A NEW MULTIPLE IMAGE ENCRYPTION SCHEME BASED ON CHAOTIC SYSTEMS

By
ZOHAIB ASGHER

4.5 cm

DEPARTMENT OF MATHEMATICS
NATIONAL UNIVERSITY OF MODERN LANGUAGES
ISLAMABAD

January, 2026

A NEW MULTIPLE IMAGE ENCRYPTION SCHEME BASED ON CHAOTIC SYSTEMS

By

ZOHAIB ASGHER

Supervised By
DR. GHULAM MURTAZA

MS Mathematics, National University of Modern Languages, Islamabad, 2025

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

MASTER OF SCIENCE
In **Mathematics**

To
DEPARTMENT OF MATHEMATICS
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: A New Multiple Image Encryption Scheme Based on Chaotic Systems

Submitted By: Zohaib Asgher **Registration #:** 73 MS/Math/F22

Master of Science in Mathematics (MS Math)
Title of the Degree

Mathematics
Name of Discipline

Dr. Ghulam Murtaza _____
Name of Research Supervisor Signature of Research Supervisor

Dr. Anum Naseem _____
Name of HOD (Math) Signature of HOD (Math)

Dr. Noman Malik _____
Name of Dean (FEC) Signature of Dean (FEC)

2 January, 2026

AUTHOR'S DECLARATION

I Zohaib Asgher

Son of Asgher Hussain

Registration # 73 MS/Math/F22

Discipline Mathematics

Candidate of **Master of Science in Mathematics (MS Math)** at the National University of Modern Languages do hereby declare that the thesis **A New Multiple Image Encryption Scheme Based on Chaotic Systems** submitted by me in partial fulfillment of MS Mathematics 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

Zohaib Asgher
Name of Candidate

2 January, 2026
Date

ABSTRACT

Title: A New Multiple Image Encryption Scheme Based on Chaotic Systems

Due to rapid developments in communication networks, the transferring of data through these networks has increased the risk. To protect this information, data encryption plays a significant role. This work extends a single chaotic map (SC3) to encrypt batches of images concurrently while maintaining high security standards. A new multiple-image encryption scheme based on the chaotic systems is designed to encrypt batches of images more efficiently and securely. By leveraging the complex dynamics and sensitivity to initial conditions inherent in chaotic maps, the scheme achieves a high level of confusion and diffusion across multiple images. The proposed multiple-image encryption scheme provides an effective and scalable solution for secure multimedia transmission.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviation	Full Form
APCR	Adaptive Power Control Routing
ARQ	Automatic Repeat Request
ASL	Asymmetric Link
AES	Advanced Encryption Standard
DES	Data Encryption Standard
IDEA	International Data Encryption Algorithm
RNG	Random Number Generator
PRNG	Pseudo-Random Number Generator
TRNG	True Random Number Generator
NPCR	Number of Pixels Change Rate
UACI	Unified Average Changing Intensity
PSNR	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error
SC3	Sine-Cosine Cross Chaotic (Map)
MAC	Medium Access Control
NIST	National Institute of Standards and Technology
UW-ASN	Underwater Acoustic Sensor Network
MPCM	Modified Piecewise Chaotic Map

LIST OF SYMBOLS

Symbol	Description
α	Control parameter in SC3 map
β	Secondary control parameter in SC3 map
$\mu(i)$	Membership function for high-quality links
δt	High precision time step
λ	Lyapunov exponent indicating chaotic behavior
x_0, y_0	Initial conditions for SC3 map
$x_\mathrm{i}, y_\mathrm{i}$	Iterative outputs of the SC3 map
$H(m)$	Entropy of an image
K	Correlation coefficient
$P(i,j), C(i,j)$	Pixel values of plain and cipher images respectively
M, N	Dimensions of the image
$NPCR$	Number of Pixels Change Rate
$UACI$	Unified Average Changing Intensity
$PSNR$	Peak Signal-to-Noise Ratio
MSE	Mean Squared Error

ACKNOWLEDGMENT

First of all, I wish to express my gratitude and deep appreciation to Almighty Allah, who made this study possible and successful. This study would not be accomplished unless the honest espousal that was extended from several sources for which I would like to express my sincere thankfulness and gratitude. Yet, there were significant contributors for my attained success and I cannot forget their input, especially my research supervisors, Asst. Prof. Dr. Ghulam Murtaza who did not leave any stone unturned to guide me during my research journey.

I shall also acknowledge the extended assistance from the administrations of Department of Mathematics who supported me all through my research experience and simplified the challenges I faced. For all whom I did not mention but I shall not neglect their significant contribution, thanks for everything.

DEDICATION

This thesis work is dedicated to my parents and my teachers throughout my education career who have not only loved me unconditionally but whose good examples have taught me to work hard for the things that I aspire to achieve

CHAPTER 1

INTRODUCTION AND LITERATURE REVIEW

The main purpose of this introductory chapter is to review some background literature that will be discussed in the succeeding chapters. The chapter outline is as follows: The first section explains some cryptographic concepts. Section 1.2 covers the principles of cryptography. Sections 1.3 and 1.4 discuss the different types of cryptography and their purposes. Section 1.5 introduces modern cryptography tools. Section 1.6 is about cryptography and chaos. A review work is presented in the section 1.7. Section 1.8 is about the role of Random numbers in cryptography. Section 1.9 is presents thesis layout and structure.

1.1 Introduction

With rapid innovations in the development of data transmission, it has become a demanding challenge to secure confidential information from attackers or prohibitive actions [1]. Through modern multimedia technologies and telecommunications, a large amount of important information cruises in daily life by means of sharing and open networking. To transmit data across any ambiguous channel, some cryptographic techniques (encryption) are needed, which change consistent information to impenetrable form. Cryptography is a modern and valuable approaches for textual information. However, because of the high-level redundancy and capacity of bulk information, they failed to provide computational- based security [2]. More than ever, researchers are worried about how to protect multimedia data using cutting edge and practical content preservation techniques to meet this problem [3]. Digital image security encompasses a wide range of features, such as secrecy, access control, authentication, and copyright protection. Encryption, which only allows parties with the necessary decryption keys to see the sent content (plain-image), often focuses on content secrecy and access control [4]. However, a few fundamental features of images (such as high redundancy values and a huge data capacity) render such encryption techniques unsuitable for image applications. Furthermore, many encryption algorithms necessitate numerous operations on compressed data, which raises the time demand. Their low ciphering (encryption) and deciphering (decryption) times can present tremendous potential in real-time communications.

The use of image encryption is the main topic of this dissertation. The majority of encryption techniques rely heavily on chaos theory due to its great sensitivity, randomness, complexity, and

computational capacity. Compared to text data, digital images have substantial correlations between neighboring pixels, and high redundancy. The concept of employing chaos in encryption was introduced by Shannon [5]. The use of chaos in cryptography has improved security the most due to its great qualities, such as its dependence on initial conditions and sensitive behavior. The nonlinear dynamical complex systems that underpin chaos-based cryptography are straightforward but deterministic. Therefore, chaos offers quick and safe communication for data protection, which is crucial when sending multimedia data via channels with quick communication systems, such internet broadband communication.

The goal of this thesis is to create cryptosystems that employ random numbers and chaotic map to create robust encryption methods that produce ciphered images with superior qualities. From this angle, chaos-based methods and random numbers work very well. The statistical confusion diffusion qualities of the suggested ciphered images are good. Pixels in encrypted images have almost little link with one another. In summary, the encryption algorithms that are given perform well in terms of multimedia security.

1.2 Fundamentals of Cryptography

Currently, our society is strongly bounded by the domain of the information epoch, which is classified by scholar and researcher assets and is functional inside data being deliberated priceless. Enlightening data exists which is used in various forms such as economic, military, and political. The protection and security of this data during transmission, saving, and in routine practice is of prime importance because the transfer of data may result in the revelation of various marketing, financial loss, or armed forces top secrets. Credit card information, bank transactions, and social security numbers must be kept secure during transmission. For the protection and security of the data or information, cryptography plays a vivacious role [6]. Cryptography is a Greek word that means “Secret writing”. The art of personating message cryptography plays a vital role so that only its legal successor can recognize it. There are two thresholds to this course. Firstly, the plaintext, or original data, is veiled. This is recognized as encryption. The reverse procedure in which the cipher text is decoded backward into the original message must be known to the authentic recipient. This process is known as decryption. Figure 1.1 illustrates that cryptographic keys are required for both encryption and decryption.

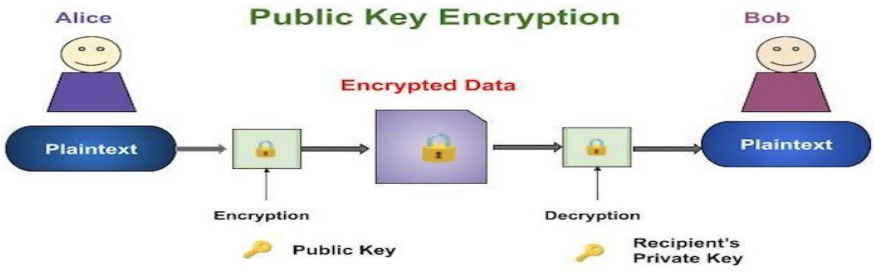


Figure 1.1: Illustration of encryption and decryption

1.3 Categories of Cryptography

Cryptography has been categorized into two forms:

1.3.1 Symmetric Key Cryptography

This category involves a person to whom the secret key should be known. Both the receiver and sender of the message may also be kept it. In private key cryptography, both the receiver and the sender each have a copy of the secret key. During this passage approach to the key is vouchsafe. There are two set-ups to ponder, in first both the interactive parties are acquainted with each other. In this situation, without any encrypting scheme, the key is shared. In the second case, familiarity is limited. For example, when seeing a secure website, keys should be swapped in a secure way [7]. Figure 1.2 classifies symmetric key cryptography into two types: block ciphers and stream ciphers.

