	24993	45390	**…**	60891	17574	2450	14862	17591
253	63653	38233	65462	44814	53339	18644	**…**	12501	58336	39859	48165	54982
254	31316	55320	57095	46737	16122	41357	**…**	13836	20195	37408	19335	6795
255	18743	6282	25944	28650	3747	48473	**…**	22284	54728	48405	34839	25202

Step 6: Additionally, perform the rotation operations on the edges of coset graph to find out rotated edges. Afterward, the values are adjusted in the range of 0 to 255 because the values

generated from logistic map are greater than 256. To overcome such limitation, a modulus method is utilized that have the advantage of mapping these values with pixels. To fully encrypt an image, mapped vertices, key sequences, and rotated edges are utilized in the following order.

- Adds 'mappedVertices' to a product of 'keySequence' and 'rotatedEdges' (element multiplication)

  The following is the Table 5.6, which consists of encrypted pixel values.

Table 5.6: Pixels of encrypted image

0	**1**	**2**	**3**	**4**	**5**	**6**	**…**	**…**	**250**	**251**	**252**	**253**	**254**	**255**
1	88	42	194	246	99	147	**…**	**…**	142	49	239	147	205	134
2	188	230	232	38	83	21	**…**	**…**	164	231	121	137	159	142
3	200	129	176	154	29	221	**…**	**…**	7	227	245	229	28	198
4	144	226	178	20	186	237	**…**	**…**	239	93	140	51	155	80
5	28	122	138	5	154	62	**…**	**…**	152	139	64	208	224	201
6	228	220	117	40	76	205	**…**	**…**	171	114	122	43	111	8
7	112	120	131	42	114	241	**…**	**…**	23	236	160	242	12	70
8	124	189	50	42	55	176	**…**	**…**	220	80	22	29	171	246
9	29	233	188	136	111	141	**…**	**…**	236	140	179	4	54	162
10	39	215	146	169	182	133	**…**	**…**	188	85	129	188	51	85
. **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**		**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**	**.** **.** **.**
246	7	1	120	239	174	129	**…**	**…**	217	44	18	248	63	130
247	105	12	208	51	18	175	**…**	**…**	230	196	238	31	87	116
248	206	124	9	211	0	161	**…**	**…**	28	150	126	134	34	206
249	17	233	222	147	204	229	**…**	**…**	76	208	115	220	209	194
250	213	67	17	74	81	126	**…**	**…**	44	178	121	206	46	62
251	159	163	175	29	88	90	**…**	**…**	158	16	87	249	209	114
252	27	106	2	99	48	180	**…**	**…**	106	38	109	26	62	232
253	147	237	193	202	183	215	**…**	**…**	64	118	247	15	226	45
254	75	113	89	74	189	133	**…**	**…**	106	180	142	77	68	38
255	89	163	105	195	3	111	**…**	**…**	245	186	94	40	133	195

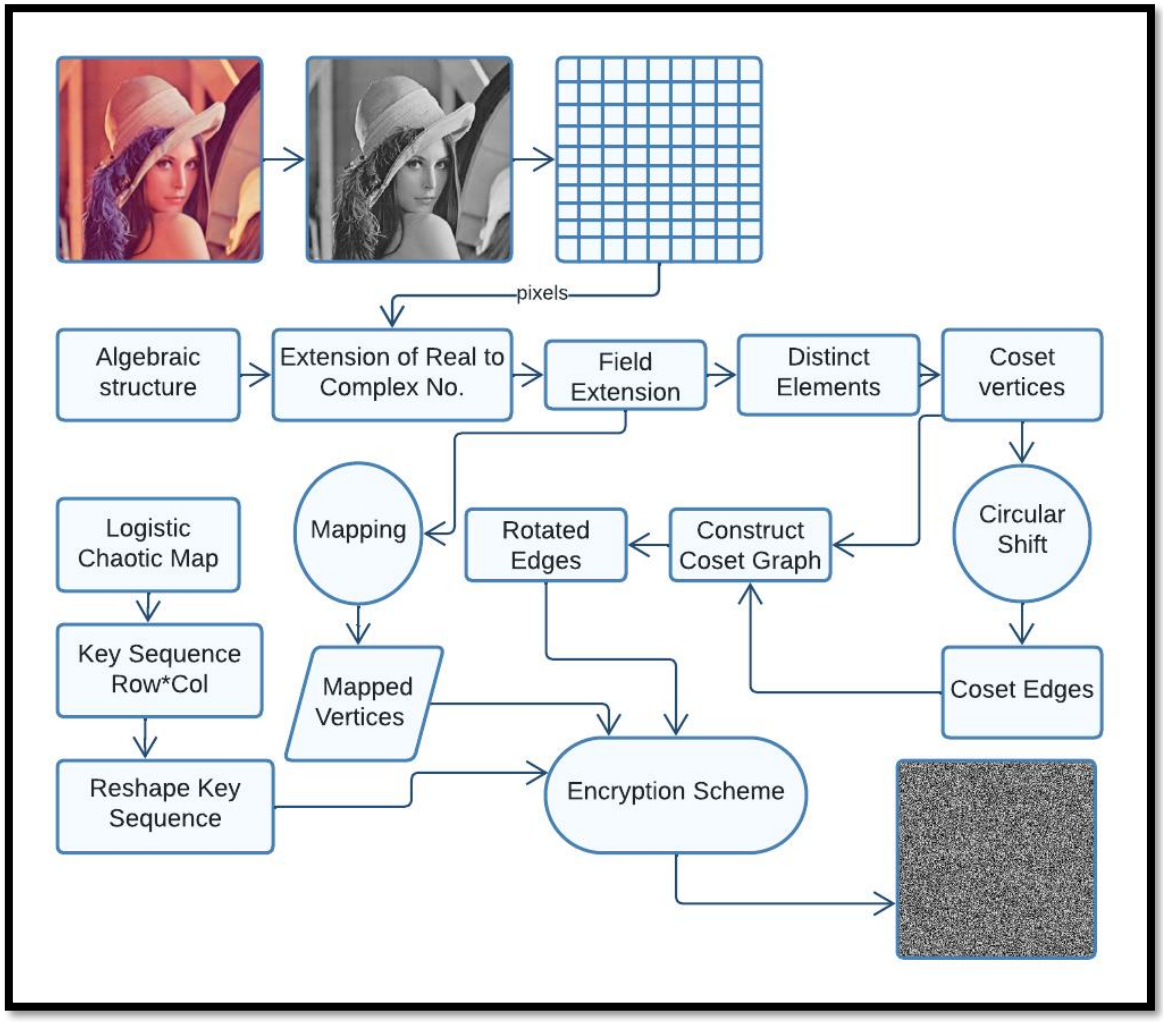


Figure 5.1: Proposed image encryption scheme

5.3.1 Image Decryption Algorithm

The image is decrypted by applying the following inverse operations of the encryption algorithm:

1. Create an array ‘decryptedVertices’ equal to the size of'mappedVertices' and initially fill it with zeros.
2. Retrieve the 2D array from ‘encryptedVertices’
3. Each element of the ‘keySequence’ that is generated from the logistic chaotic map is subtracted from the corresponding element of 'encryptedVertices', and the output is multiplied by 'roratedEdges'.
4. To ensure that output remains within range, perform the'modulus' operation for the

result of the subtraction and multiplication operations.

5. Assign the output of Step 4 to the array 'decryptedVertices', which is defined in Step 1.
6. The array ‘decryptedVertices’ is required to be reshaped to be equal to the size of another 2D array, that is, 'FieldExtension', using the MATLAB reshape function with two arguments.
7. The result of Step 6 is assigned to the ‘DecryptedImage’ array to get the original image.

5.4 Security Analysis

In order to assess the strength of the proposed encryption scheme, we conducted an image encryption experiments on the 'moon surface' image with dimensions 256 by 256 and examine the encrypted image using standard analysis techniques [221][222][223] like Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Normalized Cross-Correlation(NCC), Absolute Difference (AD), Structural Content (SC), Maximum Difference (MD), Normalized Absolute Error (NAE), Root Mean Squared Error (RMSE), Mutual Information (MI), and Structural Similarity (SSIM).

5.4.1 Normalized Cross-Correlation

The Normalized Cross-Correlation (NCC) metric is frequently employed in the fields of image processing as a means to quantify the degree of similarity between two images. The evaluation assesses the degree of correspondence between a template pattern and a reference pattern inside an image. The correlation function may be utilized to assess the degree of similarity between digital images [223]. The normalized cross-correlation quantifies the degree of similarity between the ciphered picture E(x, y) and the original image P(x, y), which have dimensions $M \times N$. In the below figure (see Fig. 5.2), red ‘x’ indicate the location of the peak in the cross-correlation. If the peak is in the center, it represents high similarity between plain and ciphered image. Whereas, if the peak is off-center, it suggests images don’t have resemblance.

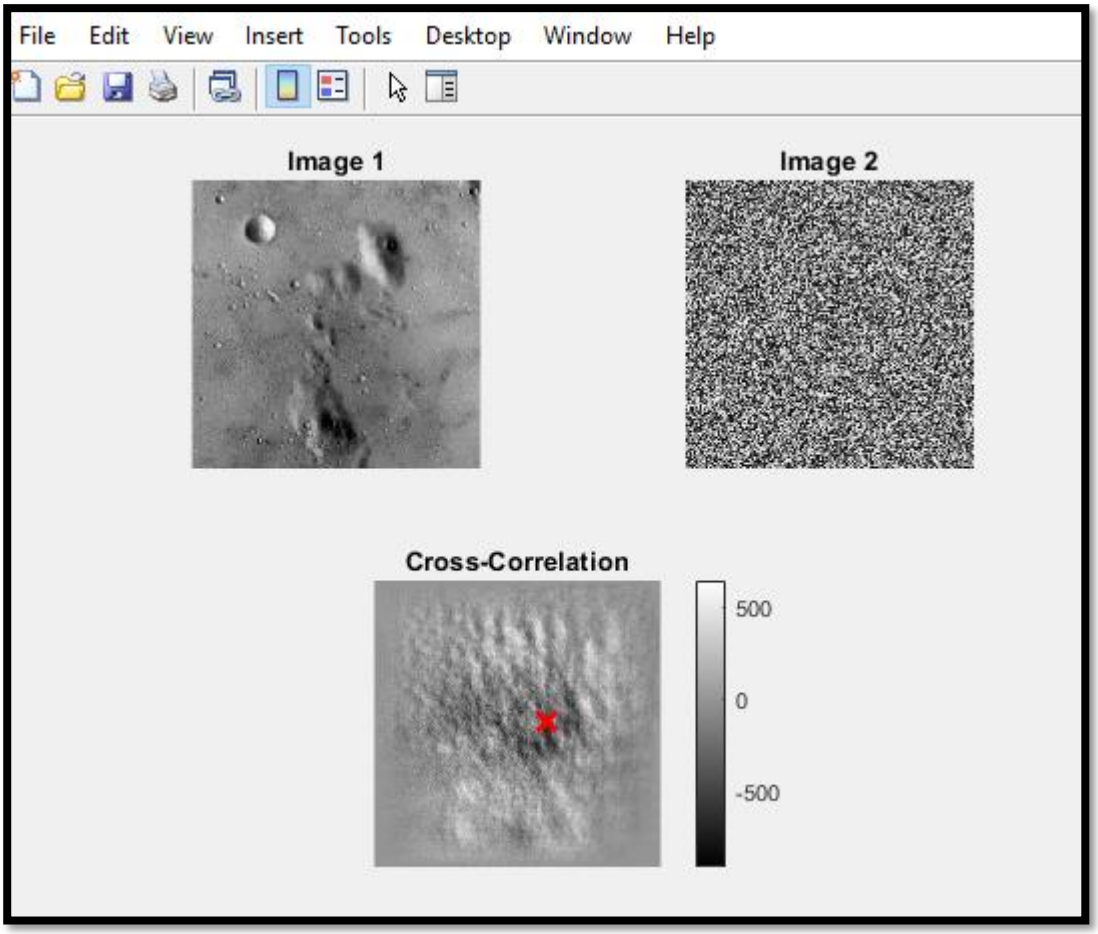


Figure 5.2: Normalized ross-correlation

5.4.2 Maximum difference

Maximum difference (MD) represents the maximum level of inaccuracy. In essence, it provides the distinction between the encrypted image E(x, y) and the original image P(x, y), both of which have dimensions $M \times N$.

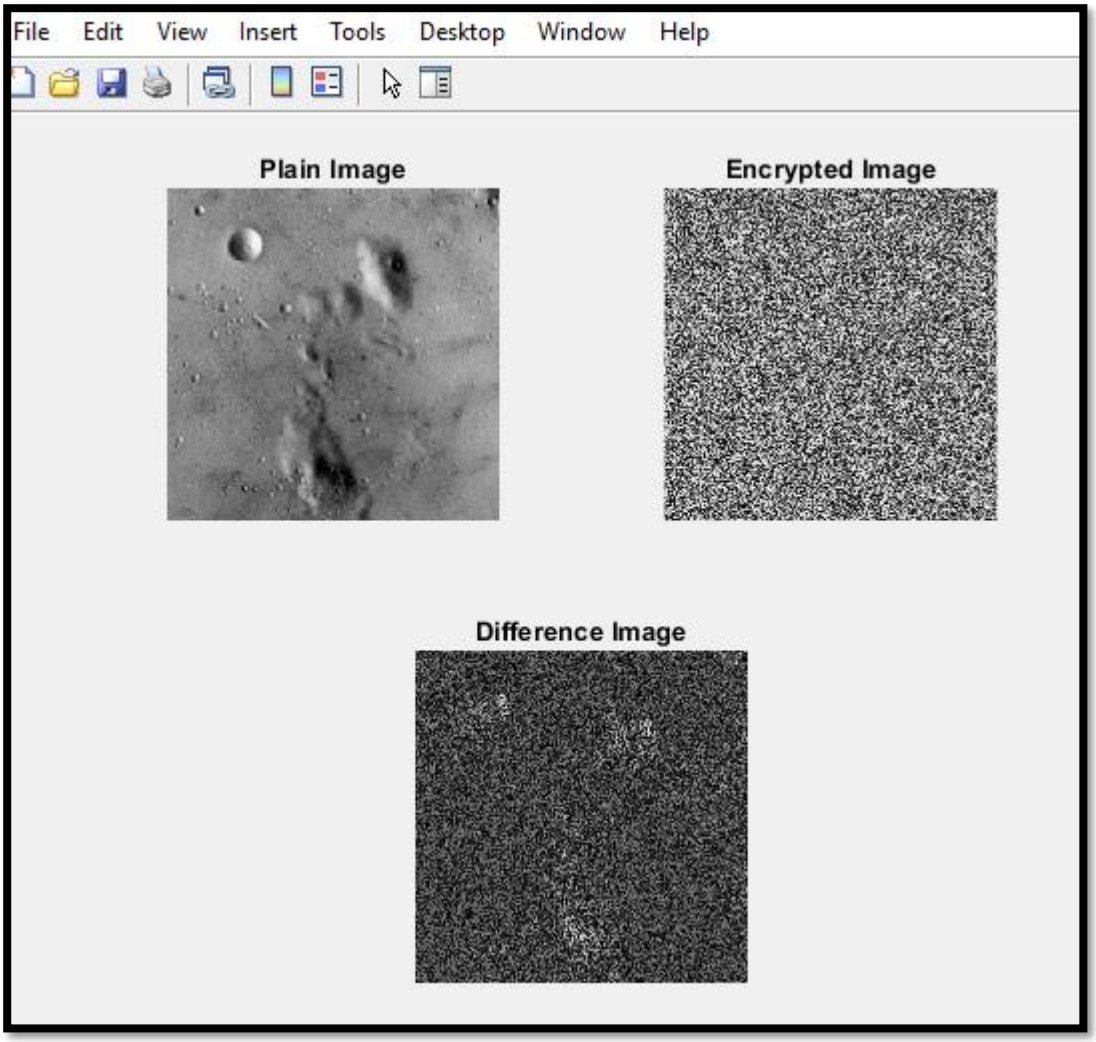


Figure 5.3: Representation of maximum difference

5.4.3 Root Mean Square Error

The root mean square error (RMSE) is a commonly employed metric in the fields of statistics and signal processing for assessing the average magnitude of discrepancies between expected and observed values. The root mean square error (RMSE) is a mathematical measure that estimates the square root of the average of the squared discrepancies between similar values. The value being referred to is the square root of the average of the squares of all mistakes. This technique is commonly employed to provide a very effective and versatile error metric suitable for statistical evaluations.

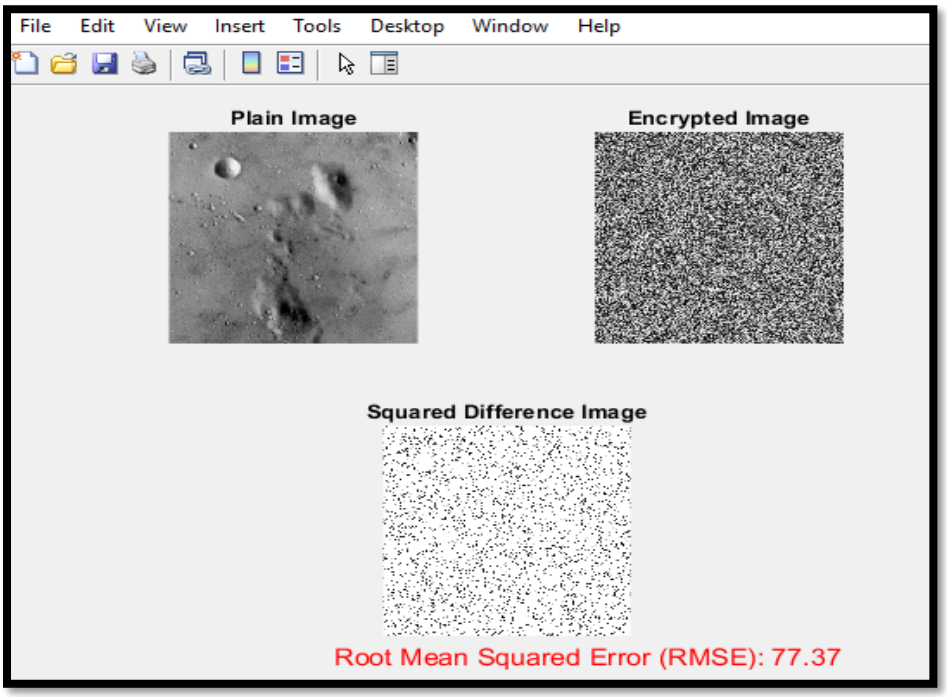


Figure 5.4: Root mean square error representation

5.4.4 The Mean Square Error (MSE)

MSE is a commonly employed measure in the domain of image processing for assessing the average squared discrepancy between the initial and encrypted image. The evaluation of the average number of errors across all data points gives a metric for assessing the overall correctness or fidelity of a reconstruction technique. A smaller mean squared error (MSE) number signifies a higher degree of similarity between the original and reconstructed signals. The process may be described as a standard calculation of the squared difference between ae reference image and an encrypted image.

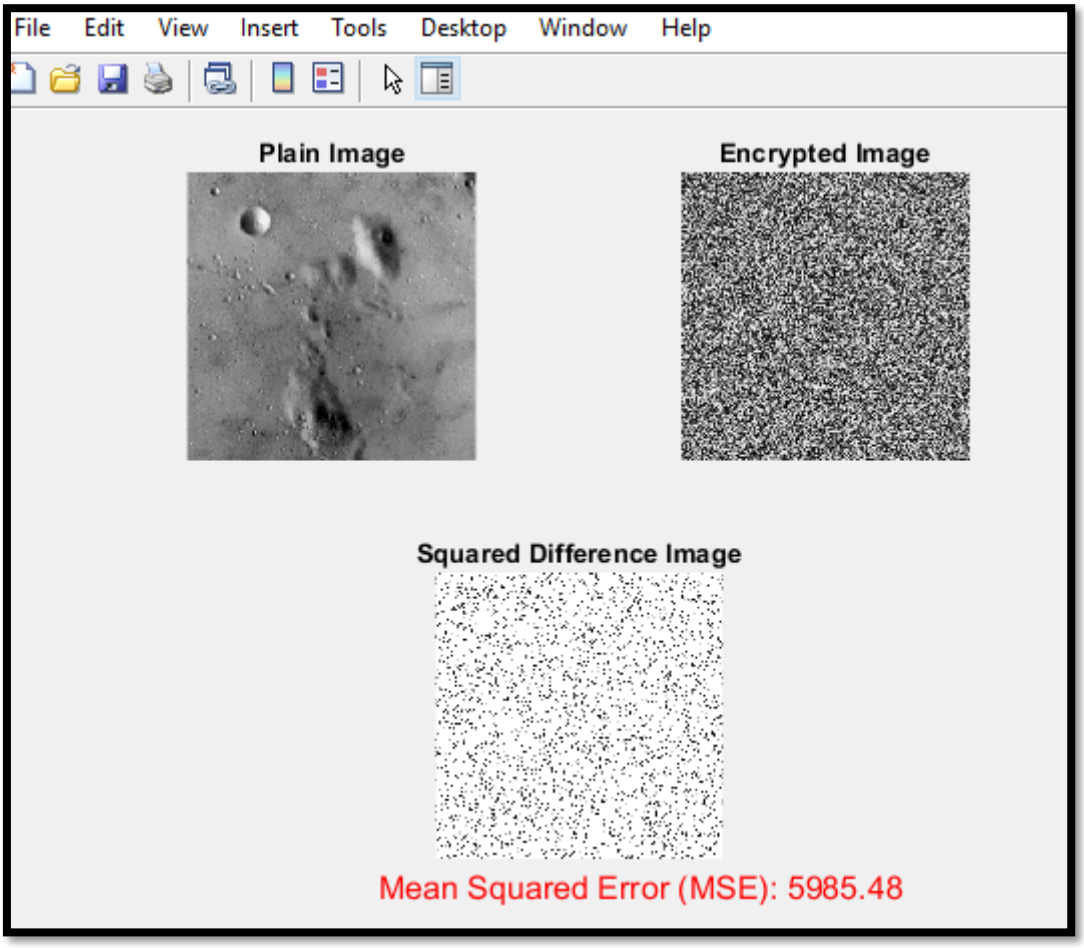


Figure 5.5: Mean square error representation

5.4.5 Average Difference

The metric known as AD is employed to quantitatively measure the average disparity or distinction between two sets of images. The AD method may be utilized to evaluate the disparity between two images or signals by computing the mean magnitude of discrepancies among matching pixels. The calculation involves determining the average variance between an encrypted picture E(x, y) and a plain image P(x, y), both of which have dimensions M * N.

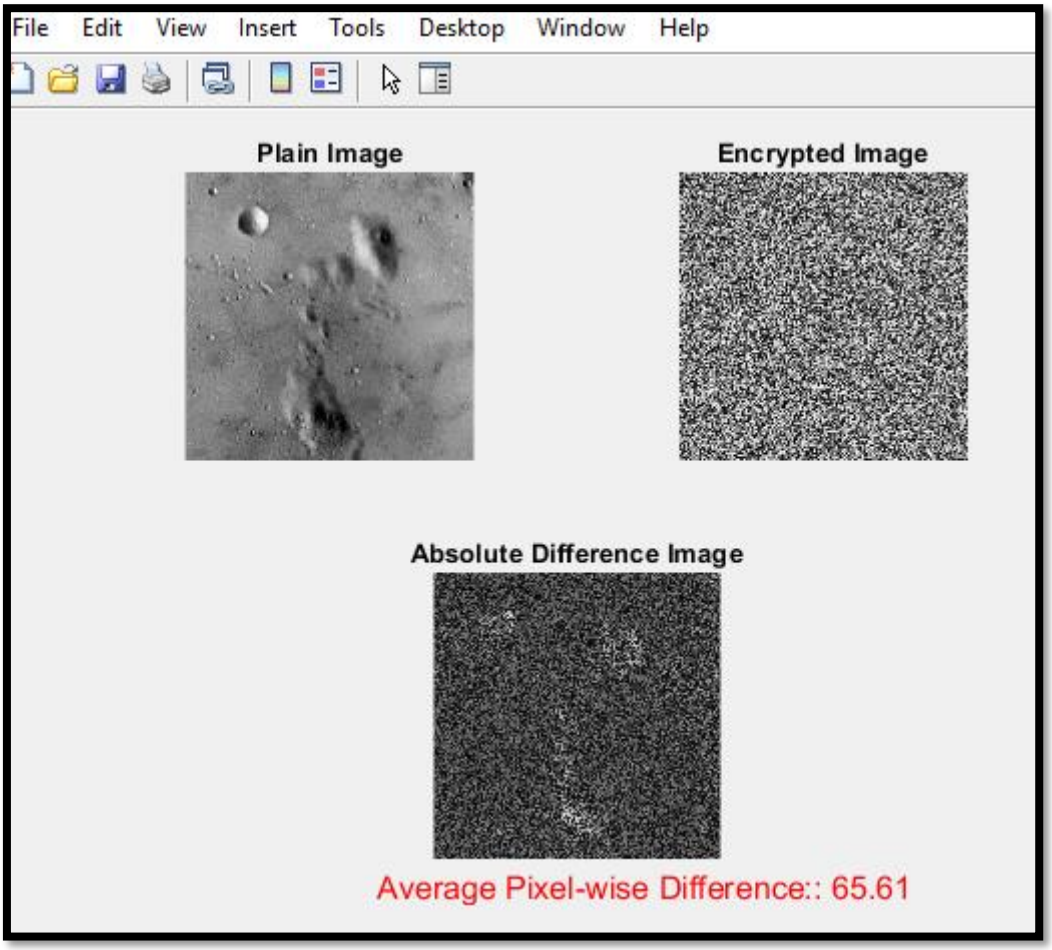


Figure 5.6: average pixel wise difference

5.4.6 Normalized Absolute Error (NAE)

The NAE is a statistical measure employed to evaluate the precision of forecasts or estimations in relation to their true value. The metric quantifies the absolute discrepancy between expected and observed values, normalized in relation to the range of the observed values. The relationship between the ciphered image E(x, y) and the original image P(x, y), both of dimensions M × N, is expressed by the mathematical expression:

$$NAE = \frac{\sum_{y=1}^{M}\sum_{x=1}^{N}|P(x,y)-E(x,y)|}{\sum_{y=1}^{M}\sum_{x=1}^{N}|P(x,y)|} \qquad (4.4)$$

The following is the average normalized absolute error for plain and encrypted images of moon surface:

Average Normalized Absolute Error: 0.263479

5.4.7 Mutual Information

The calculation of mutual information is derived from the entropy of the individual variables as well as their combined entropy. A higher mutual information (MI) value signifies a stronger level of interdependence between the variables. The quantification of evidence obtained from an encrypted image in relation to a plain image may be measured using the MI metric, which is applicable to a pair of images.

The coordinates E(x, y) and P(x, y) may be represented as, where p(x, y) denotes the joint probability function of plain image and encrypted image. Additionally, p(x) and p(y) represent the marginal probability distribution functions of P and E, respectively. The following is the mutual information value for plain and encrypted image of moon surface:

Mutual Information: 519584.999628

5.4.8 Structural Content

The role of structural content is of great importance in the protection and preservation of visual information. The process of image encryption encompasses the deliberate arrangement and concealment of the inherent patterns, forms, and characteristics present within an image, with the aim of bolstering its resilience against unauthorized intrusion. The measure being referred to is a connection-based metric used to assess the similarity between an encrypted image E(x, y) and a plain image P(x, y), both of which have dimensions $M \times N$.

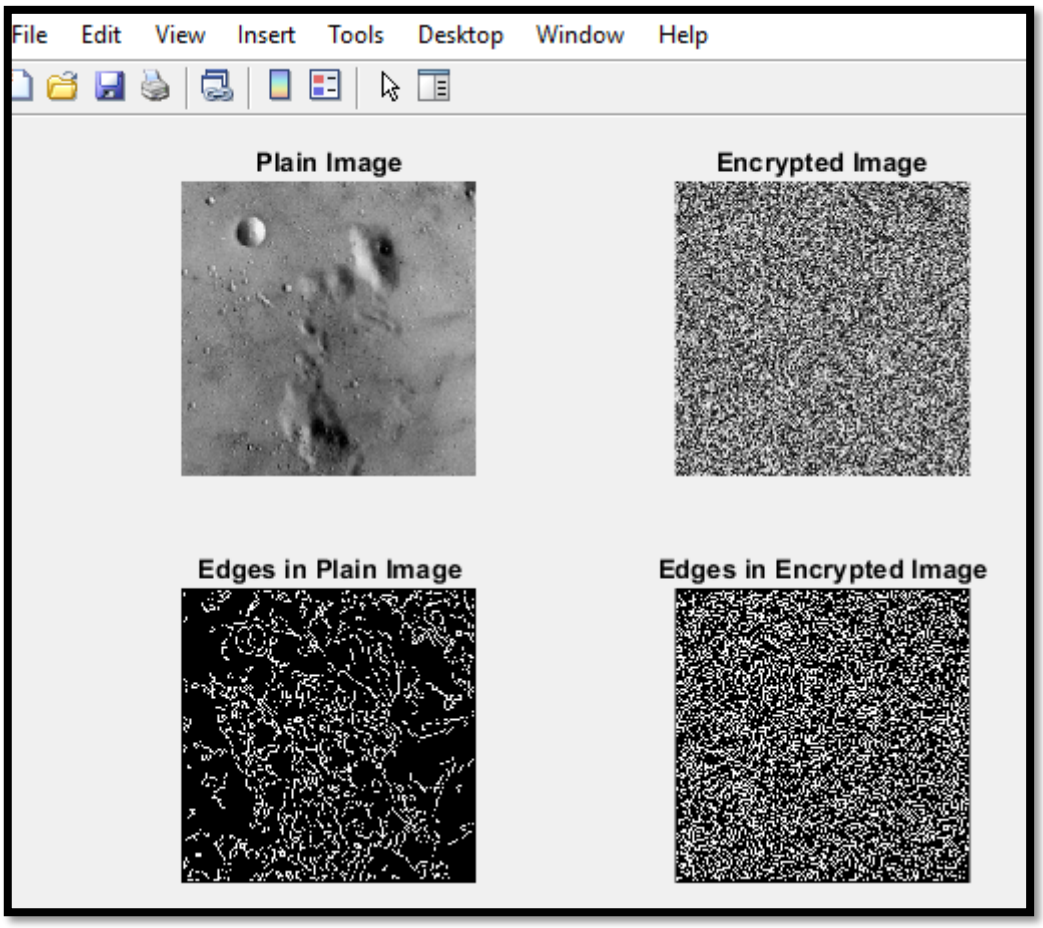


Figure 5.7: structural content for plain and encrypted images

5.4.9 Structural Similarity

The structural similarity (SS) measure is extensively employed in the field of image processing for the purpose of evaluating the perceived quality of images. This measure yields a numerical value ranging from -1 to 1, with a score of 1 indicating complete similarity. The SS has demonstrated its use in several applications, such as image reduction, restoration, and quality assessment. It offers a more comprehensive and perceptually significant evaluation of image fidelity.

The following is the structural similarity value for plain and encrypted image of moon surface:

Structural Similarity Index: 0.0348

5.4.10 Peak Signal to Noise Ratio

The peak signal-to-noise ratio (PSNR) is a metric used to assess the fidelity of an encrypted or compressed image. It quantifies the relationship between the maximum potential pixel intensity and the average squared error between the original image and its rebuilt counterpart. A greater PSNR value is indicative of a reduced degree of distortion. The purpose of this technique is to assess the deterioration of the embedded image in relation to the host image. The following is the signal to noise ratio for plain image of moon surface and corresponding encrypted image:

Peak Signal-to-Noise Ratio (PSNR): 10.15 dB

Table 5.7: Security analysis for grayscale images

Images	PSNR	SSIM	MSE	RMSE	NCC	AD	SC	MD	NAE	MI
Moon surface	10.15	0.0048	5985	77.37	0.15	88.61	0.1483	246	0.2635	0.2790
Parrots	9.16	0.0050	7883	88.79	0.20	87.47	0.1823	247	0.2881	0.1294
Lena	9.02	0.0094	6985	83.58	0.11	91.97	0.0862	255	0.2923	0.2919
Pepper	9.28	0.0086	7418	86.13	0.29	89.73	0.0156	241	0.3023	0.1252
Baboon	9.19	0.0027	5994	77.42	0.33	91.09	0.0610	239	0.2874	0.1365
House	9.04	0.0027	7123	84.40	0.32	89.81	0.0627	245	0.2904	0.3480
Fruits	9.22	0.0129	6752	82.17	0.27	91.47	0.1957	232	0.3026	0.2669

5.5 Differential Analysis

Table 5.8 presents an analysis of the post-effects of different plain images by employing the prescribed methodology. The results indicate that the proposed method for image encryption has resulted in increased NPCR and appropriate UACI values. Higher values of NPCR have been shown to suggest a greater degree of randomization in the positioning of each pixel. Furthermore, the proposed encoding algorithm ensures that the UACI values for each level of the hazy pixel are appropriately calibrated. Therefore, based on the results, it can be readily noticed that the proposed cryptosystem exhibits a high level of resistance against the selected and known plaintext attacks.

Table 5.8: Differential analysis for moon surface, parrots, baboon, pepper, and Lena images

Images	**NPCR**	**UACI**	**BACI**
Moon Surface	99.6629	33.3489	27.4830
Parrots	99.5604	33.4279	24.2892
Baboon	99.6556	33.4309	27.2261
Pepper	99.6494	33.3942	26.2554
Lena	99.6460	33.4971	26.8592
Ref [224] **(for Lena)**	99.6063	33.4579	26.7713
Ref [225] **(for Lena)**	99.6369	33.4335	26.8290
Ref [226] **(for Lena)**	99.6000	33.5700	26.5702
Ref [227] **(for Lena)**	99.6236	33.4898	26.7844

5.6 Summary

This chapter presents a novel image encryption approach that utilizes a coset graph and field extension. The initial step involves the establishment of an algebraic structure, specifically an extension of the real number system to encompass complex numbers. Following this, the aforementioned structure is utilized in the construction of a graph. The graph is formed by utilizing complex numbers as the vertices. In order to get the appropriate number of edges, the vertices undergo a circular shift. The vertices are subsequently assigned to individual image pixels; each being assigned a distinct identifier. The last stage entails the utilization of this distinct mapping for the encryption of images.

CHAPTER 6

EFFICIENT IMAGE ENCRYPTION SCHEME WITH ELLIPTIC CURVE CRYPTGRAPHY

6.1 Overview

In this chapter, we propose an innovative image encryption scheme by utilizing elliptic curve cryptography and a 4D fractional order chaotic map. The process involves taking advantage of the inherent unpredictability and sensitivity to initial conditions displayed by chaotic maps in four dimensions. We aim to enhance the robustness and security of the resulting image encryption scheme by linking this chaotic behavior with the mathematical intricacies of elliptic curves. The combination of chaotic dynamics and elliptic curve cryptography not only introduces a new level of complexity to the proposed scheme but also utilizes the distinct characteristics offered by both techniques.

6.2 Introduction

The propagation of electronic data transmission has heightened the need for robust encryption technologies. Encryption techniques use a strategy of obscuring data using complex mathematical algorithms, rendering it intelligible to those with the requisite decryption key. To ensure the privacy, integrity, and authenticity of data sent over networks or stored on devices, it is important to use a robust encryption methodology. A multitude of encryption schemes have been devised with the aim of protecting data and reducing the likelihood of unauthorized access. The safety of a bit-plane extraction and multi-chaos image encryption system was explored by Zhu et al. [228]. They used the conventional "chosen-plaintext" technique to propose a methodology that exhibits robust security and resilience against attacks. Haider et al. [229]

created an image encryption solution that relies on an optimization strategy. The objective function of this method incorporates both entropy and correlation. A novel approach to image encryption, including both confusion and dispersion, was presented by Elkandoz [230]. The proposed approach involves first creating a randomized version of the image through the manipulation of pixel arrangement. Subsequently, the pixels are distributed using XoRing encryption, which requires the use of a confidential key. Wu et al. [231] introduced a novel approach for securing audio data during its transmission via the internet. The approach used in this study involves the utilization of a layered infinite collapse mechanism inside the spatial domain of logistic maps in a two-dimensional setting. In order to guarantee secure communication inside Boolean networks that undergo asynchronous updates, Gao et al. [232] devised an innovative encryption methodology. The method uses ideas from chaos theory and employs asynchronous updates. The researchers made notable progress, creating a new encoding method and a fully parameterized two-dimensional sine map. These functions can transform the network into a Boolean matrix, which can be shared with others as an image. In their study, Xu et al. [233] proposed a method to safeguard three-dimensional image data by manipulating the starting state of a discrete system using the SHA-256 hash algorithm. The use of chaotic sequences, the Arnold matrix, and a DNA diffusion method enabled researchers to proficiently scramble and disperse the coordinate values included inside an image file. Gao et al. [234] discovered a technique for encrypting facial expressions that have been rendered chaotic. The suggested methodology involves the use of a two-dimensional logistic tent modular map and a hash function for the generation of cryptographic keys. Additionally, facial images are retrieved and then encrypted using this technique. Furthermore, Gao et al. [235] introduced a novel encryption technique that was specifically designed for three-dimensional (3D) models. The proposed methodology involves the use of a two-dimensional chaotic system, achieved by the integration of the logistic map with infinite collapse.

Concerns over the privacy and security of electronic communication tools, such as email and messaging applications, have seen a notable surge among users in recent years. In light of the susceptibility of messages to hacking or interception, there has been a recent work to enhance the security measures around them. The text-data-security techniques use a range of transformations, such as wavelet transforms, wavelet transforms based on max-plus algebra, and mathematical structures like elliptic curves. A fundamental aspect [236] of cryptosystems is the inclusion of a mechanism that enables the conversion of plaintext data into encrypted

data, making it difficult to decipher without access to the secret key used during the encryption process. The approach proposed by Sedeeg et al. [237] involves the encryption of plaintext using the Aboodh transform, followed by its decryption using the inverse Aboodh transform. The authors, Mehmood et al. [238], have proposed a unique cryptographic concept that has the potential to significantly enhance information security, particularly in the context of safeguarding sensitive data. The process of encoding and decoding data involves the use of modular arithmetic, using a mathematical approach that has been recently created. This procedure utilizes a modulus of either 26 or 63. Furthermore, the characters' numerical values in the message were subjected to the Sadiq-Emad-Eman (SEE) integral transform as proposed by Mansour et al. [239]. This approach resulted in the derivation of an algebraic equation, which was then used to construct a distinct sequence. In order to establish a symmetric cryptosystem, the use of the SEE integral transform is employed to encode the plaintext, while its corresponding inverse operation is utilized to decode the cypher text and restore it to its original form.

6.3 Background Study

The non-linear nature and high group order of elliptic curves (ECs) contribute to their resilience against a wide range of cryptographic assaults. Consequently, they have been extensively used in the field of cryptography. The extensive use of cryptographic technology may be attributed to the standardisation efforts of the National Institute of Standards and Technology (NIST) [240]. Various cryptographic algorithms have been created using elliptic curves (ECs), including the random number generator [241], [242], the S-box generator [243], [244], image encryption [245], and text encryption [140]. Azhar et al. [246] proposed a text encryption strategy by leveraging the theoretical foundations of the Pell sequence and elliptic curves. The original text undergoes a cyclic permutation of symbols, resulting in its unintelligibility. Furthermore, the Pell sequence, a weight function, and a binary sequence are used to transform the scattered plaintext into real numbers, thereby concealing it from potential adversaries. Moreover, the encoding and transmission of plaintext are further obfuscated by the generation of permutations. Different chaotic maps have been used in the past for encryption techniques and multimedia security. Liu et al. [247] proposed a group of 1D quadratic chaotic maps based on the theory of topological conjugation. This 1D chaotic map is quite different

from traditional chaotic maps. This article [248] covers the effective transfer of a coded color image using a MIMO-OFDM system over a channel affected by Rayleigh fading and additive white Gaussian noise. The performance evaluation metrics of a highly chaotic two-dimensional Logistic-Gaussian map (2D-LGHM) [249] with a wide range of hyperchaos show that it has superior ergodicity and unpredictability. In [250], the confusion phase and the diffusion phase are the two main procedures of the proposed image encryption process.