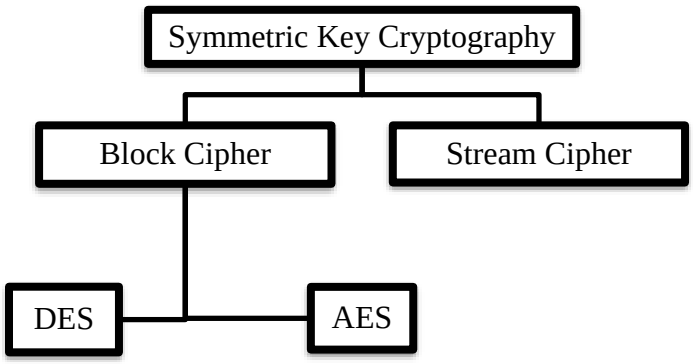


Figure 1.2: Symmetric Key Cryptography

1.3.2 Asymmetric Key Cryptography

An asymmetric key cryptography is sometimes known as 'cryptographic public key'. Asymmetric key cryptography uses two keys. One is known as the 'Public key', which may be freely transmitted over insecure channels; the other key, which can be kept hidden and not easily disseminated, is known as the 'Private key' [8].

1.4 Purposes of Cryptography

Cryptography not only plays a role in encrypting and decrypting messages, but it also used to hoist real-world complications that need safety for information or data [9]. In current cryptography, that four main purposes that arise are as follows in Figure 1.3.

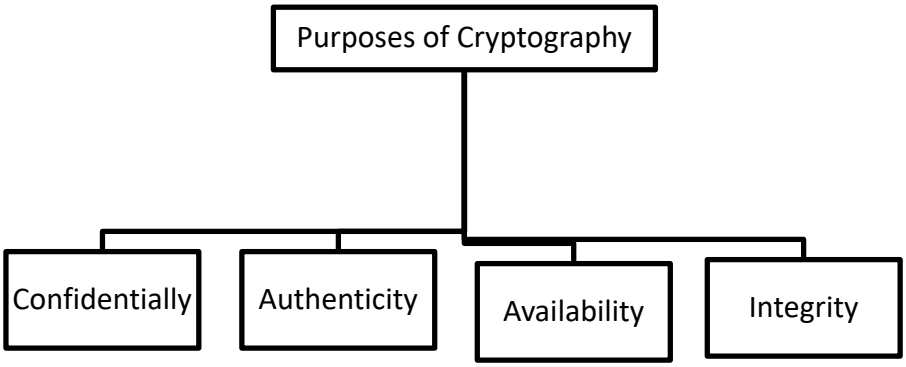


Figure 1.3: Purposes of Cryptography

1.5 Modern Cryptographic Tools

Before 1950, like an art cryptography was known, but current cryptography depends on discipline which requires provision from various fields which includes electronics, mathematics and computer science. After World War II, cryptographic research area had found the great importance by military intelligence forces. After 2 years, in 1970's the first symmetric cryptosystems i.e., public key ciphers and DES were invented. At that time, the algorithms were established with the help of computers. Then researchers recognized that worthy ciphers were established by joining small tools. These tools are substitution, permutation, diffusion and confusion [10].

1.6 Cryptography and Chaos

This section provides a very quick overview of chaotic systems. Also described are the characteristics of chaotic systems that have some bearing on cryptosystem design. This section will thus focus on the connection between encryption and chaos.

1.6.1 Chaotic System

Generally speaking, a chaotic system is any physical system that is controlled by mathematical formulas and produces behaviors that are unpredictable over time. Another name for chaos is disorder or confusion. Certain systems that undergo changes over time might occasionally exhibit chaotic motion. Thus, the two pillars of chaos theory are time and change. The graphical evaluation of that system's time series identifies the chaotic behavior. These systems are unpredictable since they

don't follow patterns. All of factors make it challenging to spot chaos in real-world issues. Nonetheless, they are seen in computer science and mathematics through the visual representation of the governing issues. Scientists are primarily drawn to chaos theory because it visualizes the complicated and disorganized behavior of a system that arises from a straightforward deterministic equation. Second, while the system in question is understandable, it is also impossible to decipher and identify from the solution trajectory.

The third pillar is the minimal prerequisite knowledge of advancing mathematics; algebra, geometry, and calculus are sufficient to comprehend the chaos. Finally, chaos can be analyzed without delving into underlying mathematical equations. These revelations surprise cryptographers and force them to use such systems to design strong cryptosystems that are harder to decipher [11, 12, 13]. Temporal chaos and spatial chaos occur when time is substituted with space and distance, respectively. The nonlinear equations that arise in differential equations or algebra are more challenging to study than linear systems. These systems also have complicated dynamics. Moreover, not all nonlinear systems have to be chaotic. Many experts believe that chaotic dynamical systems are the area of nonlinear dynamics or dynamical systems theory. Depending on energy conservation, dynamical systems fall into one of two groups. A conservative dynamical system, or friction-free system, does not lose energy. On the other hand, a dissipative system loses energy because it must endure frictional forces. When a dissipative dynamical system reaches a limiting state due to energy loss, a chaotic solution can emerge under the effect of specific constraints [14]. For continuous time intervals, a dynamical systems variations are also seen. In contrast to discrete time intervals, the measurement of such phenomena is continuous. A dynamical system's continuous change is measured using differential equations. River water movement, heat conduction, and air temperature are a few examples of such systems [14]. Differential equations are intended to be used in cyber-security to create reliable and secure systems. Nonlinear differential equation systems are used to develop the block cipher's sole nonlinear component, which can make cryptanalysis more difficult.

1.7 A Review Work

In many daily life applications such as video call conferencing, military branches, medical, communication of wireless networks images have significant role. When an image is transmitted two major issues need to be resolved, firstly check the transmitted image has assigned bandwidth and then must ensure that the images are transmitted through secure channel. So, for this purpose algorithms for encrypting images play a key role. Encryption algorithms encode the data which make it unreadable to viewer and it can be achieved by relocating or scrambling the pixel positions of image.

To secure the digital images, now a day's researchers paid attention on creating such encrypted techniques that satisfies the following properties [15]. The pixels of original and ciphered images need to be less correlated. The best encryption schemes have correlation values are near zero. The value of key space must be enormous because a larger key space number makes it more difficult for an attacker to locate the specific key. Sensitivity of key is also obligatory. In other terms, slight change of key will not decrypt the ciphered image.

Liu et al. [16], developed an encryption technique based on random numbers. Novelty of his work lies on one-time pad key generation utilizing the hash value of random noise like a digital voice recording devices. Also, the already attained chaotic system is enhanced by using this system. Because of varying input in every iteration this technique is resistant against the attacks. For key enhancement, this methodology is used, and this scheme is presented by W. Haifaa et al. [17]. The suggested scheme's keys are created by a logistic chaotic map. XOR operation is used between them and in last again XOR operation is applied between resultant and plain-image values.

With the use of density information concepts, the computing technique of DNA has high complexity. Image pixels are scrambled by permutations while the redundancy information of image is obtained by diffusion. K. Radihka et al. [18], combine sequences of DNA with chaotic maps. Image is divided in blocks then convert the decimal pixel values to binary matrices then encode them with DNA rules. After block scrambling, the sub-block division is done. In addition, DNA is added to blocks to compile the blocks again.

Eltous et al. [19], offered a color image encryption technique in which random noise is selected and then add noise signal to image after this step the image pixels are rearranged. The primary goal of this strategy is to improve efficiency and provide a high level of protection. Block-wise encryption and reordering-based encryption techniques were suggested by Khrisat et al. [20], two secret keys are used. Firstly, the image pixels are reshaped to a single-row matrix. The number of blocks is then determined, and the size of the blocks is calculated by dividing the total size of the matrix. Finally, the matrix is reordered to produce an encrypted image. For the testation of the scheme, different experimental analyses are done.

Jian et al. [21], presented an encryption system using DNA coding, quantum chaos, and the Lorenz map. To improve security, a new encryption system uses DNA four base pairs to dynamically pick eight DNA encoding rules as well as eight various forms of addition and XOR rules. The proposed scheme is tested via different statistical and experimental analyses. An innovative encryption scheme using quantum chaos is presented by Liu et al. [22], in this scheme, pixels are permuted by the Arnold

scrambling technique. For diffusion, a folding technique is utilized which modifies the diffused pixels. For high complexity and randomness, logistic and quantum chaotic maps are paired with closest-neighbor-paired lattices.

1.8 Random Number Generation (RNG)

An unpredictable sequence is known as sequence of random number. If the numbers have no correlation between them then that sequence is considered as truly random. In this way the prediction of succeeding number by using preceding is totally impossible. Distribution is the main part of any number sequence i.e., check how much the number sequences are uniformly distributed by generator. Also, the important feature of any sequence is its range [23].