Chaotic systems are divided into two main groups: (i) 1D chaotic maps defined by a single variable, and (ii) multi-dimensional chaotic maps defined by multiple variables. Although these chaotic maps have produced some promising results, they also have some drawbacks that restrict the range of real-time applications. As shown in studies [250] and [251], 1D chaotic maps have three main disadvantages: (1) a limited or fragmented range; (2) small period orbits; and (3) non-uniform data distribution. To tackle these issues for image encryption, many cryptographers have turned to multi-dimensional chaotic systems, which contain a large number of parameters and complex structures [252]. However, multi-dimensional chaotic systems require considerable computational cost and implementation challenges and may result in the emergence of a strange attractor with a non-integer dimension. Azam et al. .[253] proposed an image encryption approach based on coupled map lattices and elliptic curve cryptography with the goal of addressing the limitations of existing cryptosystems. This methodology mainly consists of two levels. In the first level, elliptic curve-based random numbers are generated in order to diffuse the original image. In the second level, substitution is performed to create confusion in the diffused image. In [254], a highly secure cryptosystem system based on bit level and hyper-chaotic permutation is developed. This methodology diffuses the image using a two-dimensional XOR operation. Afterwards, scrambled images are arranged in different directions. Ultimately, two-dimensional XOR diffusion in reverse is used to create the encrypted image. In order to improve overall security, Gavavi et al. [255] combine cryptography and steganography techniques to produce a more secure method for encrypting and hiding the input image within a carrier medium, and high security is attained by utilising elliptic curve cryptography (EEC) with a smaller key size. Gupta et al. [256] presented a very efficient image encryption technique in two levels for safe transmission of data between IoT-enabled devices. At one level, a discrete wavelet transform (DWT) watermarking technique is used, and at another, a logistic chaotic map and crossover image encryption are combined to produce a successful image encryption method. In [257], the

generalized two-dimensional Arnold map, the reality-preserving two-dimensional discrete fractional Hartley transform, and the affine Hill cipher are used to create a novel method for encrypting multiple images in this study. An encryption method based on the sigmoid logistic map, Kronecker xor product, and Hill cypher is presented in [258] for enhancing image encryption.

6.4 Preliminaries

Elliptic Curve Cryptography (ECC) is a type of asymmetric encryption algorithm that makes use of elliptic curves' mathematical structure in combination with finite fields. Various elliptic curves can be used as the basis for ECC cryptographic algorithms. These curves have various key lengths, levels of performance, and potential involvement with various algorithms. An elliptic curve (EC) over a finite field F_p with a prime modulus p can be defined as

$$E(F_p) = \{(x, y) \in F_p^2 | (Y^2 = X^3 + mX + n)(mod\ p)\} \cup \{O\} \qquad (6.1)$$

Where, $X, Y, m, n \in F_p$ and O is a point of infinity.

In other words, an elliptic curve refers to a group of points with symmetrical characteristics that satisfy a certain mathematical equation. The following options can be used to categorized the different ways that an elliptic curve may intersect a line:

Tangent: The line touches the elliptic curve only once, without intersecting the curve at any other point. This point of intersection is known as a tangent point.

Secant: In order to form a secant line, the line must cross the elliptic curve twice at different locations. The secant points are the names for these points of intersection.

No Intersection: The line does not intersect the elliptic curve at any point, so there are no points of intersection.

Moreover, ECC is widely used by websites to secure users' hypertext transfer protocol connections. It is also used in a well-known time-stamping encryption algorithm. It falls under the category of public key (asymmetric key) cryptosystems and provides equal security with a smaller key size as compared to the RSA algorithm. It is symmetric to the x-axis, and if we draw a line, it will touch a maximum of three points. Assuming that the field $\mathbb{F}$ is equivalent to the real number($\mathbb{R} = 13$), $a = 1,\ b = 6, and\ p = 11$ let's consider a curve.

Table 6.1: Finite field for irreducible polynomial

x	$x^3 + x + 6$ mod p
0	6
1	8
2	5
3	3
4	8
5	4
6	8
7	4
8	9
9	7
10	7

y	y^2mod p
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Now, the process begins to find points on an elliptic curve. When $x = 0$, the corresponding value is 6. Start searching in the $y^2 mod\ p$ column, but no value is present that is exactly equal to 6. Therefore, it can be said that$(x = 0, \dots)$ is not a point on the elliptic curve. Next, let's move to x=1. The value is 8, but upon checking the $y^2 mod\ p$ column, we find no value equal to this number. Therefore, it can be said that t $(x = 1, \dots)$ is also not a point on the elliptic curve. For x=2, the calculated value is 5, and in the corresponding targeted column, we find that 5 exists two times at y=4 and y=7. Hence, we can say that the points (2,4) and (2,7) lie on the elliptic curve The process will be continued to find out all the numbers that lie on the elliptic curve. The table (Table 6.2) displays the points that are located on the provided curve.

Table 6.2: Elliptic curve points located on curve

$\boldsymbol{x}$	$\boldsymbol{y^2}$	$\boldsymbol{P(x, y)}$
6	0	-
8	1	-
5	4	$(2,4), (2,7)$
3	9	$(3,5), (3,6)$
8	5	-
4	3	$(5,2), (5,9)$
8	3	-
4	5	$(7,2), (7,9)$
9	9	$(8,3), (8,8)$
7	4	-
7	1	$(10,2), (10,9)$

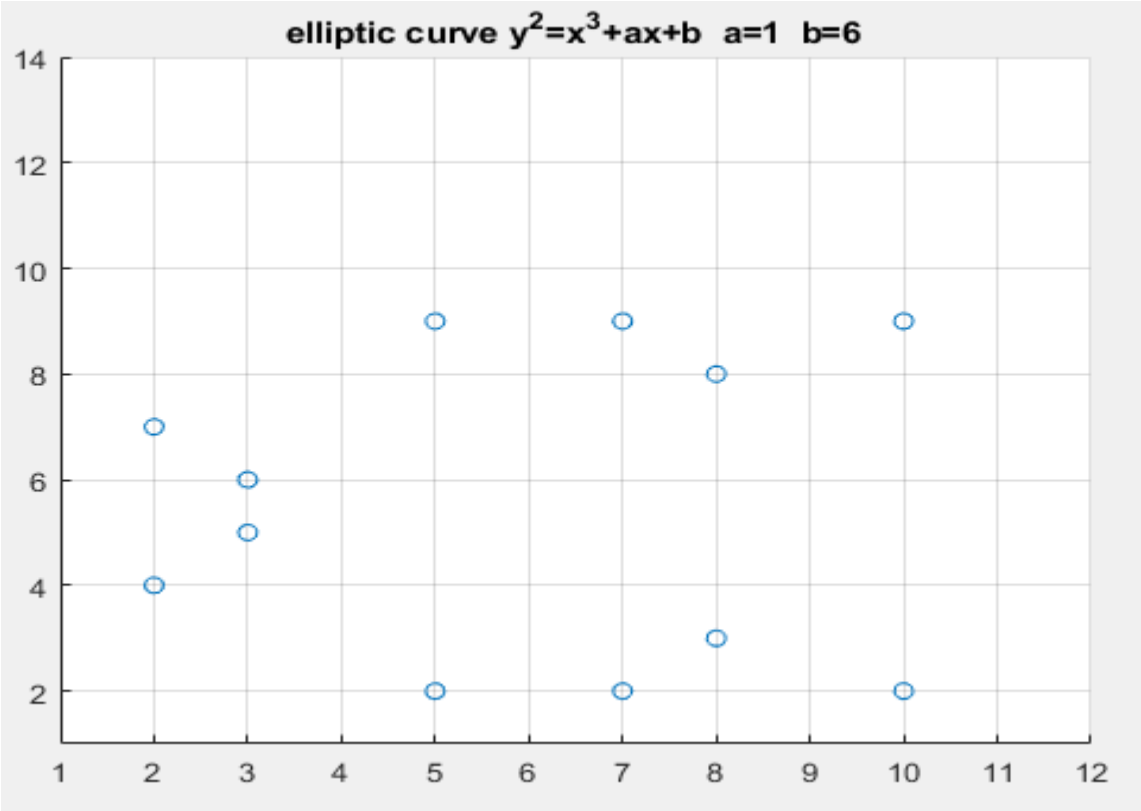


Figure 6.1: Elliptic Curve points $x^3 + x + 6$ over $\mathbb{F}_{11}$

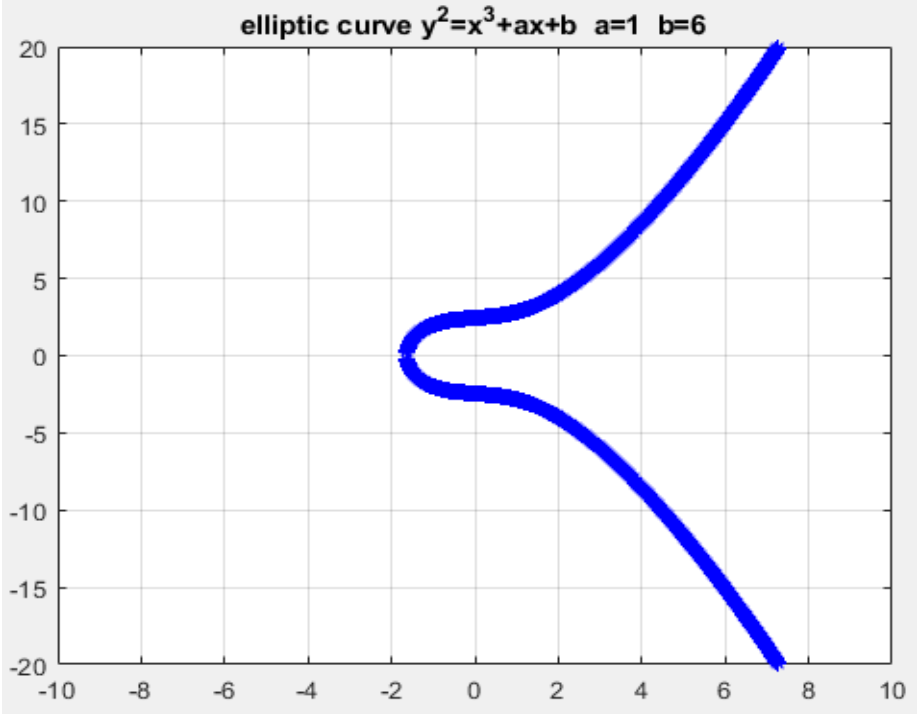


Figure 6.2: Elliptic Curve for $x^3 + x + 6$

6.4.1 Four-Dimensional Fractional Order Hyper Chaotic Map

A 4D hyperchaotic system is a nonlinear dynamic system that exhibits chaotic behaviour in four-dimensional space, meaning that it has at least two positive Lyapunov exponents. Which represents that the system is sensitive to initial conditions and unpredictable behavior. Which means a small change in the initial condition can lead to an entirely different state. In this chaotic system, four dimensions are involved. These dimensions can generate complex and irregular patterns, which can be useful in image encryption, secure communication, and different computations. Due to the large dimensionality of hyperchaotic systems, hyperchaotic theory focuses on 4D hyperchaotic systems. In our proposed image encryption technique, we utilise the following 4D hyperchaotic system, which was proposed by Ishkakova [204].

$$\frac{d^{\alpha}{}_{x}}{dt^{\alpha}} = a.y.z \tag{6.2}$$

$$\frac{d^{\alpha}{}_{y}}{dt^{\alpha}} = bx - xz - cx \tag{6.3}$$

$$\frac{d^{\alpha}{}_{z}}{dt^{\alpha}} = d.x.y - xw \tag{6.4}$$

$$\frac{d^{\alpha}{}_{w}}{dt^{\alpha}} = x - ew + y \tag{6.5}$$

In this work, we investigate some dynamical features and the paramount values for a, b, c, d, and α to get best results regarding image encryption.

6.5 Image Encryption Scheme Based on ECC and 4D Chaotic Map

The symmetric key ciphers face potential security challenges due to key distribution. A novel public key image encryption scheme is presented in this chapter, which is based on elliptic curve cryptography (ECC) and a 4D fractional order chaotic map. Specifically, the elliptic curve is first utilized to discover all elliptic curve points that will serve as the initial values for image encryption with dimensions of rows and columns. Elliptic curve points are selected carefully depending on the desired security, specific criteria, and cryptographic properties. The pixel values of the original image are mapped to the elliptic curve points, and a crossover encrypted the mapped points with the use of a public key using ECC encryption. Furthermore, choose the parameters and initial conditions for the 4D fractional order chaotic map to generate the four dimensions, transform them into one matrix equivalent to the size of the image, and then XOR

the encrypted points with the chaotic map values to perturb the encrypted points. Moreover, the below algorithm is specific to grayscale images, but if the image is RGB, then the same procedure will work for each channel separately (see Fig. 6.3). Here is an algorithm to encrypt an image using elliptic curve points and a 4D fractional-order chaotic map.

Step 1: Define an elliptic curve function E and domain parameters(a, b, p), which are represented as $E_p(a, b)$.

Step 2: Choose an elliptic curve with x or y coordinates, but it is better to choose y coordinates because they have fewer repetitions compared to x coordinates of the same curve equation.

Step 3: Convert the x and y-coordinates values into range of 0 to 255.

Step 4: Restrict the total values of x and y coordinates equal to the size of image. Like, if image size $256 \times 256 = 65536$, then x and y should be restricted till 65536.

Step 5: Select a pair of public and private keys, a public key for encryption and a private key for decryption.

Step 6: Pick the parameters and initial conditions for the 4D fractional-order chaotic map.

Step 7: Convert the image into a matrix of pixel values.

Step 8: Convert the matrix of pixels into a 1D array for easier mathematical operations.

Step 9: The pixel values of the original image are mapped to the elliptic curve y-coordinate points.

Step 10: Encrypt the mapped points with the use of a public key using ECC encryption.

Step 11: Generate the four dimensions (x, y, z, w) of 4D chaotic map and transform them into one matrix equivalent to size of image.

Step 12. XORing the encrypted points with the chaotic map values to perturb the encrypted points.

Here, for calculation, elliptic curve parameters are set to a=4021, b=3123, and p=65871; in order to generate y-coordinate points equivalent or greater than pixel values of original image (see Table 6.3).

Table 6.3: Elliptic curve points for $E_{65871}(4021,3121)$

x	$x^3 + 4021.x + 3123$ Mod p	y	$y^2 Mod\ p$	$P(x,y)$: points making elliptic curve using mod function with 256.
0	3123	0	0	(0,83), (0,170)(0,27), (0,114), (0,24), (0,111)(0,224), (0,55), (0,221), (0,52)(0,165), (0,252)
1	7145	1	1	-
2	11173	2	4	-
3	15213	3	9	-
4	19271	4	16	-
5	23353	5	25	-
6	27465	6	36	-
7	31613	7	49	-
8	35803	8	64	(8,104), (8,255)(8,95), (8,89), (8,246), (8,240)(8,80), (8,231)
9	40041	9	81	(9,241), (9,65)(9,132), (9,212), (9,182), (9,6)(9,73), (9,153), (9,123), (9,203)(9,14), (9,94)
10	44333	10	100	-
11	48685	11	121	-
12	53103	12	144	-
13	57593	13	169	-
14	62161	14	196	-
.	.	.	.	.
	.	.	.	.
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.
65519	47723	65519	58738	.
65520	29287	65520	58033	.
65521	8739	65521	57330	.
65522	51956	65522	56629	.
65523	27202	65523	55930	.
6524	354	6524	55233	.
65525	37289	65525	54538	.
65526	6271	65526	53845	.
65534	13250	65534	48373	.
65535	29635	65535	47698	.
65536	43998	65536	47025	.

The extraction and arrangement of y-coordinates column-wise are equivalent to the size of an image.

Table 6.4: elliptic curve y-coordinate points

	1	**2**	**3**	**4**	**5**	**6**	**…**	**250**	**251**	**252**	**253**	**254**	**255**	**256**
1	83	0	231	88	55	171		153	122	186	13	103	188	249
2	170	141	25	138	247	13		120	220	149	109	35	147	169
3	27	253	251	138	245	66		15	33	22	154	32	81	30
4	114	138	45	188	35	164		55	164	188	249	47	42	213
5	24	197	172	29	44	207		142	233	83	54	44	232	74
6	111	82	222	79	90	56		252	161	58	143	232	144	5
.	.													
.	.													
.	.													
.	.													
.	.						…							
.	.													
.	.													
.	.													
250	146	83	88	165	180	43		213	109	117	221	66	69	88
251	189	113	0	170	155	233		108	155	12	59	59	52	141
252	40	163	50	220	50	240		107	180	181	11	4	115	30
253	85	34	147	56	64	100		2	226	226	105	108	98	180
254	235	84	197	106	199	202		77	197	66	94	103	86	6
256	56	54	197	111	23	248		228	171	217	91	37	157	157

The pixel values of the original image are substituted for the elliptic curve y-coordinate points. After complete substitution, the original image will contain the same pixel values as the elliptic curve y-coordinate. Next, arrange the mapped points into a matrix equivalent to the size of the original image. The following formula is applied to encrypt the elliptic curve points:

$$\text{encrypted points} = \text{mod}(\text{mapped Image}^{\text{public key}}, 256)$$

We employ the following Fractional Order 4D Hyper Chaotic Map, utilizing specific initial conditions and parameters denoted as $a, b, c, d, e, and\ \alpha$. After careful selection, we have determined the values for these parameters and initial condition as follows: $a = 3, b = 2.5, c = 4, d = 6, e = 0.4, and\ \alpha = 0.4$.

$$\frac{d^{\alpha}x}{dt^{\alpha}} = 3.y.z \qquad (6.6)$$

$$\frac{d^{\alpha}y}{dt^{\alpha}} = 2.5 * x - xz - 4 * x \qquad (6.7)$$

$$\frac{d^{\alpha}{}_{z}}{dt^{\alpha}} = 6.x.y - xw \qquad (6.8)$$

$$\frac{d^{\alpha}{}_{w}}{dt^{\alpha}} = x - 0.4 * w + y \qquad (6.9)$$

In order to enhance image encryption security, a classy methodology is being employed to further strengthen the encryption scheme. This involves the chaotic map perturbation of the already encrypted points, thereby presenting an additional layer of security to the encryption process. The utilization of a 4D fractional-order chaotic map in this context is a cautious strategy aimed at enhancing the perturbation of pixels within the encrypted points. The conversion works by mapping each pixel's position in a systematic fashion, introducing a scientific operation that significantly increases the difficulty of decryption without the private key. The strength of the encryption is boosted by this advanced technique, which also aligns with modern encryption schemes. As digital multimedia evolves, the application of sophisticated transformations shows a commitment to staying ahead of potential vulnerabilities and ensuring that encrypted images are resilient to unauthorized access or tampering. The following is the method to perturb the encrypted pixels using a 4D chaotic map.

$$\text{perturbedPixels} = \text{encryptedPoints} + \text{chaoticMap}(\text{length}(\text{encryptePoints})) \quad (5.10)$$

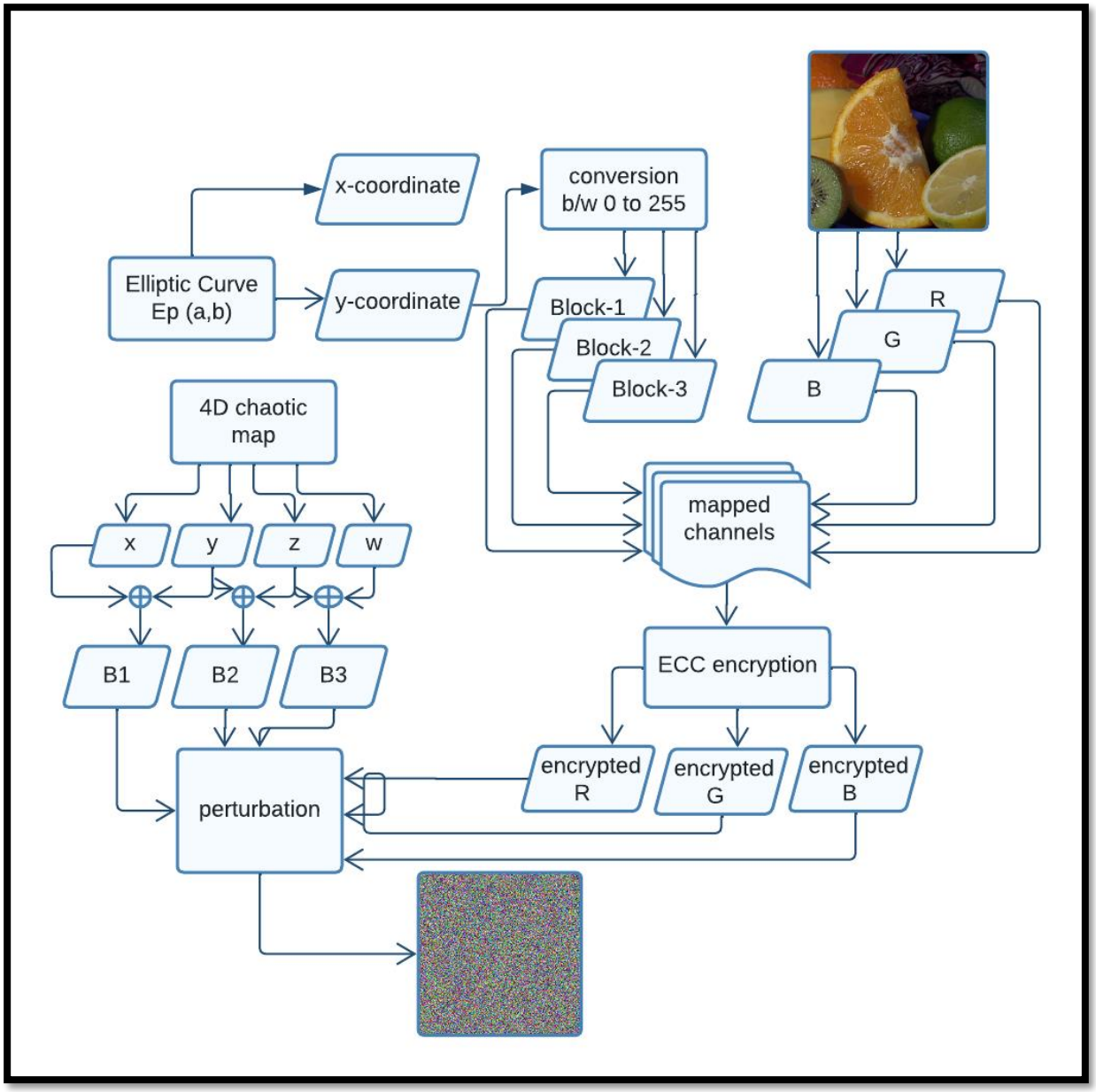


Figure 6.3: Proposed Image Encryption Scheme

6.6 Image Decryption Scheme

Image decryption is playing a key role in the field of secure communication, the process of revealing the concealed content of encrypted images. This procedure involves a decryption algorithm and keys to transform the unintelligible image back into its original form. Overall, our proposed decryption scheme is good enough to maintain a balance between privacy and security in today's digital age. The following is the algorithm to decrypt the image:

Step 1: Execute the inverse of the 4D fractional order chaotic map to reverse the perturbation.