1.8.1 Random Numbers Role in Cryptography

The random number sequences are used for different objectives, for example in generating keys for encryption, simulations and for modeling complexity. There are two main approaches to random number generation: true random number generators (TRNGs) and pseudo-random number generators (PRNGs). RNG is a technique/algorithm in which bits of binary sequences are generated which are independent statistically. PRNG is a deterministic technique which produce nearly random sequences of binary bits. The PRNG have input value known as seed and the output of it is known as binary sequences. RNG are commonly used in applications and cryptographic techniques. In cryptographic schemes like secret key of DES, RSA technique prime number are used for providing security. The output having length l of PRNG is not so random but it takes a small bit which is truly random and then expanded it to greater sequence. Like this, PRNG sequences could not be differentiated from truly random sequences. For the confirmation of output PRNG randomness some tests (statistical) and other analysis must be implemented. As a result, numerous statistical techniques are used to verify random and pseudorandom number generators. A comparison between among PRNG and TRNG is shown in Table 1.4, which depicts TRNG is the most suitable choice for cryptographic designs.

Table 1.4 Comparison between PRNG and TRNG

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

1.9 Structure of the Thesis

There are five chapters in the dissertation.

Chapter 1. The introduction and justifications for the planned work are given in this chapter. This chapter also provides a thorough overview of chaos theory and image encryptions. Additionally, the latest developments in image encryption are also discussed.

In Chapter 2, basic background definitions and core concepts are provided in this chapter.

In Chapter 3, the mathematical laws, equations, and theorems that underpin that critical analysis are included. The methods employed to achieve the necessary issue outcomes are also included. Every figure, table, and graph has the appropriate number and placement together with the necessary caption. It explains and analyzes the results' ramifications. A brief overview of an image encryption system based on a novel 2D sine-cosine cross-chaotic (SC3) map is provided, along with the main result.

In Chapter 4, discuss the mathematical ideas, equations, and theorems that support that critical analysis as well. This chapter introduces a new multiple-image encryption scheme based on a chaotic system. The techniques used to obtain the required issue results are also covered. In addition to the required title, each figure, table, and graph has the right number and location.

Chapter 5, Conclusions and Suggestions for the Future work.

CHAPTER 2

BASIC DEFINITIONS AND CONCEPTS

This chapter presents the core concepts, definition and mathematical foundation of cryptography and chaos focusing particularly on chaotic maps and their essential properties.

2.1 Cryptography

Cryptography is the study of transforming data into secret codes or encrypting information that should be kept private from others. From age time to the current era, during the time of war, the facility to interconnect secretly has been significant.

2.2 Plaintext and Cipher text

Any conversation within the language that we say the mortal language, which took the shape of plain text. It is implicit by the sender, receiver, and those who have approached to that message. A cipher signifies a secret or unreadable message. While any appropriate scheme is applied over the plain text to codify it, then the resulting codified message is known as cipher text.

2.3 Encryption and Decryption

The conversion of plain text transmissions into encrypted text is referred to as encryption. An inversion procedure for converting messages of cipher text behind the plain text is known as decryption.

2.4 Diffusion

To create disorder in data to make it more secure, Shannon presented two concepts confusion and diffusion for a good cryptosystem [10]. Diffusion is a technique in which if we alter a single plaintext bit it creates alternation in several cipher text bits. Similarly, alter of single bit of cipher text creates alternation in many plaintext bits. In case of block ciphers, bit alternation is communicated with the assistance of diffusion, from unique part of the block to other parts.

2.5 Confusion

Confusion produces a relationship between secret key and plain text. In confusion key is not directly related to cipher text. In general, every cipher text character should depend on many chunks of keys.

2.6 Logic Operation

AND Operation

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

inputs values 1, else it will be 0. Truth table for AND operation should be given as Table 2.1.

Table 2.1: Truth Table for AND Operation.

a	b	a ^ b
1	1	1
1	0	0
0	1	0
0	0	0

OR Operation

In this operation for both input $a, b \in T$, the output represented as $a \vee b$ has values equal to 0 for both input arguments having 0 value, otherwise it would be 1. The OR Table 2.2 is given below.

Table 2.2: Truth Table for OR Operation

a	b	a v b
1	1	1
1	0	1
0	1	1
0	0	0

XOR Operation

For both inputs a, b taken from T in XOR operation, the output values represented as $a \oplus b$ have zero value if both input values are identical, in other case they will be 1. XOR Table 2.3 should be given below.

Table2.3: Truth Table for XOR Operation

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

2.7 Chaos

In a deterministic system, a chaotic map indicates a state of unpredictability, unpredictable behavior, and sensitivity to initial conditions. Within the context of chaos theory, it describes the long-term behavior of dynamic systems that are highly sensitive to changes in their initial conditions, resulting in complex, seemingly random single patterns. Although chaotic systems are expectable,

successfully predicting chaotic systems is tough because they lack long-term predictability. Understanding and relating these complex and irregular performances is the goal of chaos research, which delivers vision into the important subtleties of complex systems in a ground of academic fields [24].

2.8 Different Properties of Chaotic Maps

The chaotic map has the following properties:

2.8.1 Sensitivity to Initial Conditions

. Chaotic maps are extremely sensitive to initial conditions, even modest changes to the starting environment. Subtle changes in initial values can cause dynamics to diverge considerably over time. They work like a butterfly effect in some cases where small changes in one place can make a big change for the other place. This butterfly effect is very essential in chaotic maps for encryption and decryption especially in cryptographic systems and as well as in cyber security and many other purposes also. Demonstration of sensitivity of initial condition is shown in Figure 2.1.

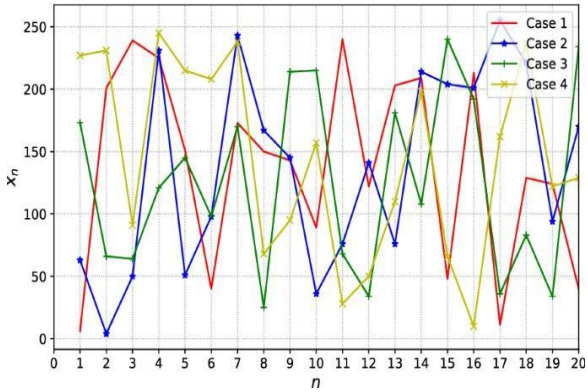


Figure 2.1: Demonstration of Sensitivity to Initial Condition of Chaotic map

2.8.2 Bifurcation

Bifurcation is a simple example of chaotic maps where a minor change in a parameter can result in a big change in the system's response. This can result in the development of chaotic regions and several coexisting attractors. Figure 2.2 illustrates the bifurcation of a logistic map.

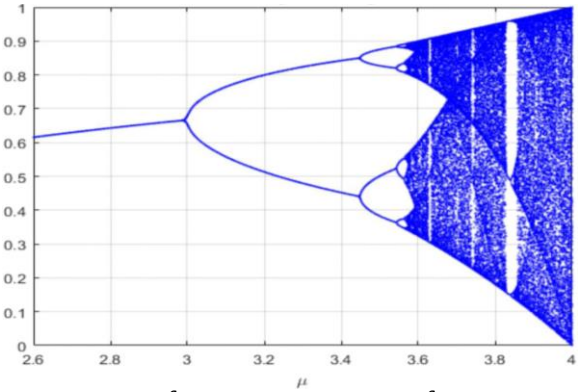


Figure2.2: Bifurcation Diagram of Logistic Map

2.8.3 Deterministic Dynamics:

Chaotic maps behave in a visionary random way, but in real, they are deterministic, which means that the governing mathematical function and their current state show both their upcoming predictions [24, 25]. The demonstration of deterministic behavior of chaotic maps is shown in Figure 2.3 below.

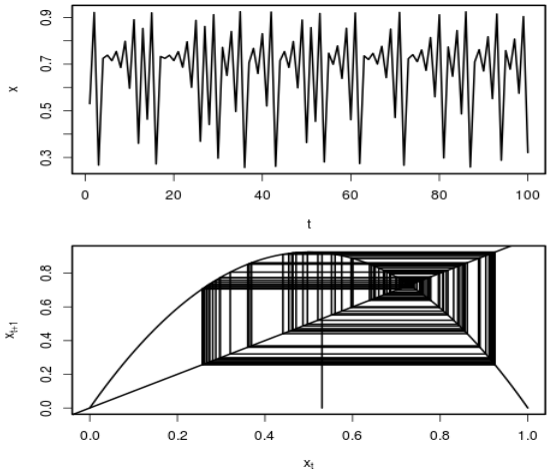


Figure 2.3: Deterministic Behavior of Chaotic maps

2.9 Type of Chaotic Maps

Here are brief details of types of chaotic maps below.

2.9.1 Logistic Map

A unit-dimensional map that shows chaotic behavior is known as logistic map. It is defined by the relation, where r is a control parameter and $\boldsymbol{x_n}$ is the current value. Equation 2.1 describes the logistic map.

$$\mathbf{x_{n+1}} = \mathbf{r x_n (1 - x_n)} \qquad 2.1)$$

Where r ranges from 0 to 4 and x is 0 to 1 [26]. Figure 2.4 is a demonstration of a logistic map.

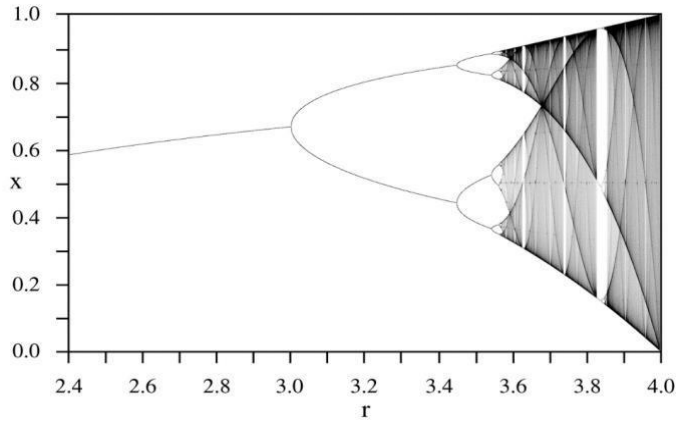


Figure 2.4: Bifurcation Diagram of Logistic Map

2.9.2 Sine Map

The sine function defines the sin map, which is a chaotic one-dimensional map. It generates a chaotic series of values, which is useful for cryptography, pseudo-random number generation, and secure communication. Mathematical it is defined in equation 2.2, and its bifurcation figure show in Figure 2.5.

$$x_{n+1=} r.sin(\pi x_n) \qquad 0 < r \leq 1 \qquad 2.2)$$

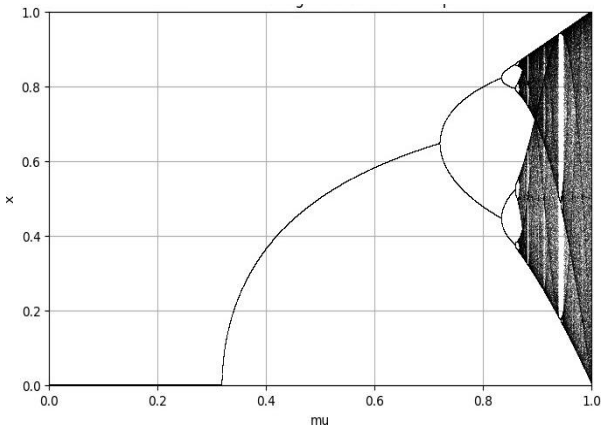


Figure 2.5: Bifurcation Diagram of Sin Map

2.9.3 Cosine Map

The Cos map is a chaotic one-dimensional map that uses the cosine function. This method is used in chaos theory and cryptography to produce pseudo-random sequences that are highly sensitive to initial conditions and control variables. Mathematical it is defined in equation 2.3, and bifurcation figure show in figure 2.6

$$x_{n+1=} r.cos(\pi x_n) \qquad 0 < r \leq 1 \qquad 2.3)$$

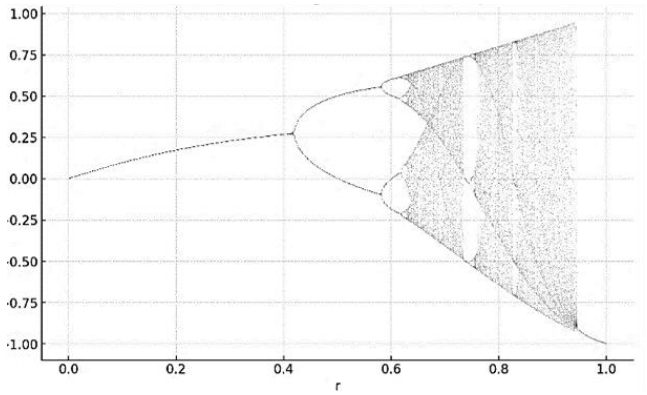


Figure 2.6: Bifurcation Diagram of Cosine Map

2.9.4 Tangent Map

The tangent map is a one-dimensional chaotic map defined by a tan function. It provides values with chaotic behavior, making it helpful for cryptography, pseudo-random number creation, and secure communication. Mathematical it is defined in equation 2.4, and its bifurcation figure show

in Figure 2.7.

$$x_{n+1=}r.tan(\pi x_n) \qquad 0 < r \leq 4 \qquad 2.4)$$

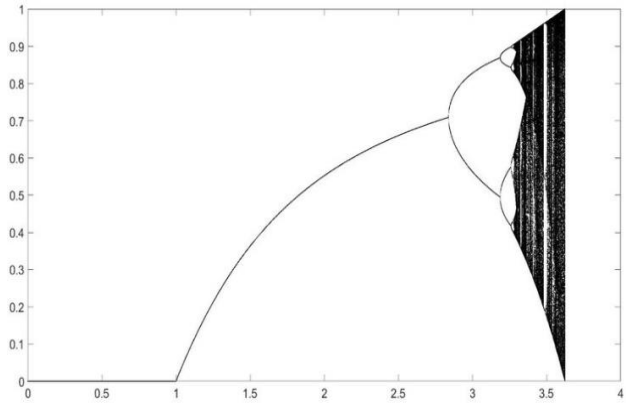


Figure 2.7: Bifurcation Diagram of Tan Map

2.9.5 Piecewise Map

A piecewise map is a function that is defined by different formulas or expressions on different Intervals of its input domain. A general piecewise map can be written as in equation 2.5.

$$f(x) = \begin{cases} f_1(x), & if\ x \in I_1 \\ f_2(x), & if\ x \in I_2 \\ & . \\ & . \\ & . \\ f_n(x), & if\ x \in I_n \end{cases} \qquad 2.5)$$

$f_1, f_2, \dots, f_n$ are different functions and $I_1, I_2, \dots I_n$ are disjoint intervals that partition the domain. Tent map is the example of Piecewise Map.

2.9.6 Tent Map

A directed piecewise linear map, commonly referred to as the tent map as shown in equation 2.6 and 2.7. Its sensitivity to starting conditions is well known [24, 25]. Demonstration of bifurcation of tent map is shown in Figure 2.8 below.

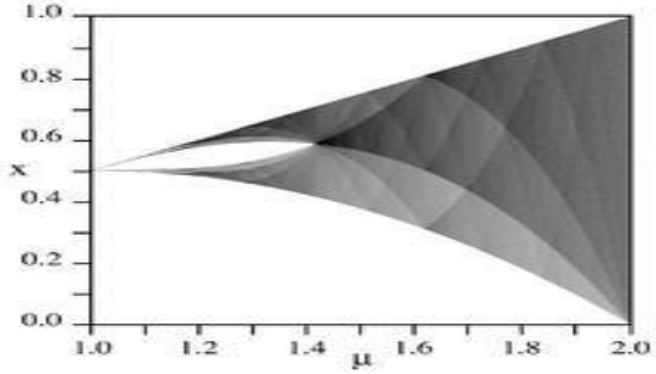


Figure2.8: Bifurcation Diagram of Tent Map

$$x_{n+1} = rx_n \quad 0 \leq x_n < 0.5 \tag{2.6}$$

$$x_{n+1} = rx_n (1 - x_n) \quad 0.5 \leq x_n < 1 \tag{2.7}$$

2.10 Tests for Chaotic Maps

Chaotic maps refer to mathematical systems that exhibit chaotic behavior, including aperiodicity, unpredictability, and sensitivity to initial conditions. Understanding a chaotic map's properties means that it is chaotic, which is the testing. These are some typical examinations and tests that are used for chaotic maps.

2.10.1 Lyapunov Exponent

The exponential divergence or convergence of adjacent illustration in the given function is measured by Lyapunov exponents. An elevated Lyapunov exponent denotes random conduct. Demonstration of Lyapunov exponent for logistic map is shown in Figure 2.9. Lyapunov exponent for logistic map will be in equation 2.8.

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \ln \left| \frac{d\{x_{n+1} = r x_n (1 - x_n)\}}{dx_n} \right| \tag{2.8}$$

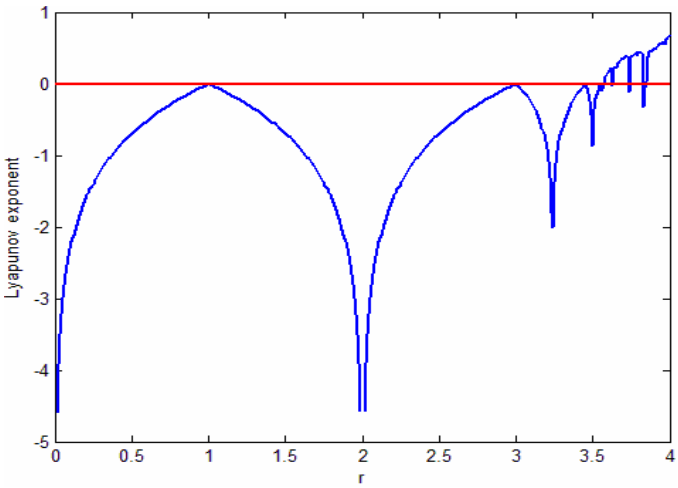


Figure 2.9: Lyapunov Exponent for Logistic Map

2.10.2 Entropy Measures

The disorder and unpredictability of the functions are determined by entropy. Chaotic behavior is shows high entropy behavior. The following formula 2.9 is applied to determine an image's entropy.

$$H(m) = -\sum_{u=0}^{n-1} P(m_u) log_2[P(m_u)], \tag{2.9}$$

Where grey-level u occurrence probability is denoted by (mu), $u = \{0, 1, 2 \ldots 2n\}$ and 2^n is greyscale image

level number. If all of the mu in the image have the same occurrence probability, then probability $P(mu) = 1/2^n$. Thus, the image displays utterly arbitrary behavior by $\mathcal{H}(m = n)$. The demonstration of entropy analysis is shown in Figure 2.10.