Step 2: Perform the decryption of elliptic curve points using a private key.

Step 3: Map the decrypted points back to reconstruct the matrix of pixels.

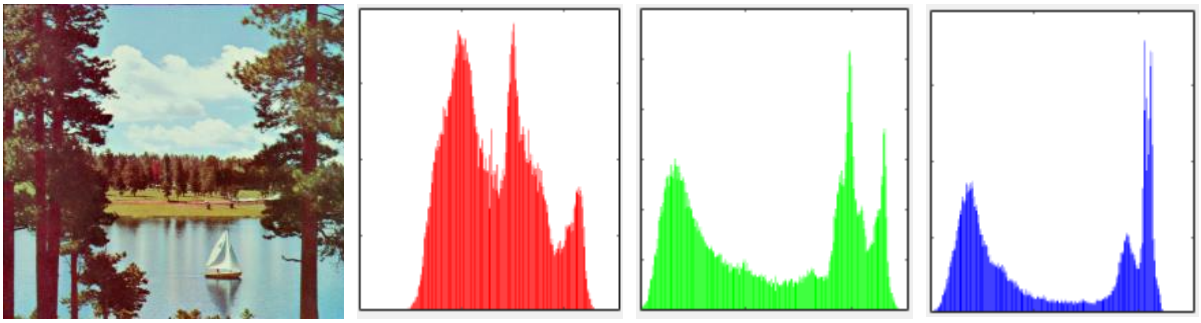
Step 4: Reverse the mapping to reconstruct the original image.

6.7 Security Analysis

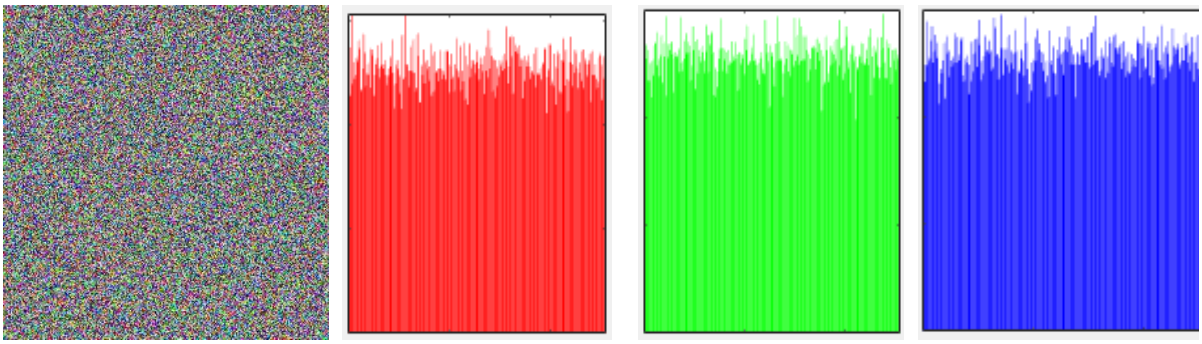
The assessment of security plays a significant role in verifying the efficacy of any encryption technique. This section presents an analysis of the proposed cryptosystem with respect to various security measures.

6.7.1 Histogram Analysis

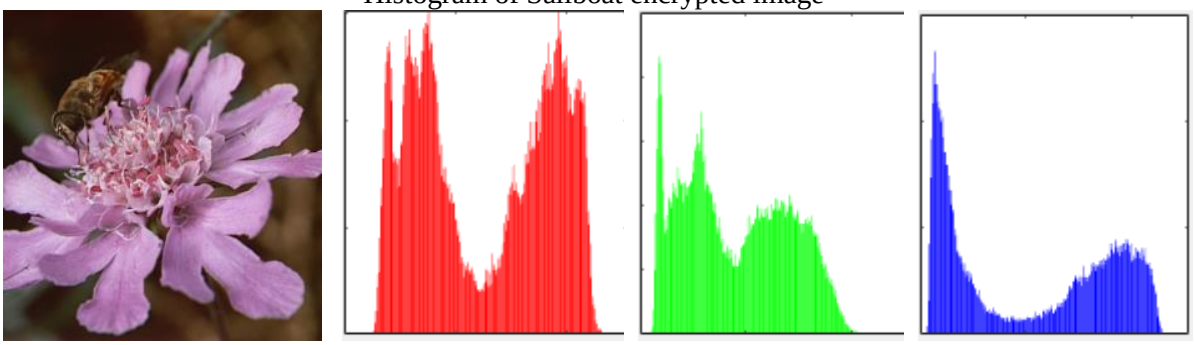
Histogram analysis is a valuable tool in cryptography that examines the distribution of pixel intensities within an original and encrypted image to detect significant changes. It is used to represent the number of pixels with numbers ranging from 0 (black) to 255 (white) in grayscale images. Figure 6.4 clearly exhibits distinct peaks and patterns for plain images. On the other hand, the encrypted images show a distribution of pixel intensities. Additionally, the histogram for encrypted images has appeared random, flat, and uniformly distributed without distinct peaks. Furthermore, the histogram of an encrypted image should ideally be uniform, meaning that each pixel intensity value occurs with roughly the same frequency.



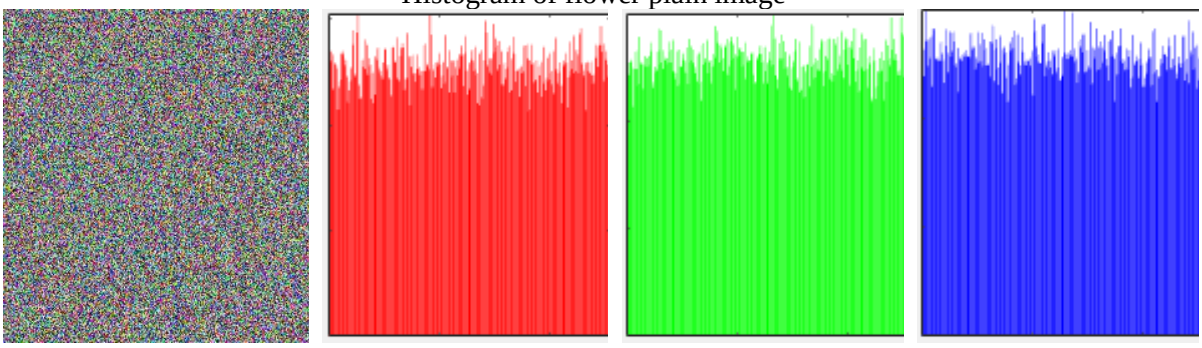
Histogram of plain image (Sailboat)



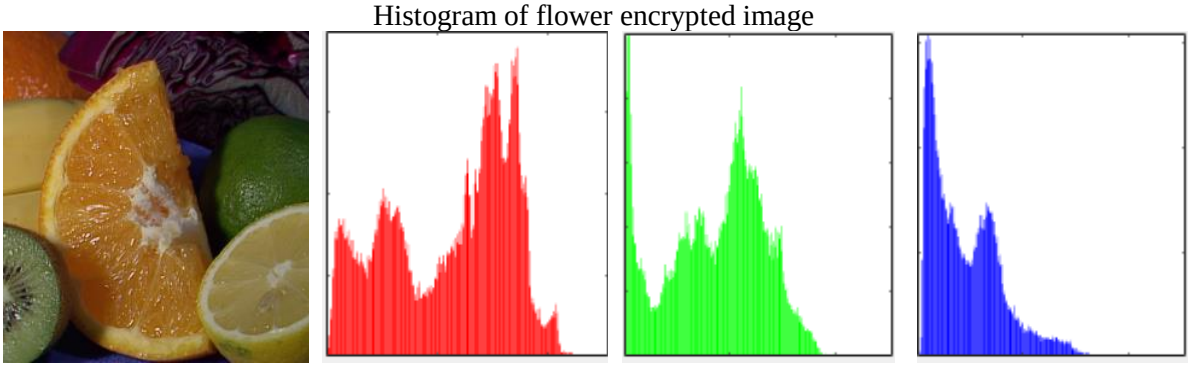
Histogram of Sailboat encrypted image



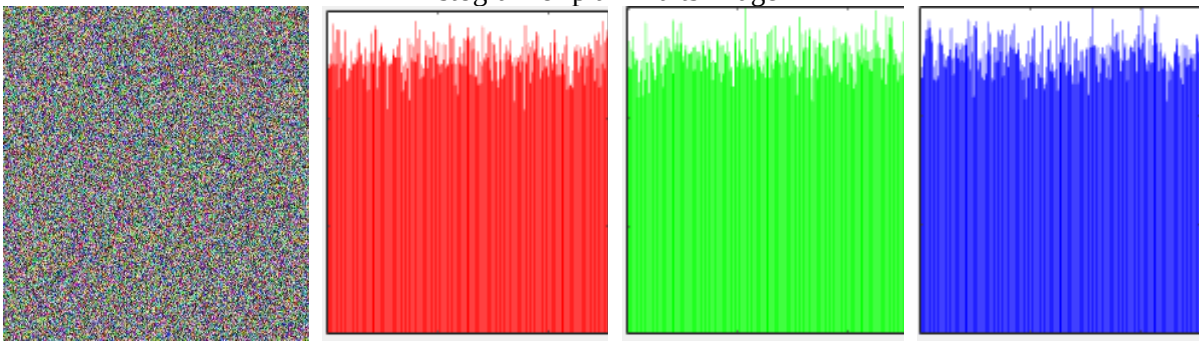
Histogram of flower plain image



Histogram of flower encrypted image



Histogram of plain fruits image



Histogram of encrypted fruits image

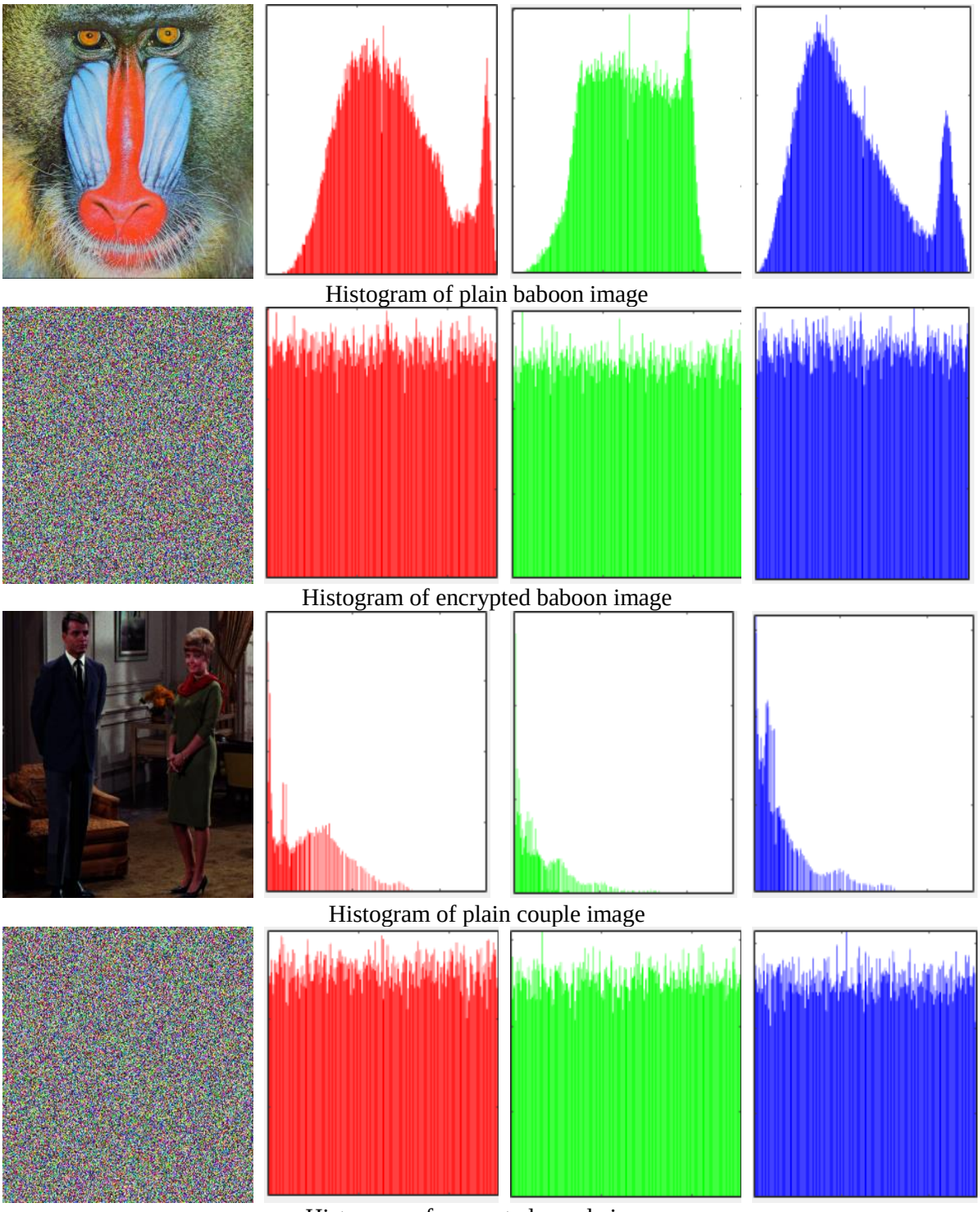
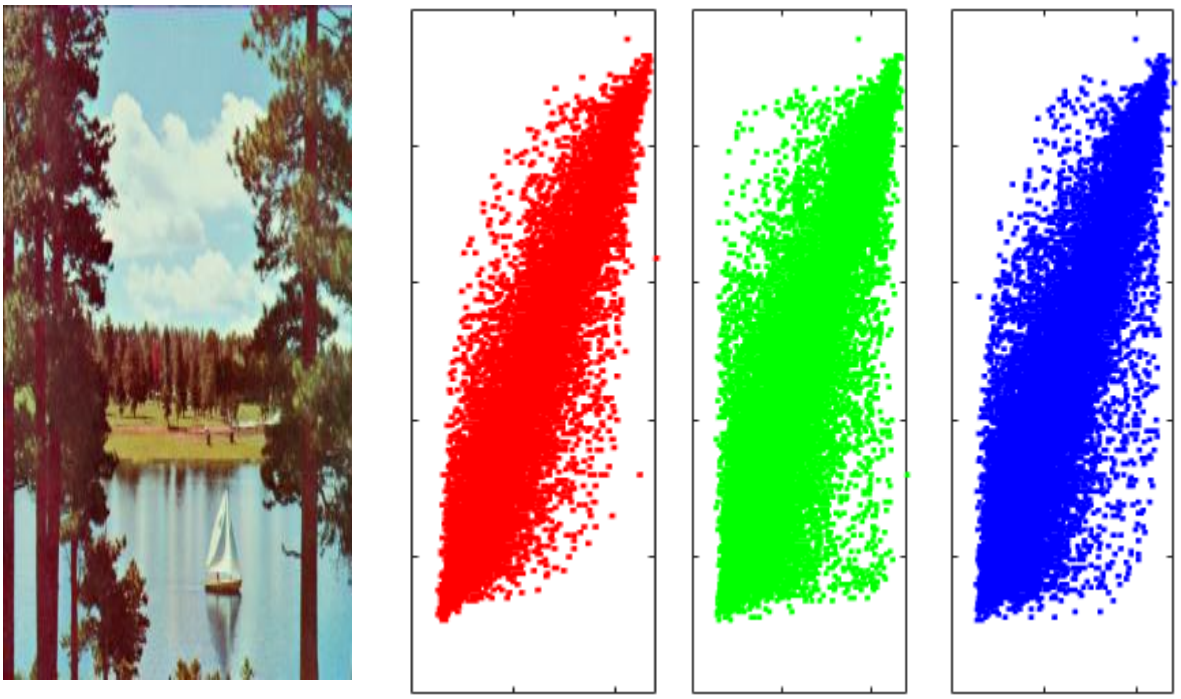


Figure 6.4: Histogram Analysis for plain and encrypted images

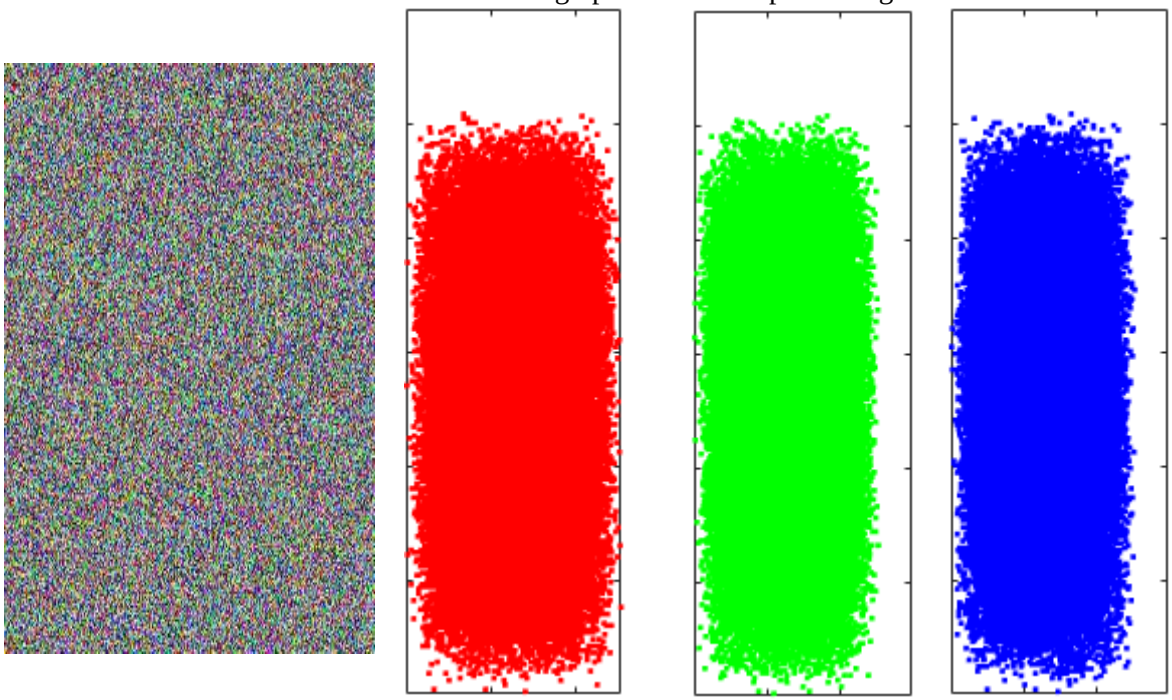
6.7.2. Correlation

The association of adjacent pixels in the horizontal, vertical, and diagonal directions of both the original and encrypted images is depicted in Figures 6.5. The results of the correlation

study may be seen in Table 6.4.