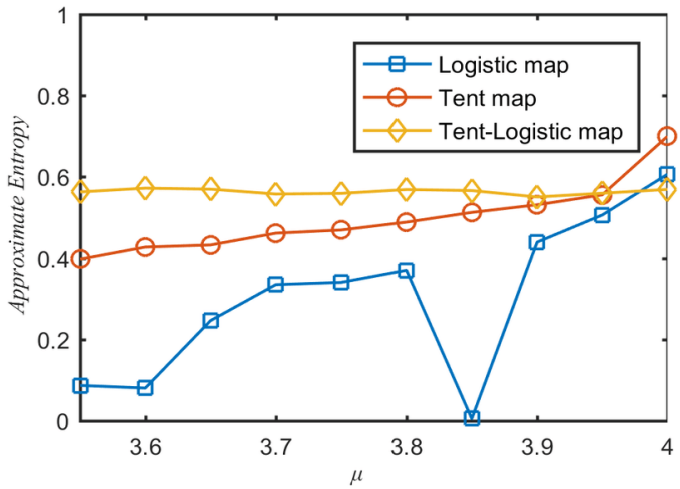


Figure 2.10: Entropy Analysis

2.10.3 Correlation

Correlation offers a relationship between nearby pixels in the image, and this relationship is divided into three different categories: horizontal, diagonal, and vertical formats. The entire texture of the image was taken into consideration during this analysis, and the equation 2.10 represents this analysis, and adjacent pixel correlation are given in equation 2.11.

$$K = \sum_{x,y} \frac{(x-\mu x)(y-\mu y)p(x,y)}{\rho_u \rho_v} \quad 2.10)$$

$$\begin{cases} R_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \\ cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(x_i - E(y)\big) \\ E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \end{cases} \quad 2.11)$$

2.10.4 The Analysis of Differential Attacks

Most attackers use a technique in which they slightly alter the original plain image before using the proposed scheme to encrypt both the plain and previously encrypted image (which they want to break) in order to extract vital information from it. Two encrypted images are thus acquired. By comparing the rates of the two ciphered images, the attackers are able to break the cryptosystem in this way. Differential analysis is the name given to this entire procedure. This means that even a little change to either would result in a full change to the ciphered text. There are two ways for evaluating an encrypted image's resistance against differential attacks: number of pixels change rate

(NPCR) and unified average changing (UACI). When NPCR [27], considers two ciphered pictures with just one pixel changed, it is assessed as follows: if $C_1(u,v)$ represents the first image and $C_2(u,v)$ represents the second as shown the formula 2.12.

$$NPCR(c_1,c_2) = \frac{\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} D(u,v)}{\mathrm{M}\times\mathrm{N}} \times 100\% \quad 2.12)$$

Equation 2.13, defines $\mathcal{D}\ (u,v)$, and $M \times N$ represents the total number of pixels.

$$\mathrm{D(u,v)} = \begin{cases} 0 & \text{if } \mathrm{c_1(u,v) = c_2(u,v)} \\ 1 & \text{if } \mathrm{c_1(u,v) \neq c_2(u,v)} \end{cases} \quad 2.13)$$

To test the pixel change number, the UACI (Unified Average Changed Intensity) [27], calculates the average change in intensity across the cipher image. This analysis is expressed mathematically by the formula 2.14.

$$UACI(c_1,c_2) = \frac{1}{M\times N}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1}\frac{|D(u,v)-P(u,v)|}{F} \times 100\% \quad 2.14)$$

Where $D\ (u,v)$ is defined in equation 2.15 and F is the maximum approved pixel value compatible with the encryption image format.

$$\mathrm{D(u,v)} = \begin{cases} 0 & \text{if } \mathrm{c_1(u,v) = c_2(u,v)} \\ 1 & \text{if } \mathrm{c_1(u,v) \neq c_2(u,v)} \end{cases} \quad 2.15)$$

2.10.5 Mean Squared Error

MSE refers to the squared average difference between the original and distorted images. The mathematical formulation of MSE is given in equation 2.16.

$$MSE = \frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\big(P(i,j) - C(i,j)\big)^2 \quad 2.16)$$

Image size is $\boldsymbol{m} \times \boldsymbol{n}$. $\boldsymbol{P(i,j)}$ and $\boldsymbol{C(i,j)}$ parameters represent pixel placement in the $\boldsymbol{i^{th}}$ and $\boldsymbol{j^{th}}$ rows and columns of the original and ciphered images. A higher MSE value is required for encryption methods to have strong security [28].

2.10.6 Peak Signal to Noise Ratio.

Noise has an impact on the signal's representation. PSNR is defined as the ratio of noise to single power, as given in equation 2.17.

$$PSNR = 10log_2(I_{max}^2) \quad 2.17)$$

I_{max}, represents the image pixel maximum value [29].

2.10.7 Classical Types of Attacks

Generally speaking, when a cryptosystem is being cryptanalyzed, it is considered that

the cryptanalyst is fully aware of the design and operation of the target cryptosystem, with the exception of the secret key. To penetrate any cryptosystem, attackers use four well-known approaches: known-plain-text attack, selected plain-text assault, cipher text only attack, and chosen cipher-text attack [29].

2.10.8 Statistical Tests:

To verify the produced time series randomness and absence of structure, run statistical tests to check on them. For instance, auto-correlation analysis and histograms may be helpful. When working with chaotic maps, several tests and studies must be conducted simultaneously in order to completely characterize the system's behavior and validate its chaotic nature [24, 25].

CHAPTER 3

A SECURE IMAGE ENCRYPTION SCHEME BASED ON A NOVEL 2D SINE-COSINE CROSS-CHAOTIC (SC3) MAP

3.1 Overview

The rapid expansion of digital image transmission across a range of industries, including cloud storage, medical imaging, communication, and military applications, has made providing secure image encryption a crucial issue [30, 31]. The increasing danger of cyber threats, illegal access, and data breaches necessitates the development of new encryption techniques that could effectively protect image data from possible attacks [32, 33]. The study [41], introduced a novel two-dimensional sine-cosine cross-chaotic (SC3) map that improved the encryption process's security and unpredictability. Because of their complex behavior and ability to generate pseudo-random sequences, chaotic maps are ideal for use in encryption methods. Two chaotic sequences produced by the SC3 map are present in the confusion and diffusion stages of the encryption. The great sensitivity of the proposed SC3-based encryption system is one of its main advantages. By rendering brute-force attacks extremely impracticable, this feature improves security. Additionally, statistical analysis, such as entropy measurement, correlation coefficient analysis, histogram uniformity evaluation, and resistance testing against differential assaults, is used to rigorously validate the encryption method. These assessments attest to the suggested method's ability to achieve high security while preserving computing efficiency. The architecture and functioning of the SC3-based image encryption system are thoroughly examined in this paper [40]. The efficacy of the suggested approach is assessed by evaluating its computational complexity, security performance, structural design, and practical application. This evaluation examines the encryption scheme's shortcomings, such as the lack of cryptanalysis against sophisticated attack models, possible processing complexity for large-scale images, and the viability of hardware implementation, even if it exhibits good security features.

3.2 Formulation of the Map

The proposed image encryption system is built using a two-phase process confusion and diffusion that exploits the unique properties of the sine–cosine cross-chaotic (SC3) map, as given in equation 3.1.

$$\begin{cases} x_{i+1} = \sin\left(\frac{\alpha}{y_i}\right)^{\frac{3}{2}} \\ y_{i+1} = \cos(\beta Cos^{-1} x_i) \end{cases} \quad 3.1)$$

Where α, β are the control parameter, $(\alpha, \beta) \in [0,1]$ and x_0, y_0, are two initial parameter, $(x_0, y_0) \in [0,1]$. To create an encrypted image, extremely resistant to cryptanalysis, the goal is to maximize unpredictability and sensitivity to beginning conditions in order to assure secure image encryption. The review thoroughly examines the encryption method's procedure, focusing on its effectiveness, security, and potential areas for improvement. The confusion phase, which involves rearranging the source image using pixels to eliminate identifiable patterns and correlations, is a crucial step in image encryption. This step is crucial because images are high redundancy the fact that nearby pixels often have similar values makes them susceptible to statistical attacks. Bifurcation analysis and the Maximum Lyapunov Exponent (MLE) are employed to confirm the SC3 chaotic map's usefulness. Encryption requires a very chaotic system since it ensures that the sequences that are created are unpredictable. The SC3 map demonstrates the required chaotic features to be the basis for a strong encryption system, as confirmed by its significantly positive Maximum Lyapunov Exponent.

3.3 Validation of the SC3 Map's Effectiveness

The effectiveness and security strength of the SC3 map are validated through two critical analytical techniques.

3.3.1 Phase Diagram and Bifurcation Analysis.

Because the pseudo-random sequence is not restricted to a single region to achieve high diffusion capacity, it exhibits both uniform dispersion and unpredictability. According to phase diagram 3.1, it is more chaotic with a high ergodicity. Bifurcation occurs when the topological structure of the output value distribution in relation to the control parameters changes as the control or bifurcation parameter (0, 1) changes.