Correlation coefficient graph for sailboat plain image



Correlation coefficient graph for sailboat encrypted image

Figure 6.5: Representation of correlation coefficient graph for fruit plain and encrypted image

Table 6.5: Correlation coefficient results for Lena, sailboat, flower, couple, and baboon images

		Correlation	
Images	**Direction**	**Plain Image**	**Encrypted Image**
Lena	Horizontal	0.9332	0.0001

	Vertical	0.9638	0.0012
	Diagonal	0.9086	-0.0019
Sailboat	Horizontal	0.9524	-0.0001
	Vertical	0.9523	-0.0028
	Diagonal	0.9228	0.0033
Flower	Horizontal	0.9743	-0.0018
	Vertical	0.9735	0.0025
	Diagonal	0.9513	0.0018
Couple	Horizontal	0.9252	-0.0011
	Vertical	0.9464	0.0019
	Diagonal	0.8909	-0.0005
Baboon	Horizontal	0.8914	-0.0008
	Vertical	0.8599	0.0002
	Diagonal	0.8315	0.0030

6.7.3 Entropy

Entropy is a quantitative measure of the degree of randomness that may be employed to describe the complexity of an image's surface. The findings of entropy analysis for both the original and encrypted images are presented in Table 6.6.

Table 6.6: Entropy analysis for Lena, sailboat, flower, couple, and baboon images

Plain Images	**R**	**G**	**B**
Lena	7.2352	7.5687	6.9169
Sailboat	7.2560	7.6093	7.1767
Flower	7.4485	7.4241	7.3760
Couple	6.2501	6.0640	5.9313
Baboon	7.6151	7.3675	7.6750
Encrypted Images	**R**	**G**	**B**
Proposed (Lena)	**7.9985**	**7.9983**	**7.9984**
Proposed (Sailboat)	**7.9989**	**7.9980**	**7.9983**
Proposed (Flower)	**7.9976**	**7.9982**	**7.9983**
Proposed (Couple)	**7.9989**	**7.9982**	**7.9988**
Proposed (Baboon)	**7.9972**	**7.9972**	**7.9971**
Ref [260]	7.9961	7.9940	7.9968
Ref [261]	7.9973	7.9969	7.9971
Ref [262]	7.9901	7.9912	7.9921

5.6.4 Contrast

An optimal level of contrast intensities in the image enhances the saturation of entities,

hence facilitating more accurate identification of the image. It may be inferred that a higher degree of differentiation in the encoded image reflects a stronger encoding process since it correlates with the quantity of confusion influenced by the S-box in the unaltered image.

6.7.4 Homogeneity

The grey-level co-occurrence matrix is utilized throughout the implementation of this examination. The process involves the summation of squared items inside the Grey-Level Co-occurrence Matrix (GLCM). The GLCM exhibits indications of the arrangement of quantities of grey picture elements in tabular form. Table 6.6 shows the results of the homogeneity analysis for the encrypted image.

6.7.5 Energy

The grey-level co-occurrence matrix was utilised during the execution of this study. The concept of energy in the Grey Level Co-occurrence Matrix (GLCM) refers to the summation of the squared values of the matrix elements.

Table 6.7: Majority logic criteria (MLC) for proposed scheme

Images	P/E	Contrast	Energy	Homogeneity
Lena	Plain Encrypted	0.36028 10.479	0.12159 0.029416	0.8809 0.4705
Sailboat	Plain Encrypted	0.50689 10.5021	0.12047 0.029275	0.8586 0.4699
Flower	Plain Encrypted	0.2662 10.5091	0.12439 0.029374	0.9065 0.4703
Couple	Plain Encrypted	0.19962 10.5148	0.36649 0.029479	0.9305 0.4696
Baboon	Plain Encrypted	0.69492 10.5043	0.095375 0.029319	0.7833 0.4695

6.8 NPCR and UACI Analysis

In the case of differential attacks, the Normalised Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Bitplane Correlation-Based Metric (BACI) are the

best ways to check the integrity of an encoded image. NPCR is a metric used to quantify the proportion of dissimilar pixels between two encrypted images. A greater value of NPCR indicates a higher level of effectiveness in encryption with regards to pixel modification. In contrast, UACI computes the mean intensity of alterations in pixels, providing another viewpoint on the influence of encryption. Lower values of the UACI are indicative of more pronounced alterations in pixel intensities. BACI focuses on the correlation between the biplanes of the original and encrypted images. The findings presented in Table 6.8 indicates that the suggested image encoding approach has resulted in increased NPCR and relevant UACI values. The observed high values of the NPCR indicate that the position of each pixel has been significantly randomized. The relevant UACI values indicate that a significant proportion of grey pixel levels are altered in the suggested encryption scheme. The suggested encrypted scheme exhibits superior NPCR values for each RGB channel compared to the other reference schemes. Additionally, the UACI values of the proposed scheme are higher than those of the schemes described in references [224] [225] [226] [227]. The comparison demonstrates that the proposed encryption method has effective diffusion features, suggesting its robustness against algebraic attacks.

Table 6.8: Comparison of statistical tests

Images	NPCR	UACI	BACI
Lena	**99.7831**	**33.5801**	**26.7851**
Sailboat	**99.6821**	**33.4321**	**26.5341**
Flower	**99.6712**	**33.3012**	**26.8291**
Couple	**99.6821**	**33.5876**	**26.2378**
Baboon	**99.6489**	**33.4310**	**26.4921**
Ref [224] (for Lena)	99.6063	33.4579	26.7713
Ref [225] (for Lena)	99.6369	33.4335	26.8290
Ref [226] (for Lena)	99.6000	33.5700	26.5702
Ref [227] (for Lena)	99.6236	33.4898	26.7844
Ref [263] (for Lena)	99.6610	32.9352	-
Ref [264] (for Lena)	99.6399	33.4308	-
Ref [265] (for Lena)	99.5721	33.1264	-
Ref [266] (for Lena)	99.61	30.42	-
Ref [267] (for Lena)	99.636	33.465	-
Ref [268] (for Lena)	99.6089	33.4727	-

6.9 Summary

This study presents a revolutionary methodology for image encryption that integrates two fundamental concepts: elliptic curve cryptography and 4D fractional order chaotic map. The utilization of elliptic curves introduces an extra layer of complexity to the encryption process by generating points. The selection of a four-dimensional (4D) map is rationalized based on its extensive array of factors, which significantly contribute to the augmentation of security measures. It is suggested that the combination of these two procedures has the potential to yield enhanced outcomes in the field of image encryption.

CHAPTER 7

CONCLUSION AND FUTURE WORK

7.1 Introduction

This chapter provides a concise and focused explanation of the outcomes obtained in this thesis and presents plans for future work. The primary focus of the proposed study can be classified into the following categories:

1. Introducing a method for efficiently generating a nonlinear component by employing a combination of linear fractional transformation and a multilayer perceptron neuron.
2. Modified the chaotic maps without altering their mathematical structure and employed various S-boxes in the ciphers to enhance image encryption strength and ensure better dispersion of pixel values.
3. The integration of coset graphs with field extensions and logistic chaotic map is presented to enhance the security of the encryption process.
4. Elliptic curve cryptography (ECC) is combined with a 4D fractional-order chaotic map to secure digital images against tampering and unauthorized attacks.

7.2 Limitations of the Study

1. While the proposed methodology for creating S-boxes is robust, the computational cost associated with the fusion of linear fractional transformation and multilayer perceptron may be significant. This may limit the applicability in resource-constrained environments such as IoT devices.

2. A significant limitation of using chaotic maps in image encryption is their vulnerability

to certain types of attacks, such as chosen-plaintext or known-plaintext attacks. Because chaotic systems are deterministic and their behavior is fully determined by their initial conditions and parameters, an attacker with access to enough plaintext-ciphertext pairs can potentially deduce the chaotic map parameters. This vulnerability can compromise the security of the encryption scheme.

7.3 Threats to validity

1. The creation of S-boxes in cryptography encounters many validity challenges, including vulnerability to linear and differential cryptanalysis, lack of bijectivity, inadequate avalanche effect, non-uniform distribution of XOR operations between input and output, and inability to satisfy the Bit Independence Criterion. It is essential for S-boxes to be constructed with high nonlinearity, unique input-output mappings, and considerable output changes in response to minor input variations in order to provide strong encryption and decryption procedures, since these variables may weaken the security of block ciphers.

2. Image encryption systems that rely on chaotic maps are susceptible to various validity challenges because of their inherent sensitivity. These include the precise replication of initial conditions for accurate decryption, the careful choice of system parameters to ensure strong encryption, the possibility of chaotic systems being predictable and exploited by attackers, and the requirement for the scheme to withstand different cryptanalytic attacks. It is crucial to address these elements in order to ensure the safety and reliability of the encryption method.

3. Quantum computing poses a significant risk to the security of Elliptic Curve Cryptography (ECC) since it has the potential to solve the discrete logarithm issue, compromising the security of ECC. Furthermore, ECC's security can be compromised by improper implementation, the use of weak elliptic curves, side-channel attacks that leverage the leakage of information from the physical functioning of the cryptosystem, and insufficient random number generation. It is essential to address these vulnerabilities in order to maintain the cryptographic integrity of ECC.

7.4 Future work

As we advanced in our research, a multitude of questions emerged within our minds that remained unanswered. This might serve as a valuable resource for future research directions or be seen as an extension of the proposed study. The following is a selection of these.

1. Future studies could explore development of image encryption schemes based on k-means clustering algorithm. The method will effectively group the pixels into clusters or layers based on their color values, which can then be used to segment the image. Comparing the efficiency and visual analysis of this scheme could yield valuable insights into their relative merits and limitations.

2. While our nonlinearity booster algorithm has demonstrated significant improvements in S-box optimization, there remains scope for further refinement. Investigating alternative techniques or incorporating additional cryptographic criteria could enhance its utility and applicability.

3. Higher-dimensional chaotic maps represent a promising avenue for the development of secure cyphers. Future research will focus on exploring and characterizing the unique properties of these maps, such as their higher key space, complexity, and sensitivity to initial conditions. By Leveraging these properties, new encryption algorithms could be crafted to enhance confusion and diffusion, key aspects of cryptographic security.

4. Extending the applications of the proposed S-boxes to IoT devices, such as developing lightweight S-boxes that provide higher security while maintaining efficiency, could further contribute to the development of secure cryptographic systems for IoT devices.

5. The emergence of quantum cryptography poses a significant challenge to current cryptographic algorithms like RSA, DSA, ECC, and AES. These algorithms depend heavily on integer factorization and discrete logarithms, which can be efficiently solved by a sufficiently powerful quantum computer. To address these risks, future research could focus on designing symmetric algorithms with larger key spaces, exploring hybrid cryptographic approaches that combine existing methods for a more robust defense.

6. The future study will examine the construction of 3D S-boxes and their applications in color image analysis.

7. Encryption protects image confidentiality, while image forensics helps verify image integrity and detect tampering. However, encrypted images are challenging to analyze because their pixel values are transformed. Therefore, future work will focus on developing a development tool that can handle decryption or work directly on encrypted data. It can also include combining encryption and forensics while maintaining security and privacy.

7.5 Conclusion

The primary objective of the proposed thesis is to achieve a secure and efficient means of data encryption and ensure the confidentiality of image transmissions via public channels. Therefore, such systems are designed and executed with real-time functionality and advanced security measures. In this thesis, novel, secure, and efficient S-box generation algorithms are introduced by using linear fractional transformation ($PGL(2, GF(2^8))$, on a Galois field, $GF(2^8)$) in connection with an artificial neural network, modified chaotic maps without modification of their mathematical structure (Zaslavsky map, Henon map, and Baker's map). In addition, a novel nonlinearity booster algorithm is presented to improve the cryptographic strength without compromising the efficiency of S-boxes. The nonlinearity booster algorithm has proven to be effective in block cyphers, greatly enhancing the security of multimedia and serving as a crucial factor in maintaining the integrity and authenticity of multimedia content. To evaluate the robustness of the proposed S-boxes, we have employed a range of cryptographic tests, including nonlinearity, strict avalanche criterion, bit independence criterion, linear approximation probability, differential approximation probability, and bijectivity. The results of these tests are satisfactory and meet our expectations. To showcase the applications of the proposed S-boxes, this thesis further applies the constructed S-boxes to image encryption applications. The encryption algorithm has been experimentally evaluated through several measures such as entropy, correlation, homogeneity, energy, contrast, NPCR, UACI, BACI, histogram analysis, and other statistical analyses and visual analyses. The experimental results demonstrate that our scheme is robust against various attacks, including brute force and linear

and differential attacks. Lastly, experimental results and further security analysis verified the significance of our scheme in supporting real-time image encryption.

REFERENCES

[1] C. E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.

[2] I. Hussain, T. Shah, H. Mahmood, and M. Afzal, “Comparative Analysis of S-boxes Based on Graphical SAC,” *Int. J. Comput. Appl.*, vol. 2, no. 5, pp. 5–8, 2010, doi: 10.5120/669-938.

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

[4] 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.

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

[6] Y. Jia, Z. Yin, X. Zhang, and Y. Luo, “Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting,” *Signal Processing*, vol. 163, pp. 238–246, 2019, doi: 10.1016/j.sigpro.2019.05.020.

[7] M. Alawida, A. Samsudin, J. Sen Teh, and R. S. Alkhawaldeh, “A new hybrid digital chaotic system with applications in image encryption,” *Signal Processing*, vol. 160, pp. 45–58, 2019, doi: 10.1016/j.sigpro.2019.02.016.

[8] Z. Hua, Z. Zhu, S. Yi, Z. Zhang, and H. Huang, “Cross-plane colour image encryption using a two-dimensional logistic tent modular map,” *Inf. Sci. (Ny).*, vol. 546, pp. 1063–1083, 2021, doi: 10.1016/j.ins.2020.09.032.

[9] W. Wen, K. Wei, Y. Zhang, Y. Fang, and M. Li, “Colour light field image encryption based on DNA sequences and chaotic systems,” *Nonlinear Dyn.*, vol. 99, no. 2, pp. 1587–1600, 2020, doi: 10.1007/s11071-019-05378-8.

[10] Z. Xia, X. Wang, W. Zhou, R. Li, C. Wang, and C. Zhang, “Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms,” *Signal Processing*, vol. 157, pp. 108–118, 2019, doi: 10.1016/j.sigpro.2018.11.011.

[11] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, “Color Image Encryption Through Chaos and KAA Map,” *IEEE Access*, vol. 11, pp. 11541–11554, 2023, doi: 10.1109/ACCESS.2023.3242311.

[12] Q. Lai, G. Hu, U. Erkan, and A. Toktas, “A novel pixel-split image encryption scheme based on 2D Salomon map,” *Expert Syst. Appl.*, vol. 213, 2023, doi: 10.1016/j.eswa.2022.118845.

[13] W. Alexan, Y. L. Chen, L. Y. Por, and M. Gabr, “Hyperchaotic Maps and the Single Neuron Model: A Novel Framework for Chaos-Based Image Encryption,” *Symmetry (Basel).*, vol. 15, no. 5, 2023, doi: 10.3390/sym15051081.

[14] Z. Liu, Y. Wang, Y. Zhao, and L. Y. Zhang, “A stream cipher algorithm based on 2D coupled map lattice and partitioned cellular automata,” *Nonlinear Dyn.*, vol. 101, no. 2, pp. 1383–1396, 2020, doi: 10.1007/s11071-020-05804-2.

[15] S. C. Wang, C. H. Wang, and C. Xu, “An image encryption algorithm based on a hidden attractor chaos system and the Knuth–Durstenfeld algorithm,” *Opt. Lasers Eng.*, vol. 128, 2020, doi: 10.1016/j.optlaseng.2019.105995.

[16] S. Zhou, X. Wang, and Y. Zhang, “Novel image encryption scheme based on chaotic signals with finite-precision error,” *Inf. Sci. (Ny).*, vol. 621, pp. 782–798, 2023, doi: 10.1016/j.ins.2022.11.104.

[17] C. Xu, J. Sun, and C. Wang, “An Image Encryption Algorithm Based on Random Walk and Hyperchaotic Systems,” *Int. J. Bifurc. Chaos*, vol. 30, no. 4, 2020, doi: 10.1142/S0218127420500601.

[18] Z. Hua, Y. Zhang, and Y. Zhou, “Two-Dimensional Modular Chaotification System for Improving Chaos Complexity,” *IEEE Trans. Signal Process.*, vol. 68, pp. 1937–1949, 2020, doi: 10.1109/TSP.2020.2979596.

[19] Y. Zhang, Y. Li, W. Wen, Y. Wu, and J. xin Chen, “Deciphering an image cipher based on 3-cell chaotic map and biological operations,” *Nonlinear Dyn.*, vol. 82, no. 4, pp. 1831–1837, 2015, doi: 10.1007/s11071-015-2280-1.

[20] S. Kumar *et al.*, “SHC: 8-bit Compact and Efficient S-Box Structure for Lightweight Cryptography,” *IEEE Access*, vol. 12, pp. 39430–39449, 2024, doi: 10.1109/ACCESS.2024.3372388.

[21] W. Q. Wu and L. S. Kong, “Image encryption algorithm based on a new 2D polynomial chaotic map and dynamic S-box,” *Signal, Image Video Process.*, vol. 18, no. 4, pp. 3213–3228, 2024, doi: 10.1007/s11760-023-02984-3.

[22] H. Wen, Z. Feng, C. Bai, Y. Lin, X. Zhang, and W. Feng, “Frequency-domain image encryption based on IWT and 3D S-box,” *Phys. Scr.*, vol. 99, no. 5, 2024, doi: 10.1088/1402-4896/ad30ec.

[23] F. Artuğer, “A novel algorithm based on DNA coding for substitution box generation problem,” *Neural Comput. Appl.*, vol. 36, no. 3, pp. 1283–1294, 2024, doi: 10.1007/s00521-023-09095-7.

[24] J. Ali, M. K. Jamil, A. S. Alali, R. Ali, and Gulraiz, “A medical image encryption scheme based on Mobius transformation and Galois field,” *Heliyon*, vol. 10, no. 1, 2024, doi: 10.1016/j.heliyon.2023.e23652.

[25] L. D. Singh *et al.*, “Image encryption using dynamic S-boxes generated using elliptic curve points and chaotic system,” *J. Inf. Secur. Appl.*, vol. 83, 2024, doi: 10.1016/j.jisa.2024.103793.

[26] A. Malal and C. Tezcan, “FPGA-friendly compact and efficient AES-like 8 × 8 S-box,” *Microprocess. Microsyst.*, p. 105007, Jan. 2024, doi: 10.1016/j.micpro.2024.105007.

[27] F. Artuğer and F. Özkaynak, “A new post-processing approach for improvement of nonlinearity property in substitution boxes,” *Integration*, vol. 94, p. 102105, 2024, doi: 10.1016/j.vlsi.2023.102105.

[28] A. Hadj Brahim, A. Ali Pacha, and N. Hadj Said, “An image encryption scheme based on a modified AES algorithm by using a variable S-box,” *J. Opt.*, vol. 53, no. 2, pp. 1170–1185, 2024, doi: 10.1007/s12596-023-01232-8.

[29] H. Zhang and H. Hu, “An image encryption algorithm based on a compound-coupled chaotic system,” *Digit. Signal Process. A Rev. J.*, vol. 146, 2024, doi: 10.1016/j.dsp.2023.104367.

[30] Y. Kumar and V. Guleria, “Mixed-multiple image encryption algorithm using RSA cryptosystem with fractional discrete cosine transform and 2D-Arnold Transform,” *Multimed. Tools Appl.*, vol. 83, no. 13, pp. 38055–38081, 2024, doi: 10.1007/s11042-023-16953-y.

[31] B. Arshad, N. Siddiqui, Z. Hussain, and M. Ehatisham-ul-Haq, “A Novel Scheme for Designing Secure Substitution Boxes (S-Boxes) Based on Mobius Group and Finite Field,” *Wirel. Pers. Commun.*, vol. 124, no. 4, pp. 3527–3548, 2022, doi: 10.1007/s11277-022-09524-1.

[32] O. Sengel, M. A. Aydin, and A. Sertbas, “An Efficient Generation and Security Analysis of Substitution Box Using Fingerprint Patterns,” *IEEE Access*, vol. 8, pp. 160158–160176, 2020, doi: 10.1109/ACCESS.2020.3021055.

[33] L. Li, J. Liu, Y. Guo, and B. Liu, “A new S-box construction method meeting strict avalanche criterion,” *J. Inf. Secur. Appl.*, vol. 66, 2022, doi: 10.1016/j.jisa.2022.103135.

[34] An Braeken, “Cryptographic Properties of Boolean Functions and S-Boxes,” 2006. [Online]. Available: https://securewww.esat.kuleuven.be/cosic/publications/thesis-129.pdf

[35] H. Liu, J. Liu, and C. Ma, “Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption,” *Multimed. Tools Appl.*, vol. 82, no. 16, pp. 23899–23914, 2023, doi: 10.1007/s11042-022-12069-x.

[36] H. Liu, A. Kadir, and C. Xu, “Cryptanalysis and constructing S-Box based on chaotic map and backtracking,” *Appl. Math. Comput.*, vol. 376, 2020, doi: 10.1016/j.amc.2020.125153.

[37] Y. Si, H. Liu, and Y. Chen, “Constructing Keyed Strong S-Bo Using an Enhanced Quadratic Map,” *Int. J. Bifurc. Chaos*, vol. 31, no. 10, 2021, doi: 10.1142/S0218127421501467.

[38] Y. Wang, K. W. Wong, C. Li, and Y. Li, “A novel method to design S-box based on chaotic map and genetic algorithm,” *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 376, no. 6–7, pp. 827–833, 2012, doi: 10.1016/j.physleta.2012.01.009.

[39] L. Lacko-Bartošová, “Linear and differential cryptanalysis of reduced-round AES,” *Tatra Mt. Math. Publ.*, vol. 50, no. 1, pp. 51–61, 2011, doi: 10.2478/v10127-011-0036-y.

[40] S. Das, J. K. M. S. U. Zaman, and R. Ghosh, “Generation of AES S-boxes with Various Modulus and Additive Constant Polynomials and Testing their Randomization,” *Procedia Technol.*, vol. 10, pp. 957–962, 2013, doi: 10.1016/j.protcy.2013.12.443.

[41] K. Kazlauskas, G. Vaicekauskas, and R. Smaliukas, “An Algorithm for Key-Dependent S-Box Generation in Block Cipher System,” *Inform.*, vol. 26, no. 1, pp. 51–65, 2015, doi: 10.15388/Informatica.2015.38.

[42] F. H. Nejad, S. Sabah, and A. J. Jam, “Analysis of avalanche effect on advance encryption standard by using dynamic S-Box depends on rounds keys,” *2014 Int. Conf. Comput. Sci. Technol. ICCST 2014*, 2014, doi: 10.1109/ICCST.2014.7045184.

[43] H. Singh, “Enhancing AES using Novel Block Key Generation Algorithm and Key Dependent S-boxes,” *Int. J. Cyber-Security Digit. Forensics*, vol. 5, no. 1, pp. 30–45, 2016, doi: 10.17781/p001985.

[44] B. K. Maram and J. M. Gnanasekar, “Evaluation of Key Dependent S-Box Based Data Security Algorithm using Hamming Distance and Balanced Output,” *TEM J.*, vol. 5, no. 1, pp. 67–75, 2016.

[45] Q. Lu, C. Zhu, and X. Deng, “An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box,” *IEEE Access*, vol. 8, pp. 25664–25678, 2020, doi: 10.1109/ACCESS.2020.2970806.

[46] E. Corona-Bermúdez, J. C. Chimal-Eguía, U. Corona-Bermúdez, and M. E. Rivero-Ángeles, “Chaos Meets Cryptography: Developing an S-Box Design with the Rössler Attractor,” *Mathematics*, vol. 11, no. 22, p. 4575, Nov. 2023, doi: 10.3390/math11224575.

[47] V. A. Thakor, M. A. Razzaque, A. D. Darji, and A. R. Patel, “A novel 5-bit S-box design for lightweight cryptography algorithms,” *J. Inf. Secur. Appl.*, vol. 73, 2023, doi: 10.1016/j.jisa.2023.103444.

[48] Y. Si, H. Liu, and M. Zhao, “Constructing keyed strong S-Box with higher nonlinearity based on 2D hyper chaotic map and algebraic operation,” *Integration*, vol. 88, pp. 269–277, 2023, doi: 10.1016/j.vlsi.2022.10.011.

[49] S. Fahd, M. Afzal, D. Shah, W. Iqbal, and Y. Abbas, “Detection of non-trivial preservable quotient spaces in S-Box(es),” *Neural Comput. Appl.*, vol. 35, no. 25, pp. 18343–18355, 2023, doi: 10.1007/s00521-023-08654-2.

[50] S. Maiti and D. R. Chowdhury, “Design of fault-resilient S-boxes for AES-like block ciphers,” *Cryptogr. Commun.*, vol. 13, no. 1, pp. 71–100, 2021, doi: 10.1007/s12095-020-00452-0.

[51] M. Gupta and A. Sinha, “Enhanced-AES encryption mechanism with S-box splitting for wireless sensor networks,” *Int. J. Inf. Technol.*, vol. 13, no. 3, pp. 933–941, 2021, doi: 10.1007/s41870-021-00626-w.

[52] A. H. Zahid *et al.*, “Dynamic S-Box Design Using a Novel Square Polynomial Transformation and Permutation,” *IEEE Access*, vol. 9, pp. 82390–82401, 2021, doi: 10.1109/ACCESS.2021.3086717.

[53] S. Shaukat Jamal, D. Shah, A. Deajim, and T. Shah, “The Effect of the Primitive Irreducible Polynomial on the Quality of Cryptographic Properties of Block Ciphers,” *Secur. Commun. Networks*, vol. 2020, 2020, doi: 10.1155/2020/8883884.

[54] A. H. Zahid *et al.*, “Construction of Optimized Dynamic S-Boxes Based on a Cubic Modular Transform and the Sine Function,” *IEEE Access*, vol. 9, pp. 131273–131285, 2021, doi: 10.1109/ACCESS.2021.3113338.

[55] Y. Wang, Z. Zhang, L. Y. Zhang, J. Feng, J. Gao, and P. Lei, “A genetic algorithm for constructing bijective substitution boxes with high nonlinearity,” *Inf. Sci. (Ny).*, vol. 523, pp. 152–166, 2020, doi: 10.1016/j.ins.2020.03.025.

[56] V. Nandan and R. G. S. Rao, “Low-power AES S-box design using dual-basis tower field extension method for cyber security applications,” *Complex Intell. Syst.*, vol. 9, no. 3, pp. 2959–2967, 2023, doi: 10.1007/s40747-021-00556-x.

[57] D. James and T. L. Priya, “An innovative approach for dynamic key dependent S-Box to enhance security of IoT systems,” *Meas. Sensors*, vol. 30, 2023, doi: 10.1016/j.measen.2023.100923.

[58] T. A. Al-Maadeed, I. Hussain, A. Anees, and M. T. Mustafa, “A image encryption algorithm based on chaotic Lorenz system and novel primitive polynomial S-boxes,” *Multimed. Tools Appl.*, vol. 80, no. 16, pp. 24801–24822, 2021, doi: 10.1007/s11042-021-10695-5.

[59] 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.

[60] S. Zhu, X. Deng, W. Zhang, and C. Zhu, “Secure image encryption scheme based on a new robust chaotic map and strong S-box,” *Math. Comput. Simul.*, vol. 207, pp. 322–346, 2023, doi: 10.1016/j.matcom.2022.12.025.

[61] V. Rijmen, “Efficient Implementation of the Rijndael S-box,” *Kathol. Univ. Leuven, Dept. ESAT. Belgium*, no. JULY 2000, pp. 1–3, 2000, [Online]. Available: http://www.networkdls.com/Articles/sbox.pdf

[62] F. Piper and S. Murphy, *Team-Fly Cryptography: A Very Short Introduction by Fred Piper and Sean Murphy Oxford University Press © 2002 (142*, vol. 2002. 2002.

[63] Niels Ferguson, Bruce Schneier, Tadayoshi Kohno and B. S. Niels Ferguson, *Cryptography Engineering: Design Principles and Practical Applications, Chapter 9.4: The Generator*. Wiley, 2010.

[64] S. Mister and C. Adams, “Practical S-box design,” *Work. Sel. Areas Cryptogr. SAC*, pp. 1–17, 1996, [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.40.7715&rep=rep1&type=pdf

[65] C. Carlet, “Boolean Functions for Cryptography and Error-Correcting Codes,” *Boolean Model. Methods Math. Comput. Sci. Eng.*, pp. 257–397, 2013, doi: 10.1017/cbo9780511780448.011.

[66] H. Alsaif, R. Guesmi, A. Kalghoum, B. M. Alshammari, and T. Guesmi, “A Novel

Strong S-Box Design Using Quantum Crossover and Chaotic Boolean Functions for Symmetric Cryptosystems," *Symmetry (Basel).*, vol. 15, no. 4, 2023, doi: 10.3390/sym15040833.

[67] R. Zhang *et al.*, "Boolean chaos," *Phys. Rev. E - Stat. Nonlinear, Soft Matter Phys.*, vol. 80, no. 4, 2009, doi: 10.1103/PhysRevE.80.045202.

[68] Z. Jiang and Q. Ding, "Construction of an s-box based on chaotic and bent functions," *Symmetry (Basel).*, vol. 13, no. 4, 2021, doi: 10.3390/sym13040671.

[69] R. Guesmi, M. A. Ben Farah, A. Kachouri, and M. Samet, "Chaos-based designing of a highly nonlinear S-box using Boolean functions," in *12th International Multi-Conference on Systems, Signals and Devices, SSD 2015*, 2015. doi: 10.1109/SSD.2015.7348106.

[70] M. A. B. Farah, A. Farah, and T. Farah, "An image encryption scheme based on a new hybrid chaotic map and optimized substitution box," *Nonlinear Dyn.*, vol. 99, no. 4, pp. 3041–3064, 2020, doi: 10.1007/s11071-019-05413-8.

[71] M. Ahmad and Z. Ahmad, "Random Search Based Efficient Chaotic Substitution Box Design for Image Encryption," *Int. J. Rough Sets Data Anal.*, vol. 5, no. 2, pp. 131–147, 2018, doi: 10.4018/ijrsda.2018040107.

[72] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, 2018, doi: 10.1007/s00521-016-2511-5.

[73] M. Usama, O. Rehman, I. Memon, and S. Rizvi, "An efficient construction of key-dependent substitution box based on chaotic sine map," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 12, 2019, doi: 10.1177/1550147719895957.

[74] M. Gabr *et al.*, "Application of DNA Coding, the Lorenz Differential Equations and a Variation of the Logistic Map in a Multi-Stage Cryptosystem," *Symmetry (Basel).*, vol. 14, no. 12, 2022, doi: 10.3390/sym14122559.

[75] W. Alexan, M. Elbeltagy, and A. Aboshousha, "RGB Image Encryption through Cellular Automata, S-Box and the Lorenz System," *Symmetry (Basel).*, vol. 14, no. 3, 2022, doi: 10.3390/sym14030443.

[76] M. M. Dimitrov, "On the Design of Chaos-Based S-Boxes," *IEEE Access*, vol. 8, pp. 117173–117181, 2020, doi: 10.1109/ACCESS.2020.3004526.

[77] W. Yan and Q. Ding, "A novel s-box dynamic design based on nonlinear-transform of 1d chaotic maps," *Electron.*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111313.

[78] M. S. Mahmood Malik *et al.*, "Generation of Highly Nonlinear and Dynamic AES Substitution-Boxes (S-Boxes) Using Chaos-Based Rotational Matrices," *IEEE Access*, vol. 8, pp. 35682–35695, 2020, doi: 10.1109/ACCESS.2020.2973679.

[79] A. Alghafis, N. Munir, M. Khan, and I. Hussain, "An Encryption Scheme Based on Discrete Quantum Map and Continuous Chaotic System," *Int. J. Theor. Phys.*, vol. 59, no. 4, pp. 1227–1240, 2020, doi: 10.1007/s10773-020-04402-7.

[80] E. Tanyildizi and F. Ozkaynak, “A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps,” *IEEE Access*, vol. 7, pp. 117829–117838, 2019, doi: 10.1109/ACCESS.2019.2936447.

[81] F. Riaz and N. Siddiqui, “Design of an efficient cryptographic substitution box by using improved chaotic range with the golden ratio,” *Int. J. Comput. Sci. Inf. Secur.*, vol. 18, no. 1, pp. 89–94, 2020.

[82] J. Daemen and V. Rijmen, *The Design of Rijndael*. 2002. [Online]. Available: http://portal.acm.org/citation.cfm?id=560131

[83] M. S. de Alencar, *Cryptography and Network Security*. 2022. doi: 10.1515/9781683926900.

[84] J. Huntington, *Data Communications and Networking*. 2007. doi: 10.1016/b978-0-240-80937-3.50021-0.

[85] W. M. Rittinghouse,John W; Hancock, *Cyber Security Operations Handbook*. 2004.

[86] H. M. Heys, “A tutorial on linear and differential cryptanalysis,” *Cryptologia*, vol. 26, no. 3, pp. 189–221, 2002, doi: 10.1080/0161-110291890885.

[87] V. F. Kleist, *The code book: the science of secrecy from ancient egypt to quantum cryptography [Book Review]*, vol. 24, no. 2. 2005. doi: 10.1109/mahc.2002.1010078.

[88] T. Haider, N. A. Azam, and U. Hayat, “Substitution box generator with enhanced cryptographic properties and minimal computation time,” *Expert Syst. Appl.*, vol. 241, 2024, doi: 10.1016/j.eswa.2023.122779.

[89] L. Burnett, “Heuristic Optimization of Boolean Functions and Substitution Boxes for Cryptography,” 2005.

[90] T. W. Cusick and P. Stanica, *Cryptographic Boolean Functions and Applications*. 2009. doi: 10.1016/B978-0-12-374890-4.X0001-8.

[91] T. Siegenthaler, “Correlation-Immunity of Nonlinear Combining Functions for Cryptographic Applications,” *IEEE Trans. Inf. Theory*, vol. 30, no. 5, pp. 776–780, 1984, doi: 10.1109/TIT.1984.1056949.

[92] M. Matsui, “Linear cryptanalysis method for DES cipher,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 765 LNCS, pp. 386–397, 1994, doi: 10.1007/3-540-48285-7_33.

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

[94] C. Carlet, “A larger class of cryptographic boolean functions via a study of the maiorana-McFarland construction,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 2442, pp. 549–564, 2002, doi: 10.1007/3-540-45708-9_35.

[95] O. S. Rothaus, “On ‘bent’ functions,” *J. Comb. Theory, Ser. A*, vol. 20, no. 3, pp. 300–305, 1976, doi: 10.1016/0097-3165(76)90024-8.

[96] K. Moeen, “Progressive product reduction for polynomial basis multiplication over GF(3m),” 2016.

[97] D. R. Hankerson, G. A. Harris, and P. D. Johnson, *DR. DUBLIN retires.*, vol. 36, no. 2. 1953.

[98] A. Aidoo and K. B. Gyam, “Construction of Irreducible Polynomials in Galois elds, GF(2m) Using Normal Bases,” *Asian Res. J. Math.*, pp. 1–15, 2019, doi: 10.9734/arjom/2019/v14i330131.

[99] S. Abrahamyan, “Construction of irreducible polynomials over finite fields,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6244 LNCS, pp. 1–3, 2010, doi: 10.1007/978-3-642-15274-0_1.

[100] L. C. Nizam Chew and E. S. Ismail, “S-box construction based on linear fractional transformation and permutation function,” *Symmetry (Basel).*, vol. 12, no. 5, May 2020, doi: 10.3390/SYM12050826.

[101] S. Farwa, T. Shah, and L. Idrees, “A highly nonlinear S-box based on a fractional linear transformation,” *Springerplus*, vol. 5, no. 1, Dec. 2016, doi: 10.1186/s40064-016-3298-7.

[102] A. H. Zahid *et al.*, “Efficient Dynamic S-Box Generation Using Linear Trigonometric Transformation for Security Applications,” *IEEE Access*, vol. 9, pp. 98460–98475, 2021, doi: 10.1109/ACCESS.2021.3095618.

[103] Z. Hua, J. Li, Y. Chen, and S. Yi, “Design and application of an S-box using complete Latin square,” *Nonlinear Dyn.*, vol. 104, no. 1, pp. 807–825, 2021, doi: 10.1007/s11071-021-06308-3.

[104] H. S. Alhadawi, M. A. Majid, D. Lambić, and M. Ahmad, “A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm,” *Multimed. Tools Appl.*, vol. 80, no. 5, pp. 7333–7350, 2021, doi: 10.1007/s11042-020-10048-8.

[105] O. A. Dawood, M. Khalaf, F. M. Mohammed, and H. K. Almulla, “Design a Compact Non-linear S-Box with Multiple-Affine Transformations,” in *Communications in Computer and Information Science*, Springer, 2020, pp. 439–452. doi: 10.1007/978-3-030-38752-5_34.

[106] B. M. Alshammari, R. Guesmi, T. Guesmi, H. Alsaif, and A. Alzamil, “Implementing a symmetric lightweight cryptosystem in highly constrained iot devices by using a chaotic s-box,” *Symmetry (Basel).*, vol. 13, no. 1, pp. 1–20, Jan. 2021, doi: 10.3390/sym13010129.

[107] T. Shah, A. Qamar, and I. Hussain, “Substitution box on maximal cyclic subgroup of units of a galois ring,” *Zeitschrift fur Naturforsch. - Sect. A J. Phys. Sci.*, vol. 68, no. 8–9, pp. 567–572, 2013, doi: 10.5560/ZNA.2013-0021.

[108] M. F. Bin Roslan, K. Seman, A. H. Ab Halim, and M. N. A. Syam Mohd Sayuti, “Substitution Box Design Based from Symmetric Group Composition,” *J. Phys. Conf. Ser.*, vol. 1366, no. 1, 2019, doi: 10.1088/1742-6596/1366/1/012001.

[109] A. Hussain Alkhaldi, I. Hussain, and M. A. Gondal, “A novel design for the construction of safe S-boxes based on TD ERC sequence,” *Alexandria Eng. J.*, vol. 54,

no. 1, pp. 65–69, 2015, doi: 10.1016/j.aej.2015.01.003.

[110] G. Ivanov, N. Nikolov, and S. Nikova, “Cryptographically strong S-boxes generated by modified immune algorithm,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9540, pp. 31–42, 2016, doi: 10.1007/978-3-319-29172-7_3.

[111] D. Lambić, “A novel method of S-box design based on discrete chaotic map,” *Nonlinear Dyn.*, vol. 87, no. 4, pp. 2407–2413, 2017, doi: 10.1007/s11071-016-3199-x.

[112] H. Nasry, A. A. Abdallah, A. K. Farhan, H. E. Ahmed, and W. I. E. Sobky, “Multi Chaotic System to Generate Novel S-Box for Image Encryption,” *J. Phys. Conf. Ser.*, vol. 2304, no. 1, 2022, doi: 10.1088/1742-6596/2304/1/012007.

[113] A. Y. Al-Dweik, I. Hussain, M. Saleh, and M. T. Mustafa, “A novel method to generate key-dependent s-boxes with identical algebraic properties,” *J. Inf. Secur. Appl.*, vol. 64, 2022, doi: 10.1016/j.jisa.2021.103065.