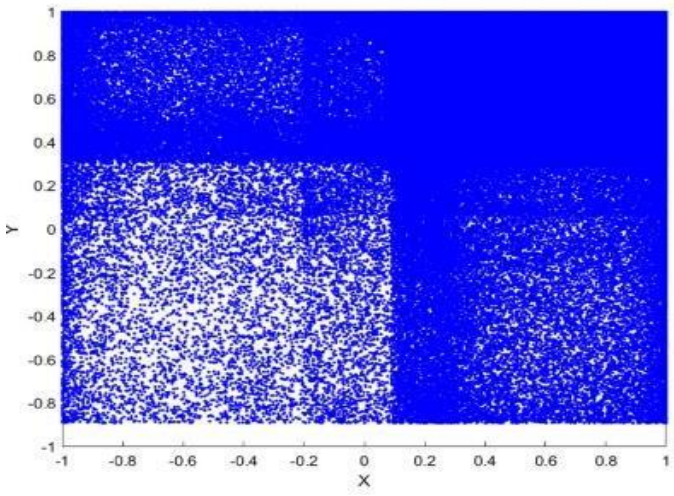
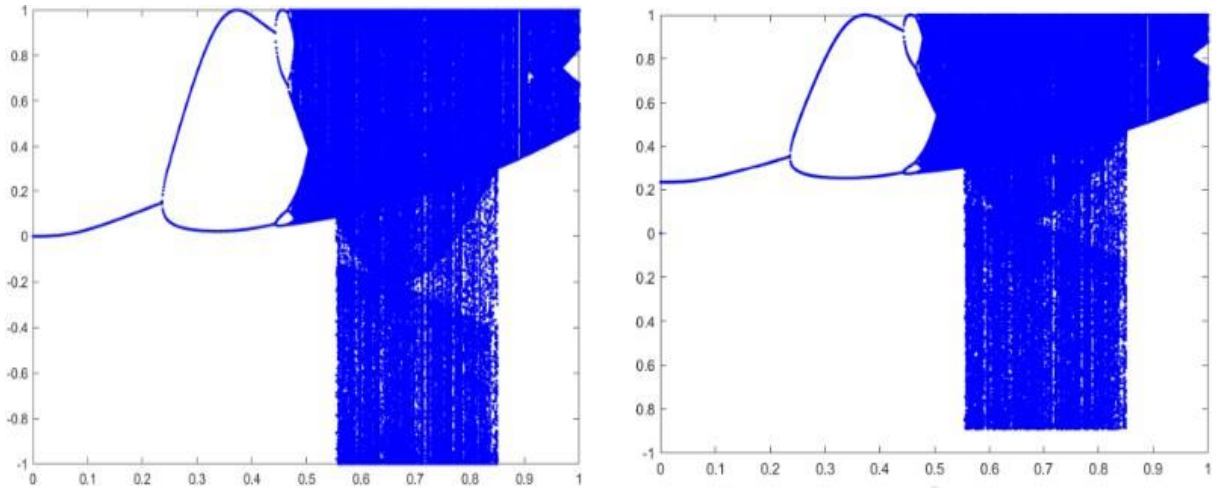


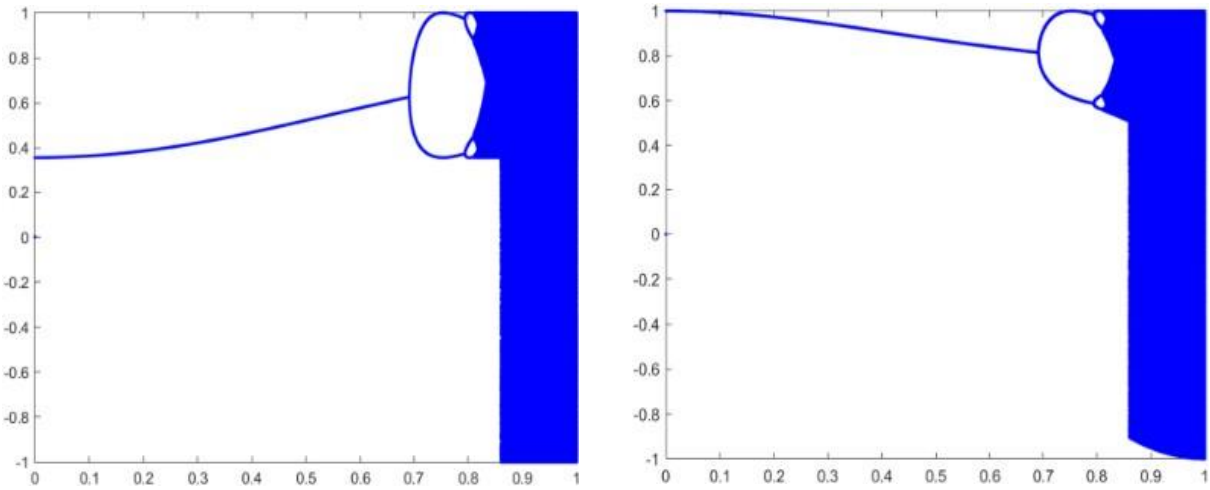
Fig. 3.1: Phase Diagram of Chaotic Map

The Bifurcation Diagrams show the variations of α and β. Figure 3.2 (a) and (b) depicts the X and Y sequence are bifurcation diagram with a step value of 0.001 when α ranges from 0 to 1 and $\beta = 0.85$. The fixed point and periodic window are shown by solid lines, while the chaotic zone is represented by dots. The proposed map exhibits chaotic behavior when the control parameter α is between 0.49 and 1. Figures 3.3 (a) and (b) depict the bifurcation diagrams for the X and Y sequences, with β ranging from 0 to 1 and α = 0.90.



(a) X sequence (b) Y sequence

Figure 3.2: (a) and (b) Bifurcation Diagram when α varies



(a) X sequence (b) Y sequence

Figure 3.3: (a) and (b) Bifurcation Diagram when β varies

3.3.2 Maximum Lyapunov Exponent (MLE)

A dynamical system's sensitivity to beginning conditions and unpredictable nature define its chaotic behavior. The Lyapunov exponent is a quantitative measure that determines a dynamic system's chaotic behavior [34]. It is defined in equation 3.2

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln|f'(x_i)| \qquad 3.2)$$

λ is the control parameter α varies from 0 to 1 and β = 0.85 as illustrated in Figure 3.4 and 3.5, respectively, the Lyapunov exponent in this work by maintaining α= vary, β=fixed, and β vary, α fixed. The higher LE number indicates that the system is more unpredictable. Also show in Table 3.1 and Table 3.2.

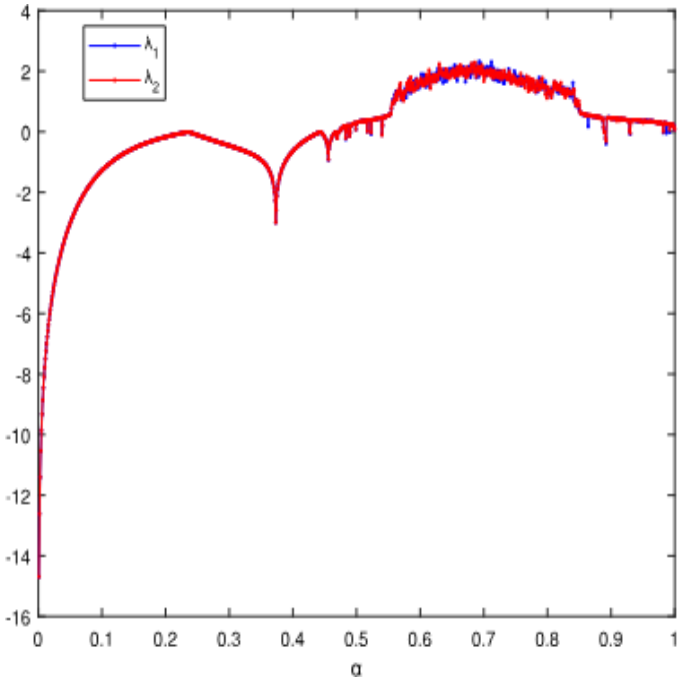


Figure 3.4: Lyapunov Exponent (α = vary β = 0.85)

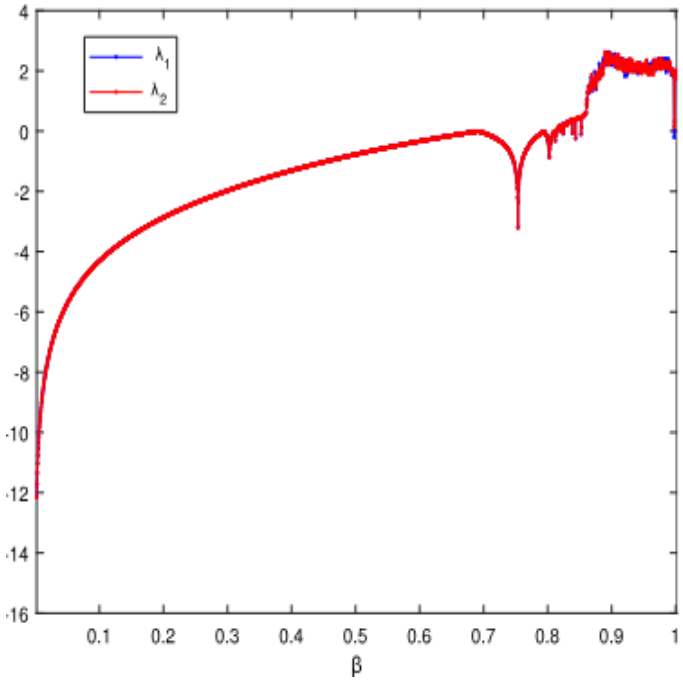


Figure 3.5: Lyapunov Exponent (β = vary α = 0.90)

Table 3.1: Lyapunov Exponent Value for the Suggested Map

(α,β)	LE (λ_1)	LE (λ_2)
(0.85, 0.90)	1.9577	2.1899
(0.88, 0.95)	2.2718	2.3670
(0.70, 0.90)	2.7632	2.4306
(0.75, 0.85)	1.8427	1.6771

Table 3. 2: Lyapunov Exponent Value of the Present Chaotic Map [34]

(IC, PC)	LE
(0.3, 8)	1.38632
(0.4, 7.6)	1.09744
(0.5, 6)	0.968348

3.4 A Proposed Cryptosystem based on the SC3 Map

The cryptosystem for image encryption is designed in this part using the 2D DC3 Map to withstand differential, statistical, and brute force attacks. To withstand all kinds of attacks, the encryption technique shuffles and replaces the image pixels with other values. The first step is to converts the input plain image into a cipher image via bitwise XOR and pixel shuffling. R_1 and R_2 are pseudo-random sequences, respectively. Using the specified 2D SC3 map, the pseudo-random sequences R_1 and R_2 were generated based on the shared secret key. The initial parameter $(x_0, y_0)$and control parameter (α, β) combined together $(x_0 , y_0, \alpha, \beta)$ and $(x_0' , y_0', \alpha', \beta')$ to create the secret key K_1 and K_2, for the confusion and diffusion layers. Algorithms 1 and 2 explain the encryption and decryption procedure.