[114] A. Waheed, F. Subhan, M. M. Suud, M. Alam, and S. Ahmad, “An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges,” *Multimed. Tools Appl.*, vol. 82, no. 19, pp. 29689–29712, 2023, doi: 10.1007/s11042-023-14910-3.

[115] S. V. Radhakrishnan and S. Subramanian, “An analytical approach to s-box generation,” *Comput. Electr. Eng.*, vol. 39, no. 3, pp. 1006–1015, 2013, doi: 10.1016/j.compeleceng.2012.11.019.

[116] K. Mohamed, F. Hani Hj Mohd Ali, S. Ariffin, N. Hafiza Zakaria, and M. Nazran Mohammed Pauzi, “An Improved AES S-box Based on Fibonacci Numbers and Prime Factor,” *Int. J. Netw. Secur.*, vol. 20, no. 6, p. 1206, 2018, doi: 10.6633/IJNS.201811.

[117] D. Lambić and M. Živković, “Comparison of random S-Box generation methods,” *Publ. l’Institut Math.*, vol. 93, no. 107, pp. 109–115, 2013, doi: 10.2298/PIM1307109L.

[118] P. Mroczkowski, “Generating Pseudorandom S-Boxes – a Method of Improving the Security of Cryptosystems Based on Block Ciphers,” *J. Telecommun. Inf. Technol.*, vol. nr 2, no. 2, pp. 74–79, 2023, doi: 10.26636/jtit.2009.2.931.

[119] M. M. Dimitrov, “On the Design of Chaos-Based S-Boxes,” *IEEE Access*, vol. 8, pp. 117173–117181, 2020, doi: 10.1109/ACCESS.2020.3004526.

[120] D. Zhu, X. Tong, M. Zhang, and Z. Wang, “A new s-box generation method and advanced design based on combined chaotic system,” *Symmetry (Basel).*, vol. 12, no. 12, pp. 1–17, 2020, doi: 10.3390/sym12122087.

[121] A. H. Zahid *et al.*, “A Novel Construction of Dynamic S-Box with High Nonlinearity Using Heuristic Evolution,” *IEEE Access*, vol. 9, pp. 67797–67812, 2021, doi: 10.1109/ACCESS.2021.3077194.

[122] A. Javeed, T. Shah, and Attaullah, “Design of an S-box using Rabinovich-Fabrikant system of differential equations perceiving third order nonlinearity,” *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 6649–6660, 2020, doi: 10.1007/s11042-019-08393-4.

[123] M. T. Tran, D. K. Bui, and A. D. Duong, “Gray S-box for Advanced Encryption Standard,” *Proc. - 2008 Int. Conf. Comput. Intell. Secur. CIS 2008*, vol. 1, pp. 253–258, 2008, doi: 10.1109/CIS.2008.205.

[124] L. Cui and Y. Cao, “A new S-box structure named affine-power-affine,” *Int. J. Innov. Comput. Inf. Control*, vol. 3, no. 3, pp. 751–759, 2007.

[125] I. Hussain, T. Shah, M. A. Gondal, and W. A. Khan, “Construction of Cryptographically Strong 8x8 S-boxes,” *World Appl. Sci. J.*, vol. 13, no. 11, pp. 2389–2395, 2011.

[126] X. Yi, S. X. Cheng, X. H. You, and K. Y. Lam, “Method for obtaining cryptographically strong 8×8 S-boxes,” *Conf. Rec. / IEEE Glob. Telecommun. Conf.*, vol. 2, pp. 689–693, 1997, doi: 10.1109/glocom.1997.638418.

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

[128] H. Feistel, “Cryptography and Computer Privacy,” *Sci. Am.*, vol. 228, no. 5, pp. 15–23, 1973, doi: 10.1038/scientificamerican0573-15.

[129] B. Abd-El-Atty, “Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem,” *Complex Intell. Syst.*, 2023, doi: 10.1007/s40747-023-00988-7.

[130] K. Z. Zamli, F. Din, and H. S. Alhadawi, “Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization,” *Neural Comput. Appl.*, vol. 35, no. 14, pp. 10449–10471, 2023, doi: 10.1007/s00521-023-08243-3.

[131] R. H. Sani, S. Behnia, and J. Ziaei, “Construction of S-box based on chaotic piecewise map: Watermark application,” *Multimed. Tools Appl.*, vol. 82, no. 1, pp. 1131–1148, 2023, doi: 10.1007/s11042-022-13278-0.

[132] Y. Qobbi, A. Abid, M. Jarjar, S. El Kaddouhi, A. Jarjar, and A. Benazzi, “Adaptation of a genetic operator and a dynamic S-box for chaotic encryption of medical and color images,” *Sci. African*, vol. 19, 2023, doi: 10.1016/j.sciaf.2023.e01551.

[133] N. Abughazalah, A. Latif, M. W. Hafiz, M. Khan, A. S. Alanazi, and I. Hussain, “Construction of multivalued cryptographic boolean function using recurrent neural network and its application in image encryption scheme,” *Artif. Intell. Rev.*, vol. 56, no. 6, pp. 5403–5443, 2023, doi: 10.1007/s10462-022-10295-1.

[134] X. Sun, Z. Chen, L. Wang, and C. He, “A lossless image compression and encryption algorithm combining JPEG-LS, neural network and hyperchaotic system,” *Nonlinear Dyn.*, vol. 111, no. 16, pp. 15445–15475, 2023, doi: 10.1007/s11071-023-08622-4.

[135] A. Kadir, M. S. Azzaz, and R. Kaibou, “Chaos-based Key Generator using Artificial Neural Networks Models,” *2023 Int. Conf. Adv. Electron. Control Commun. Syst. ICAECCS 2023*, 2023, doi: 10.1109/ICAECCS56710.2023.10105105.

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

[137] J. Kim and R. C. W. Phan, “Advanced differential-style cryptanalysis of the NSA’s

Skipjack block Cipher," *Cryptologia*, vol. 33, no. 3, pp. 246–270, 2009, doi: 10.1080/01611190802653228.

[138] N. Siddiqui *et al.*, "A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field," *PLoS One*, vol. 15, no. 11 November, 2020, doi: 10.1371/journal.pone.0241890.

[139] A. Mahboob *et al.*, "A Novel Construction of Substitution Box Based on Polynomial Mapped and Finite Field with Image Encryption Application," *IEEE Access*, vol. 10, pp. 119244–119258, 2022, doi: 10.1109/ACCESS.2022.3218643.

[140] H. Isa, S. A. A. Syed Junid, M. R. Z'aba, R. Endut, S. M. Ammar, and N. Ali, "Enhancement of Non-Permutation Binomial Power Functions to Construct Cryptographically Strong S-Boxes," *Mathematics*, vol. 11, no. 2, p. 446, 2023, doi: 10.3390/math11020446.

[141] H. Muhammad Waseem and S. O. Hwang, "Design of highly nonlinear confusion component based on entangled points of quantum spin states," *Sci. Rep.*, vol. 13, no. 1, p. 1099, 2023, doi: 10.1038/s41598-023-28002-7.

[142] A. Khompysh, N. Kapalova, K. Algazy, D. Dyusenbayev, and K. Sakan, "Design of substitution nodes (S-Boxes) of a block cipher intended for preliminary encryption of confidential information," *Cogent Eng.*, vol. 9, no. 1, 2022, doi: 10.1080/23311916.2022.2080623.

[143] Y. Su, X. Tong, M. Zhang, and Z. Wang, "A new S-box three-layer optimization method and its application," *Nonlinear Dyn.*, vol. 111, no. 3, pp. 2841–2867, 2023, doi: 10.1007/s11071-022-07956-9.

[144] S. Zhou, Y. Qiu, X. Wang, and Y. Zhang, "Novel image cryptosystem based on new 2D hyperchaotic map and dynamical chaotic S-box," *Nonlinear Dyn.*, vol. 111, no. 10, pp. 9571–9589, 2023, doi: 10.1007/s11071-023-08312-1.

[145] S. Abdullah, A. O. Almagrabi, and I. Ullah, "A New Approach to Artificial Intelligent Based Three-Way Decision Making and Analyzing S-Box Image Encryption Using TOPSIS Method," *Mathematics*, vol. 11, no. 6, 2023, doi: 10.3390/math11061559.

[146] J. Chapmann, *Neural networks: Introduction to artificial neurons, backpropagation algorithms and multilayer feedforward networks*, vol. 2. 2017.

[147] K. L. Du and M. N. S. Swamy, *Neural network Design*. 2006. [Online]. Available: http://scholar.google.com/scholar?hl=en&sugexp=gsih&pq=badminton+training&xhr=t&q=neural+network+design&cp=16&qe=bmV1cmFsIG5ldHdvcmsgZA&qesig=k9_6OUSCnOMtzbLRV7Bxag&pkc=AFgZ2tnXZWxdMzsRdm7bQlAZ9Ouzahw-8F-Iap-NFqR9QR-QaxLC0MI5wrX4F_gMeseaytVjRLbReEMmERZgMf

[148] S. Farwa, T. Shah, and L. Idrees, "A highly nonlinear S-box based on a fractional linear transformation," *Springerplus*, vol. 5, no. 1, 2016, doi: 10.1186/s40064-016-3298-7.

[149] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, "A projective general linear group based algorithm for the construction of substitution box for block ciphers," *Neural Comput. Appl.*, vol. 22, no. 6, pp. 1085–1093, 2013, doi: 10.1007/s00521-012-0870-0.

[150] A. Alghafis, N. Munir, and M. Khan, “An encryption scheme based on chaotic Rabinovich-Fabrikant system and S8 confusion component,” *Multimed. Tools Appl.*, vol. 80, no. 5, pp. 7967–7985, 2021, doi: 10.1007/s11042-020-10142-x.

[151] A. H. Zahid, M. J. Arshad, and M. Ahmad, “A novel construction of efficient substitution-boxes using cubic fractional transformation,” *Entropy*, vol. 21, no. 3, pp. 1–13, 2019, doi: 10.3390/e21030245.

[152] F. Artuğer and F. Özkaynak, “SBOX-CGA: substitution box generator based on chaos and genetic algorithm,” *Neural Comput. Appl.*, 2022, doi: 10.1007/s00521-022-07589-4.

[153] N. Hematpour, S. Ahadpour, and S. Behnia, “Presence of dynamics of quantum dots in the digital signature using DNA alphabet and chaotic S-box,” *Multimed. Tools Appl.*, vol. 80, no. 7, pp. 10509–10531, 2021, doi: 10.1007/s11042-020-10059-5.

[154] I. Shahzad, Q. Mushtaq, and A. Razaq, “Construction of New S-Box Using Action of Quotient of the Modular Group for Multimedia Security,” *Secur. Commun. Networks*, vol. 2019, 2019, doi: 10.1155/2019/2847801.

[155] E. S. Abuelyamam, “Residues of prime numbers as entries for the S-Box,” *Proc. - 2013 Int. Conf. Comput. Electr. Electron. Eng. ’Research Makes a Differ. ICCEEE 2013*, pp. 584–588, 2013, doi: 10.1109/ICCEEE.2013.6634005.

[156] A. H. Zahid, E. Al-Solami, and M. Ahmad, “A Novel Modular Approach Based Substitution-Box Design for Image Encryption,” *IEEE Access*, vol. 8, pp. 150326–150340, 2020, doi: 10.1109/ACCESS.2020.3016401.

[157] M. Ramzan, T. Shah, M. M. Hazzazi, A. Aljaedi, and A. R. Alharbi, “Construction of S-Boxes Using Different Maps over Elliptic Curves for Image Encryption,” *IEEE Access*, vol. 9, pp. 157106–157123, 2021, doi: 10.1109/ACCESS.2021.3128177.

[158] M. Niemiec and L. MacHowski, “A new symmetric block cipher based on key-dependent S-boxes,” *Int. Congr. Ultra Mod. Telecommun. Control Syst. Work.*, pp. 474–478, 2012, doi: 10.1109/ICUMT.2012.6459712.

[159] 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, 2005, doi: 10.1016/j.chaos.2004.04.023.

[160] A. Razaq, S. Akhter, A. Yousaf, U. Shuaib, and M. Ahmad, “A group theoretic construction of highly nonlinear substitution box and its applications in image encryption,” *Multimed. Tools Appl.*, vol. 81, no. 3, pp. 4163–4184, 2022, doi: 10.1007/s11042-021-11635-z.

[161] A. Razaq, A. Ullah, H. Alolaiyan, and A. Yousaf, “A Novel Group Theoretic and Graphical Approach for Designing Cryptographically Strong Nonlinear Components of Block Ciphers,” *Wirel. Pers. Commun.*, vol. 116, no. 4, pp. 3165–3190, 2021, doi: 10.1007/s11277-020-07841-x.

[162] A. Razaq, A. Yousaf, U. Shuaib, N. Siddiqui, A. Ullah, and A. Waheed, “A Novel Construction of Substitution Box Involving Coset Diagram and a Bijective Map,” *Secur. Commun. Networks*, vol. 2017, 2017, doi: 10.1155/2017/5101934.

[163] A. Razaq, Iqra, M. Ahmad, M. A. Yousaf, and S. Masood, “A novel finite rings based algebraic scheme of evolving secure S-boxes for images encryption,” *Multimed. Tools Appl.*, vol. 80, no. 13, pp. 20191–20215, 2021, doi: 10.1007/s11042-021-10587-8.

[164] A. Razaq *et al.*, “A Novel Method for Generation of Strong Substitution-Boxes Based on Coset Graphs and Symmetric Groups,” *IEEE Access*, vol. 8, pp. 75473–75490, 2020, doi: 10.1109/ACCESS.2020.2989676.

[165] A. Razaq, H. A. Al-Olayan, A. Ullah, A. Riaz, and A. Waheed, “A Novel Technique for the Construction of Safe Substitution Boxes Based on Cyclic and Symmetric Groups,” *Secur. Commun. Networks*, vol. 2018, 2018, doi: 10.1155/2018/4987021.

[166] A. H. Zahid and M. J. Arshad, “An innovative design of substitution-boxes using cubic polynomial mapping,” *Symmetry (Basel).*, vol. 11, no. 3, 2019, doi: 10.3390/sym11030437.

[167] A. Waheed, F. Subhan, M. M. Suud, Y. H. Malik, and E. Al., “Construction of nonlinear component of block cipher using coset graph,” *AIMS Math.*, vol. 8, no. 9, pp. 21644–21667, 2023, doi: 10.3934/math.20231104.

[168] 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, 2016, doi: 10.1007/s11277-016-3436-0.

[169] Y. Tian, Q. Liu, D. Liu, Y. Kang, P. Deng, and F. He, “Updates to Grasselli’s Peak Shear Strength Model,” *Rock Mech. Rock Eng.*, vol. 51, no. 7, pp. 2115–2133, 2018, doi: 10.1007/s00603-018-1469-2.

[170] G. A. Gakam Tegue *et al.*, “A Novel Image Encryption Scheme Combining a Dynamic S-Box Generator and a New Chaotic Oscillator with Hidden Behavior,” *Arab. J. Sci. Eng.*, vol. 48, no. 8, pp. 10653–10672, 2023, doi: 10.1007/s13369-023-07715-x.

[171] L. Wang, Y. Cao, H. Jahanshahi, Z. Wang, and J. Mou, “Color image encryption algorithm based on Double layer Josephus scramble and laser chaotic system,” *Optik (Stuttg).*, vol. 275, 2023, doi: 10.1016/j.ijleo.2023.170590.

[172] W. Alexan, N. Alexan, and M. Gabr, “Multiple-Layer Image Encryption Utilizing Fractional-Order Chen Hyperchaotic Map and Cryptographically Secure PRNGs,” *Fractal Fract.*, vol. 7, no. 4, 2023, doi: 10.3390/fractalfract7040287.

[173] Z. H. Guan, F. Huang, and W. Guan, “Chaos-based image encryption algorithm,” *Phys. Lett. Sect. A Gen. At. Solid State Phys.*, vol. 346, no. 1–3, pp. 153–157, 2005, doi: 10.1016/j.physleta.2005.08.006.

[174] J. Bian *et al.*, “A true random number generator based on double threshold-switching memristors for image encryption,” *Appl. Phys. Lett.*, vol. 122, no. 19, 2023, doi: 10.1063/5.0145875.

[175] Q. Liang and C. Zhu, “A new one-dimensional chaotic map for image encryption scheme based on random DNA coding,” *Opt. Laser Technol.*, vol. 160, 2023, doi: 10.1016/j.optlastec.2022.109033.

[176] W. Zhao, Z. Chang, C. Ma, and Z. Shen, “A Pseudorandom Number Generator Based on the Chaotic Map and Quantum Random Walks,” *Entropy*, vol. 25, no. 1, 2023, doi:

10.3390/e25010166.

[177] D. Das and C. Pradhan, “Image Encryption Based on Cyclic Chaos, PRNG and Arnold’s Cat Map,” in *Lecture Notes in Networks and Systems*, 2023, pp. 281–291. doi: 10.1007/978-981-19-7615-5_25.

[178] Chaos and Cryptography, “Baker’s map || Chaotic map || Generate chaotic keys || Generate prime numbers [Video].” 2021. [Online]. Available: https://www.youtube.com/watch?v=3jNZBVq_Za4&t=158s

[179] Chaos and Cryptography, “PRNG with Zaslavasky Map || Pseudo Random Number Generator [Video].” 2021. [Online]. Available: https://www.youtube.com/watch?v=5B_bVNg8QWw&t=21s

[180] Chaos and Cryptography, “Generation to chaotic values of Henon Map || 2D chaotic map [Video].” 2021. [Online]. Available: https://www.youtube.com/watch?v=TE7n8ZsGoRg

[181] J. Wang, Y. Yang, T. Wang, R. Simon Sherratt, and J. Zhang, “Big data service architecture: A survey,” *J. Internet Technol.*, vol. 21, no. 2, pp. 393–405, 2020, doi: 10.3966/160792642020032102008.

[182] J. Zhang, S. Zhong, T. Wang, H. C. Chao, and J. Wang, “Blockchain-based Systems and Applications: A survey,” *J. Internet Technol.*, vol. 21, no. 1, pp. 1–14, 2020, doi: 10.3966/160792642020012101001.

[183] H. H. Bu, N. C. Kim, K. W. Park, and S. H. Kim, “Content-based image retrieval using combined texture and color features based on multi-resolution multi-direction filtering and color autocorrelogram,” *J. Ambient Intell. Humaniz. Comput.*, 2019, doi: 10.1007/s12652-019-01466-0.

[184] Z. A. Abduljabbar *et al.*, “Provably Secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map,” *IEEE Access*, vol. 10, pp. 26257–26270, 2022, doi: 10.1109/ACCESS.2022.3151174.

[185] N. Guisande, M. P. Di Nunzio, N. Martinez, O. A. Rosso, and F. Montani, “Chaotic dynamics of the Hénon map and neuronal input-output: A comparison with neurophysiological data,” *Chaos*, vol. 33, no. 4, 2023, doi: 10.1063/5.0142773.

[186] H. Alhumyani, “Dual Image Cryptosystem Using Henon Map and Discrete Fourier Transform,” *Intell. Autom. Soft Comput.*, vol. 36, no. 3, pp. 2933–2945, 2023, doi: 10.32604/iasc.2023.034689.

[187] M. A. Midoun, X. Wang, and M. Z. Talhaoui, “A sensitive dynamic mutual encryption system based on a new 1D chaotic map,” *Opt. Lasers Eng.*, vol. 139, 2021, doi: 10.1016/j.optlaseng.2020.106485.

[188] X. Gao, “Image encryption algorithm based on 2D hyperchaotic map,” *Opt. Laser Technol.*, vol. 142, 2021, doi: 10.1016/j.optlastec.2021.107252.

[189] X. Liu, X. Tong, Z. Wang, and M. Zhang, “A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its’ applications in image encryption,” *Chaos, Solitons and Fractals*, vol. 154, 2022, doi: 10.1016/j.chaos.2021.111693.

[190] A. Arab, M. J. Rostami, and B. Ghavami, “An image encryption method based on chaos system and AES algorithm,” *J. Supercomput.*, vol. 75, no. 10, pp. 6663–6682, 2019, doi: 10.1007/s11227-019-02878-7.

[191] X. Liu, X. Tong, M. Zhang, and Z. Wang, “A highly secure image encryption algorithm based on conservative hyperchaotic system and dynamic biogenetic gene algorithms,” *Chaos, Solitons and Fractals*, vol. 171, 2023, doi: 10.1016/j.chaos.2023.113450.

[192] M. Akraam, T. Rashid, and S. Zafar, “An image encryption scheme proposed by modifying chaotic tent map using fuzzy numbers,” *Multimed. Tools Appl.*, vol. 82, no. 11, pp. 16861–16879, 2023, doi: 10.1007/s11042-022-13941-6.

[193] M. Zhao, H. Liu, and Y. Niu, “Batch generating keyed strong S-Boxes with high nonlinearity using 2D hyper chaotic map,” *Integration*, vol. 92, pp. 91–98, 2023, doi: 10.1016/j.vlsi.2023.05.006.

[194] T. Shah, M. U. Safdar, A. Ali, and T. ul Haq, “Color image encryption by a non-chain Galois ring extension,” *Phys. Scr.*, vol. 98, no. 12, 2023, doi: 10.1088/1402-4896/ad0bba.

[195] Y. Liu, X. Tong, and J. Ma, “Image encryption algorithm based on hyper-chaotic system and dynamic S-box,” *Multimed. Tools Appl.*, vol. 75, no. 13, pp. 7739–7759, 2016, doi: 10.1007/s11042-015-2691-5.

[196] B. Idrees, S. Zafar, T. Rashid, and W. Gao, “Image encryption algorithm using S-box and dynamic Hénon bit level permutation,” *Multimed. Tools Appl.*, vol. 79, no. 9–10, pp. 6135–6162, 2020, doi: 10.1007/s11042-019-08282-w.

[197] M. U. Safdar, T. Shah, A. Ali, and T. ul Haq, “Construction of algebraic complex 9-bit lookup tables using non-chain-ring and its applications in data security,” *Integration*, vol. 94, 2024, doi: 10.1016/j.vlsi.2023.102095.

[198] H. Wen and Y. Lin, “Cryptanalysis of an image encryption algorithm using quantum chaotic map and DNA coding,” *Expert Syst. Appl.*, vol. 237, 2024, doi: 10.1016/j.eswa.2023.121514.

[199] X. Liu, X. Tong, Z. Wang, and M. Zhang, “Efficient high nonlinearity S-box generating algorithm based on third-order nonlinear digital filter,” *Chaos, Solitons and Fractals*, vol. 150, 2021, doi: 10.1016/j.chaos.2021.111109.

[200] X. Tong, L. Cheng, Z. Wang, and M. Zhang, “Design of S-box multi-objective optimization algorithm based on combined chaotic system,” *Phys. Scr.*, vol. 99, no. 2, 2024, doi: 10.1088/1402-4896/ad1282.

[201] A. G. Mohamed, N. O. Korany, and S. E. El-Khamy, “New DNA Coded Fuzzy Based (DNAFZ) S-Boxes: Application to Robust Image Encryption Using Hyper Chaotic Maps,” *IEEE Access*, vol. 9, pp. 14284–14305, 2021, doi: 10.1109/ACCESS.2021.3052161.

[202] H. Nejati, A. Beirami, and W. H. Ali, “Discrete-time chaotic-map truly random number generators: Design, implementation, and variability analysis of the zigzag map,” *Analog Integr. Circuits Signal Process.*, vol. 73, no. 1, pp. 363–374, 2012, doi: 10.1007/s10470-012-9893-9.

[203] S. Chen, S. Feng, W. Fu, and Y. Zhang, “Logistic map: Stability and entrance to chaos,” in *Journal of Physics: Conference Series*, 2021. doi: 10.1088/1742-6596/2014/1/012009.

[204] K. Iskakova, M. M. Alam, S. Ahmad, S. Saifullah, A. Akgül, and G. Yılmaz, “Dynamical study of a novel 4D hyperchaotic system: An integer and fractional order analysis,” *Math. Comput. Simul.*, vol. 208, pp. 219–245, 2023, doi: 10.1016/j.matcom.2023.01.024.

[205] J. Daemen and V. Rijmen, “AES proposal: Rijndael,” no. October 1999, 1999.

[206] I. Hussain, T. Shah, M. A. Gondal, W. A. Khan, and H. Mahmood, “A group theoretic approach to construct cryptographically strong substitution boxes,” *Neural Comput. Appl.*, vol. 23, no. 1, pp. 97–104, 2013, doi: 10.1007/s00521-012-0914-5.

[207] O. S. Faragallah *et al.*, “Secure color image cryptosystem based on chaotic logistic in the FrFT domain,” *Multimed. Tools Appl.*, vol. 79, no. 3–4, pp. 2495–2519, 2020, doi: 10.1007/s11042-019-08190-z.

[208] M. Ahmad, M. N. Doja, and M. M. S. Beg, “Security analysis and enhancements of an image cryptosystem based on hyperchaotic system,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 1, pp. 77–85, 2021, doi: 10.1016/j.jksuci.2018.02.002.

[209] X. Wang, L. Liu, and Y. Zhang, “A novel chaotic block image encryption algorithm based on dynamic random growth technique,” *Opt. Lasers Eng.*, vol. 66, pp. 10–18, 2015, doi: 10.1016/j.optlaseng.2014.08.005.

[210] X. Wu, D. Wang, J. Kurths, and H. Kan, “A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system,” *Inf. Sci. (Ny).*, vol. 349–350, pp. 137–153, 2016, doi: 10.1016/j.ins.2016.02.041.

[211] J. Amreen and S. Naduvath, “Coset component signed graph of a group,” *Discret. Math. Algorithms Appl.*, vol. 16, no. 3, 2024, doi: 10.1142/S1793830923500313.

[212] T. Kaufman and I. Oppenheim, “High dimensional expanders and coset geometries,” *Eur. J. Comb.*, vol. 111, 2023, doi: 10.1016/j.ejc.2023.103696.

[213] S. Sing, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Vintage; Reprint edition (August 29, 2000), 2000.

[214] C. Paar and J. Pelzl, “Understanding Cryptography,” *Underst. Cryptogr.*, 2010, doi: 10.1007/978-3-642-04101-3.

[215] B. Johnson, *BREAK THE CODE Cryptography for Beginners*. Courier Corporation, 2013.

[216] T. Shah and A. Qureshi, “S-box on subgroup of galois field,” *Cryptography*, vol. 3, no. 2, pp. 1–9, 2019, doi: 10.3390/cryptography3020013.

[217] M. Asif, S. Mairaj, Z. Saeed, M. U. Ashraf, K. Jambi, and R. M. Zulqarnain, “A Novel Image Encryption Technique Based on Mobius Transformation,” *Comput. Intell. Neurosci.*, vol. 2021, pp. 1–14, 2021, doi: 10.1155/2021/1912859.

[218] B. Fine and G. Rosenberger, “Fields and Field Extensions,” no. part 2, pp. 74–103,

1997, doi: 10.1007/978-1-4612-1928-6_6.

[219] A. Broumandnia, “Image encryption algorithm based on the finite fields in chaotic maps,” *J. Inf. Secur. Appl.*, vol. 54, 2020, doi: 10.1016/j.jisa.2020.102553.

[220] C. Chen, K. Sun, and S. He, “An improved image encryption algorithm with finite computing precision,” *Signal Processing*, vol. 168, 2020, doi: 10.1016/j.sigpro.2019.107340.

[221] Q. Huynh-Thu and M. Ghanbari, “Scope of validity of PSNR in image/video quality assessment,” *Electron. Lett.*, vol. 44, no. 13, pp. 800–801, 2008, doi: 10.1049/el:20080522.

[222] Z. Wang and A. C. Bovik, “A universal image quality index,” *IEEE Signal Process. Lett.*, vol. 9, no. 3, pp. 81–84, 2002, doi: 10.1109/97.995823.

[223] S. Jahangir, “Algebra and Chaos based Nonlinear Block Cipher Component Designing and Their Applications to Image Encryption,” 2021.

[224] Y. Shen, J. Huang, L. Chen, T. Wen, T. Li, and G. Zhang, “Fast and Secure Image Encryption Algorithm with Simultaneous Shuffling and Diffusion Based on a Time-Delayed Combinatorial Hyperchaos Map,” *Entropy*, vol. 25, no. 5, 2023, doi: 10.3390/e25050753.

[225] P. K. Naskar, S. Bhattacharyya, K. C. Mahatab, K. G. Dhal, and A. Chaudhuri, “An efficient block-level image encryption scheme based on multi-chaotic maps with DNA encoding,” *Nonlinear Dyn.*, vol. 105, no. 4, pp. 3673–3698, 2021, doi: 10.1007/s11071-021-06761-0.

[226] X. Chai, K. Yang, and Z. Gan, “A new chaos-based image encryption algorithm with dynamic key selection mechanisms,” *Multimed. Tools Appl.*, vol. 76, no. 7, pp. 9907–9927, 2017, doi: 10.1007/s11042-016-3585-x.

[227] A. Toktas, U. Erkan, and D. Ustun, “An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm,” *Nonlinear Dyn.*, vol. 105, no. 2, pp. 1885–1909, 2021, doi: 10.1007/s11071-021-06675-x.

[228] S. Zhu and C. Zhu, “Security analysis and improvement of an image encryption cryptosystem based on bit plane extraction and multi chaos,” *Entropy*, vol. 23, no. 5, 2021, doi: 10.3390/e23050505.

[229] T. Haider, N. A. Azam, and U. Hayat, “A Novel Image Encryption Scheme Based on ABC Algorithm and Elliptic Curves,” *Arab. J. Sci. Eng.*, vol. 48, no. 8, pp. 9827–9847, 2023, doi: 10.1007/s13369-022-07383-3.

[230] M. T. Elkandoz and W. Alexan, “Image encryption based on a combination of multiple chaotic maps,” *Multimed. Tools Appl.*, vol. 81, no. 18, pp. 25497–25518, 2022, doi: 10.1007/s11042-022-12595-8.

[231] R. Wu *et al.*, “AEA-NCS: An audio encryption algorithm based on a nested chaotic system,” *Chaos, Solitons and Fractals*, vol. 165, 2022, doi: 10.1016/j.chaos.2022.112770.

[232] S. Gao *et al.*, “Asynchronous Updating Boolean Network Encryption Algorithm,”

IEEE Trans. Circuits Syst. Video Technol., vol. 33, no. 8, pp. 4388–4400, 2023, doi: 10.1109/TCSVT.2023.3237136.

[233] J. Xu, C. Zhao, and J. Mou, "A 3D Image Encryption Algorithm Based on the Chaotic System and the Image Segmentation," *IEEE Access*, vol. 8, pp. 145995–146005, 2020, doi: 10.1109/ACCESS.2020.3005925.

[234] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, and X. Tang, "EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory," *Inf. Sci. (Ny).*, vol. 621, pp. 766–781, 2023, doi: 10.1016/j.ins.2022.11.121.

[235] S. Gao *et al.*, "A 3D model encryption scheme based on a cascaded chaotic system," *Signal Processing*, vol. 202, 2023, doi: 10.1016/j.sigpro.2022.108745.

[236] W. Stallings, "Cryptography and network security : principles and practice / William Stallings.," *Pers. Educ. Inc*, p. 752, 2016, [Online]. Available: http://spydus8.nmit.vic.edu.au:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat00793a&AN=nmit.86859&site=eds-live

[237] A. K. Hassan Sedeeg, "An Application of the New Integral 'Aboodh Transform' in Cryptography," *Pure Appl. Math. J.*, vol. 5, no. 5, p. 151, 2016, doi: 10.11648/j.pamj.20160505.12.

[238] Subiono, J. Cahyono, D. Adzkiya, and B. Davvaz, "A cryptographic algorithm using wavelet transforms over max-plus algebra," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 3, pp. 627–635, 2022, doi: 10.1016/j.jksuci.2020.02.004.

[239] S. Tedmori and N. Al-Najdawi, "Image cryptographic algorithm based on the Haar wavelet transform," *Inf. Sci. (Ny).*, vol. 269, pp. 21–34, 2014, doi: 10.1016/j.ins.2014.02.004.

[240] D. R. L. Brown and C. Research, "SEC 2: Recommended Elliptic Curve Domain Parameters," *Stand. Effic. Cryptogr.*, vol. 2, no. Sec 2, p. 33, 2010, [Online]. Available: http://www.secg.org/sec2-v2.pdf

[241] I. Ullah, N. A. Azam, and U. Hayat, "Efficient and secure substitution box and random number generators over Mordell elliptic curves," *J. Inf. Secur. Appl.*, vol. 56, 2021, doi: 10.1016/j.jisa.2020.102619.

[242] G. Murtaza, N. A. Azam, and U. Hayat, "Designing an Efficient and Highly Dynamic Substitution-Box Generator for Block Ciphers Based on Finite Elliptic Curves," *Secur. Commun. Networks*, vol. 2021, 2021, doi: 10.1155/2021/3367521.

[243] M. A. M. Khan, N. A. Azam, U. Hayat, and H. Kamarulhaili, "A novel deterministic substitution box generator over elliptic curves for real-time applications," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 1, pp. 219–236, 2023, doi: 10.1016/j.jksuci.2022.11.012.

[244] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Processing*, vol. 187, p. 108144, 2021, doi: 10.1016/j.sigpro.2021.108144.

[245] U. Hayat, N. A. Azam, H. R. Gallegos-Ruiz, S. Naz, and L. Batool, "A Truly Dynamic Substitution Box Generator for Block Ciphers Based on Elliptic Curves Over Finite

Rings," *Arab. J. Sci. Eng.*, vol. 46, no. 9, pp. 8887–8899, 2021, doi: 10.1007/s13369-021-05666-9.

[246] S. Azhar, N. A. Azam, and U. Hayat, "Text Encryption Using Pell Sequence and Elliptic Curves with Provable Security," *Comput. Mater. Contin.*, vol. 71, no. 2, pp. 4971–4988, 2022, doi: 10.32604/cmc.2022.023685.

[247] L. Liu and J. Wang, "A cluster of 1D quadratic chaotic map and its applications in image encryption," *Math. Comput. Simul.*, vol. 204, pp. 89–114, 2023, doi: 10.1016/j.matcom.2022.07.030.

[248] A. Naguib, W. El-Shafai, and M. Shokair, "Performance evaluation of an encrypted color image transmission over wireless network with different chaotic-based techniques," *J. Opt.*, vol. 52, no. 4, pp. 2275–2284, 2023, doi: 10.1007/s12596-023-01093-1.

[249] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map," *Appl. Math. Comput.*, vol. 442, p. 127738, 2023, doi: 10.1016/j.amc.2022.127738.

[250] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik (Stuttg).*, vol. 272, p. 170316, 2023, doi: 10.1016/j.ijleo.2022.170316.

[251] F. ul Islam and G. Liu, "Designing S-Box Based on 4D-4Wing Hyperchaotic System," *3D Res.*, vol. 8, no. 1, 2017, doi: 10.1007/s13319-017-0119-x.

[252] S. Liu, Q. Wang, C. Liu, Y. Sun, and L. He, "Natural Exponential and Three-Dimensional Chaotic System," *Adv. Sci.*, vol. 10, no. 15, Mar. 2023, doi: 10.1002/advs.202204269.

[253] N. A. Azam, G. Murtaza, and U. Hayat, "A novel image encryption scheme based on elliptic curves and coupled map lattices," *Optik (Stuttg).*, vol. 274, p. 170517, 2023, doi: 10.1016/j.ijleo.2023.170517.

[254] D. Wei, M. Jiang, and Y. Deng, "A secure image encryption algorithm based on hyper-chaotic and bit-level permutation," *Expert Syst. Appl.*, vol. 213, p. 119074, 2023, doi: 10.1016/j.eswa.2022.119074.

[255] M. Ganavi, "Two-Layer Security of Images Using Elliptic Curve Cryptography with Discrete Wavelet Transform," vol. 15, no. 2, pp. 31–47, 2023, doi: 10.5815/ijcnis.2023.02.03.

[256] M. Gupta, V. P. Singh, K. K. Gupta, and P. K. Shukla, "An efficient image encryption technique based on two-level security for internet of things," *Multimed. Tools Appl.*, vol. 82, no. 4, pp. 5091–5111, 2023, doi: 10.1007/s11042-022-12169-8.

[257] S. Sabir and V. Guleria, "Multi-layer security based multiple image encryption technique," *Comput. Electr. Eng.*, vol. 106, p. 108609, 2023, doi: 10.1016/j.compeleceng.2023.108609.

[258] D. E. Mfungo, X. Fu, X. Wang, and Y. Xian, "Enhancing Image Encryption with the Kronecker xor Product, the Hill Cipher, and the Sigmoid Logistic Map," *Appl. Sci.*, vol. 13, no. 6, p. 4034, 2023, doi: 10.3390/app13064034.

[259] S. W. Jirjees, N. A. Yousif, and A. T. Hashim, “Colour Image Privacy Based on Cascaded Design of Symmetric Block Cipher,” *J. Eng. Sci. Technol.*, vol. 17, no. 3, pp. 2135–2156, 2022.

[260] **柴秀**丽, **甘志**华, **路**杨, 张苗辉, and 陈怡然, “A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system,” *Chinese Phys. B*, vol. 10, 2016.

[261] J. Wu, X. Liao, and B. Yang, “Color image encryption based on chaotic systems and elliptic curve ElGamal scheme,” *Signal Processing*, vol. 141, pp. 109–124, 2017, doi: 10.1016/j.sigpro.2017.04.006.

[262] 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.

[263] A. Waheed and F. Subhan, “S-box design based on logistic skewed chaotic map and modified Rabin-Karp algorithm: applications to multimedia security,” *Phys. Scr.*, vol. 99, no. 5, p. 055236, 2024, doi: 10.1088/1402-4896/ad3991.

[264] D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, “A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information,” *Appl. Sci.*, vol. 13, no. 12, p. 7113, 2023, doi: 10.3390/app13127113.

[265] M. Tanveer *et al.*, “Multi-Images Encryption Scheme Based on 3D Chaotic Map and Substitution Box,” *IEEE Access*, vol. 9, pp. 73924–73937, 2021, doi: 10.1109/ACCESS.2021.3081362.

[266] Z. Liu, C. Wu, J. Wang, and Y. Hu, “A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-Chaos,” *IEEE Access*, vol. 7, pp. 78367–78378, 2019, doi: 10.1109/ACCESS.2019.2922376.

[267] T. Wang and M. hui Wang, “Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding,” *Opt. Laser Technol.*, vol. 132, p. 106355, 2020, doi: 10.1016/j.optlastec.2020.106355.

[268] J. Wu, X. Liao, and B. Yang, “Image encryption using 2D Hénon-Sine map and DNA approach,” *Signal Processing*, vol. 153, pp. 11–23, 2018, doi: 10.1016/j.sigpro.2018.06.008.

APPENDIX A

LIST OF PUBLICATIONS

1. A. Waheed, F. Subhan, M. Mohd Su'ud, and M. Mansoor Alam, "Molding robust S-box design based on linear fractional transformation and multilayer Perceptron: Applications to multimedia security," Egypt. Informatics J., vol. 26, no. 3, p. 100480, 2024, doi: 10.1016/j.eij.2024.100480.

2. A. Waheed, F. Subhan, M. M. Suud, M. Alam, and S. Ahmad, "An analytical review of current S-box design methodologies, performance evaluation criteria, and major challenges," Multimed. Tools Appl., vol. 82, no. 19, pp. 29689–29712, 2023, doi: 10.1007/s11042-023-14910-3.

3. A. Waheed, F. Subhan, M. M. Suud, M. Mansoor Alam, and S. Haider, "Design and optimization of nonlinear component of block cipher: Applications to multimedia security," Ain Shams Eng. J., vol. 15, no. 3, p. 102507, 2023, doi: 10.1016/j.asej.2023.102507.

4. A. Waheed and F. Subhan, "S-box design based on logistic skewed chaotic map and modified Rabin-Karp algorithm: applications to multimedia security," Phys. Scr., vol. 99, no. 5, p. 055236, 2024, doi: 10.1088/1402-4896/ad3991.

5. A. Waheed, F. Subhan, M. M. Suud, Y. H. Malik, and E. Al., "Construction of nonlinear component of block cipher using coset graph," AIMS Math., vol. 8, no. 9, pp. 21644–21667, 2023, doi: 10.3934/math.20231104.