3.5 Pixel Scrambling leads to Confusion

According to the confusion principle, the relationship between the cipher image and the secret key should be as subtle and difficult as feasible. A single modification to the secret key must have an impact on the cipher image. The pixel shuffling phase permutes the basic image using the pseudo-random sequenceR_1, reducing the correlation between adjacent pixels.

3.6 Diffusion using bit Manipulation

By creating it as complicated as much as feasible to fend off the differential attack, the diffusion concept conceals the connection between the plaintext and ciphered images. The diffusion phase conceals

the relationship between plain and cipher images while maintaining the cipher image's consistent pixel value distribution. Statistical attacks are made more difficult by converting the plain image into a cipher image with a consistent distribution of pixel values.

3.7 Image Encryption Algorithm

Algorithm 1. Key setup and Encryption process

1. Read the $2D$ plain image P of size $W \times H$ and convert into 1D vector $P = \{p_1, p_2 \ldots p_N\}, where\ N = W \times H$
2. Generate the control parameters $\alpha, \beta\ \varepsilon$ [0,1] and obtain initial parameters x_0, y_0 ε [0,1]
3. Secret Key $K_1 = (x_0, y_0, \alpha, \beta)$ and $K_2 = (x_0', y_0', \alpha', \beta')$
4. $For\ i \leftarrow 1$ to N do
5. $x_{i+1} = \sin\left(\frac{\alpha}{y_i}\right)^{\frac{3}{2}}$
6. $t_1 = (x_{i+1} \times 10)^{15} and$ W × H
7. $Insert\ t_1\ into\ R_1$
8. $y_{i+1} = \cos(\beta acos x_i)$;
9. $t_2 = (y_{i+1} \times 10^{15}) and 256$;
10. Insert $t_2\ into\ R_2$;
11. **end**
12. For $j \leftarrow 1\ to\ N\ do$
13. $1 \leftarrow swap(p[j], p[R1[j]])$
14. ***end***
15. $For\ i \leftarrow 1\ to\ N\ do$
16. $C[k] \leftarrow XOR(I[k], R_2[k])$;
17. ***end***
18. Reshape the sequence C into size of $W \times H$ cipher image

3.8 Image Decryption Algorithm

Algorithm 2. Key setup and Decryption process

1. Obtain the secret key $K_1 = (x_0, y_0, \alpha, \beta)$ and $K_2 = (x_0', y_0', \alpha', \beta')$
2. Read the cipher image C of size $W \times H$ and decompose $1D$ vector of size N $(W \times H)$;
3. ***For*** $i \leftarrow 1$ to N **do**
4. $x_{i+1} = \sin(\frac{\alpha}{y_i})^{\frac{3}{2}}$
5. $t_1 = (x_{i+1} \times 10)^{15} and$ W × H
6. $Insert\ t_1\ into\ R_1$
7. $y_{i+1} = \cos(\beta acos x_i)$;
8. $t_2 = (y_{i+1} \times 10^{15}) and 256$;
9. $Insert\ t_2\ into\ R_2$;
10. ***end***
11. For $j \leftarrow 1\ to\ N\ do$
12. $1[j] \leftarrow XOR(C[j], p[R2[j]])$
13. ***end***
14. $For\ k \leftarrow 1\ to\ N\ do$
15. $P \leftarrow swap(I[k], R_2[k])$;
16. ***end***
17. Reshape the sequence C into size of $W \times H$ plain image

3.9 Experimental Details

The purpose of this study is to evaluate the security and performance of the encryption system by running a MATLAB experiment on a standard image, "Lena 512", "Baboon", "Peppers", "Nike logo", and "Airplane". The confusion and diffusion layer's pseudo-random sequences $R_1$and R_2 are constructed using the two secret keys (K_1, K_2). The starting parameters (x_0, y_0) and the parameters for control is(α, β). Consider as secret key K_1, where $x_0\ , y_0, x'_0\ , y'_0 \in [0,1]$ and $K_2 = x'_0\ , y'_0, \alpha', \beta'$, where

$x_0 = 0.5217649304251095,\ y_0 = 6392750215680951,$

$\alpha = 0.5672104389217190,\ \beta = 0.8502175864356750,$

$x'_0 = 0.7356439802176543,\ \ y'_0 = 0.8530267952419067,$

$\alpha' = 0.5678093425186743 \quad \beta' = 0.9256810743901653.$

In comparison to the current image encryption system, the scheme's encryption computation quality is lower, but the encryption or decryption time is significantly faster. Figure 3.6 (a) to (i) display the decrypted Lena, Pepper, and Baboon as well as the encrypted and standard test images.

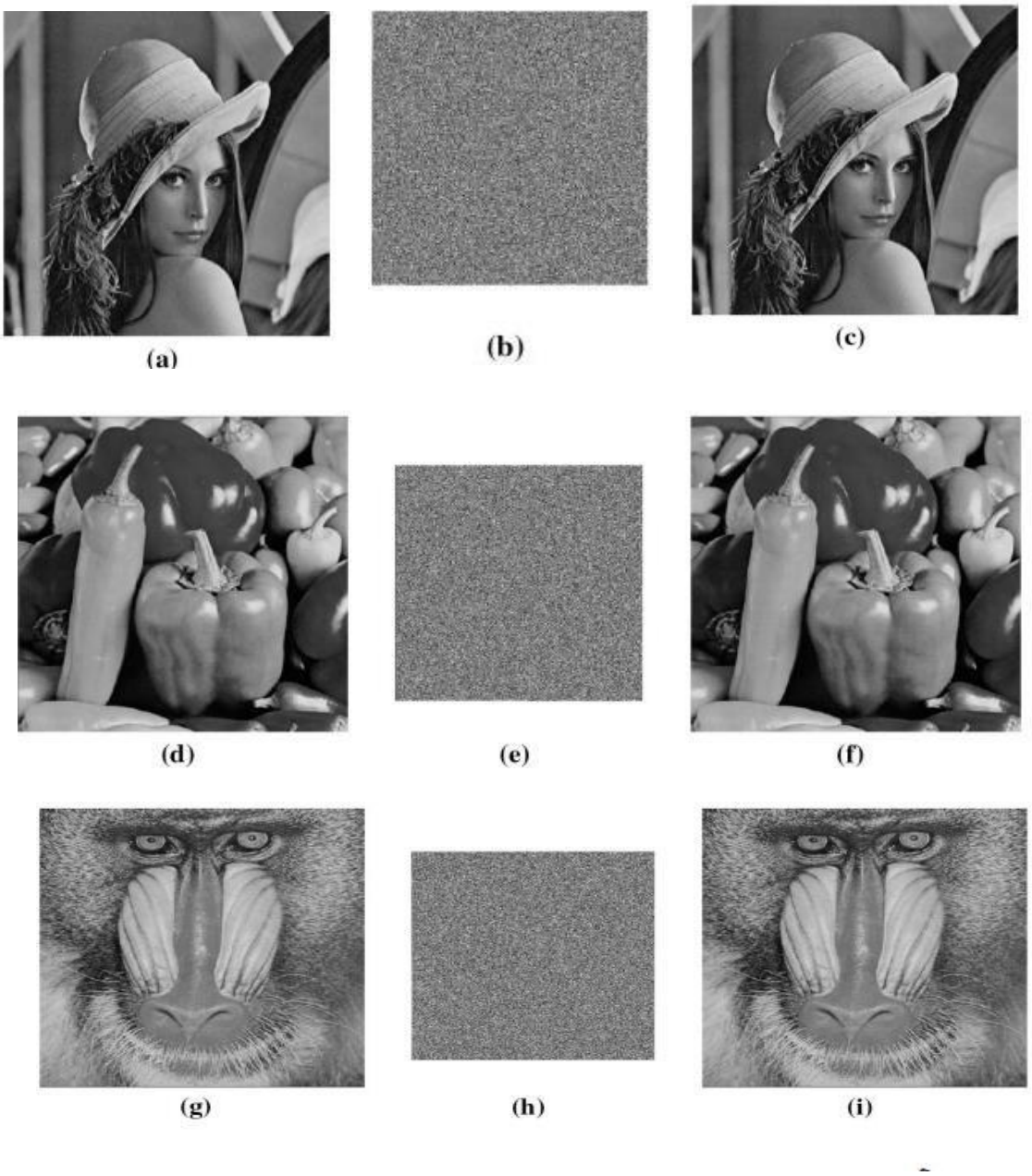


Figure 3.6: (a) Lena original Image, (b) Encrypted, (c) Decrypted, (d) Original image Peppers, (e) Encrypted, (f) Decrypted, (g) Original Image Baboon, (h) Encrypted (i) Decrypted

3.10 Security and Performance Analysis

This section presents five grayscale images of key space analysis, statistical analysis, differential cryptanalysis, and encryption quality of an image encryption system.

3.11 Analyzing Key Spaces

Figures 3.6 (a) through (i) depict conventional test images, encrypted images, and decrypted images of "Baboon", "Peppers," and "Lena". The encrypted images are both unidentified and noisy. As a result, the attacker has a difficult time discovering any hidden information and recovering the plain image or secret key. To withstand exhaustive searches or brute force attacks, the entire key search space should be fairly large. This work suggests a method for encrypting images using 2D SC3 maps. The secret key is obtained using four parameters $(x_0, y_0, \alpha, \beta)$. Since the computational precision in our experiment is limited to 10^{-16}, the entire key space is $10^{64} \approx 2^{213}$. The comparison results of the secret's whole search space are shown in Table 3.3.

Table 3.3: Secret Key Comparison Results.

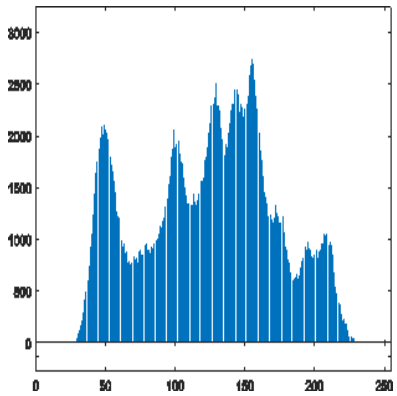
Algorithm	Key space
Proposed	$10^{64} \approx 2^{213}$
Ref. [36]	10^{60}
Ref. [35]	2^{256}
Ref. [37]	2^{232}
Ref. [38]	2^{100}
Ref. [39]	2^{624}

3.12 Resistant to Statistical Attack

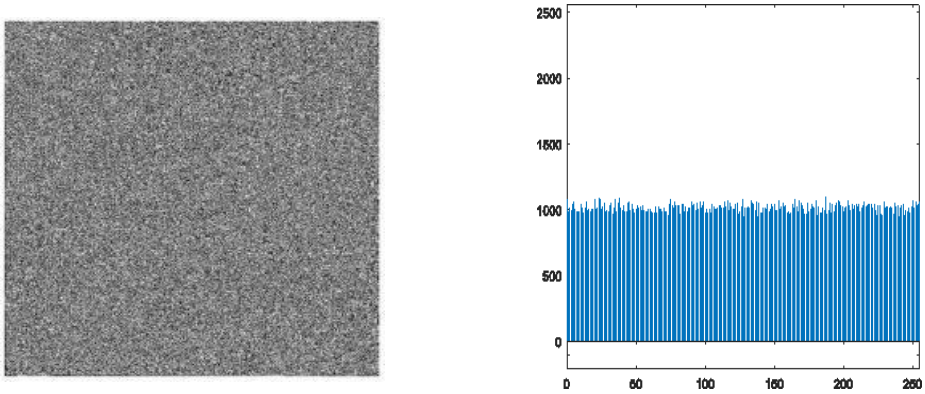
3.12.1 Analyzing Histograms

The histogram depicts the distribution of pixel values in the image 0 to 255. Figures 3.7 (a) to (d), 3.8 (a) to (d), and 3.9 (a) to (d) demonstrate how a secure image cryptosystem should create a consistent distribution of encrypted image pixel values, making it extremely difficult for an attacker to breach.

(a)

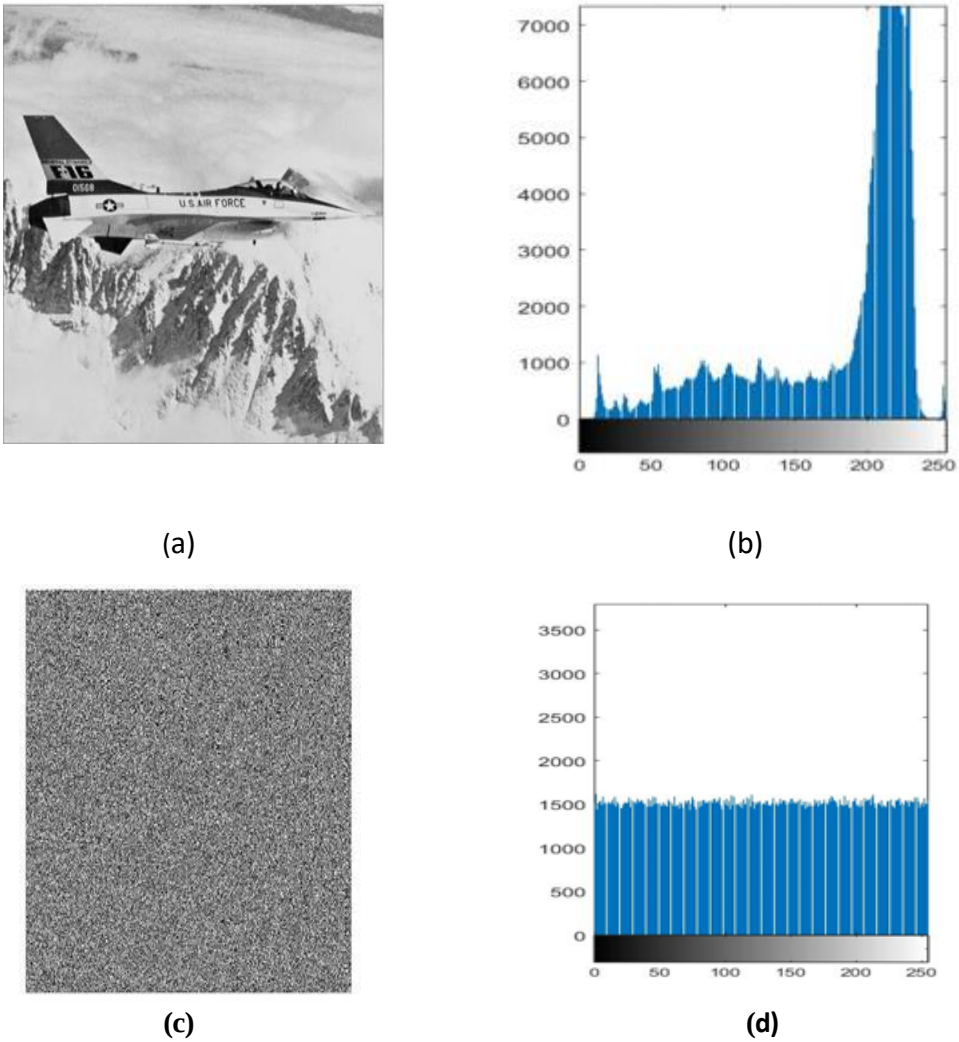


(b)



(c) (d)

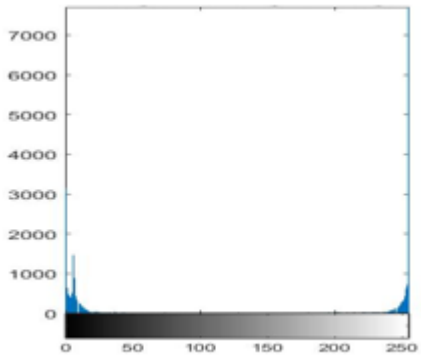
Figure 3.7: (a) Original image Lena, (b) Histogram, (c) Encrypted Image Lena, (d) Histogram



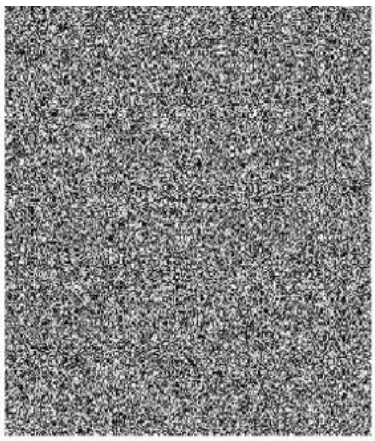
(a) (b)

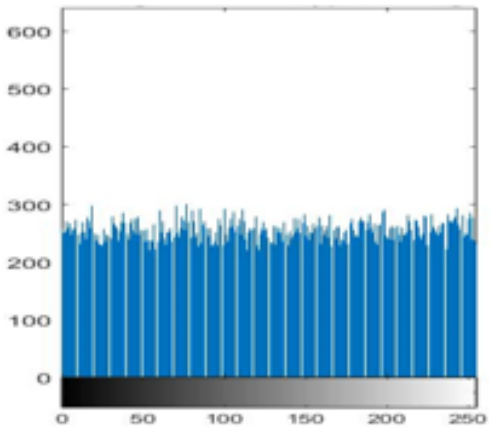
(c) (d)

Figure 3.8: (a) Original Image of the Airplane, (b) Histogram of the Original image, (c) Encrypted Image of the Airplane, (d) Histogram of the Encrypted Image



(a) (b)





(c) (d)

Figure 3.9: (a) Original image Nike, (b) Histogram of the original image Nike, (c) Encrypted image Nike, and (d) Histogram of the encrypted image Nike

3.12.2 Correlation Analysis among Adjacent Pixels

To calculate the correlation coefficient between the plain and cipher images, we randomly choose 3000 pairs of surrounding pixels in the horizontal, vertical, and diagonal axes. Figures 3.10 (a), (b), (c), and 3.11 (a), (b), and (c) show the correlations between the original Airplane image and the cipher image on the diagonal, horizontally, and vertically, respectively. Figures 3.12 (a), (b), (c), and 3.13 (a), (b) and (c) depict the correlations between the plain Nike image and the encrypted image on the diagonal, horizontally, and vertically. Table 3.4 displays the correlation coefficient between the adjacent pixels of the original and encrypted images, whereas Table 3.5 compares the Lena images.

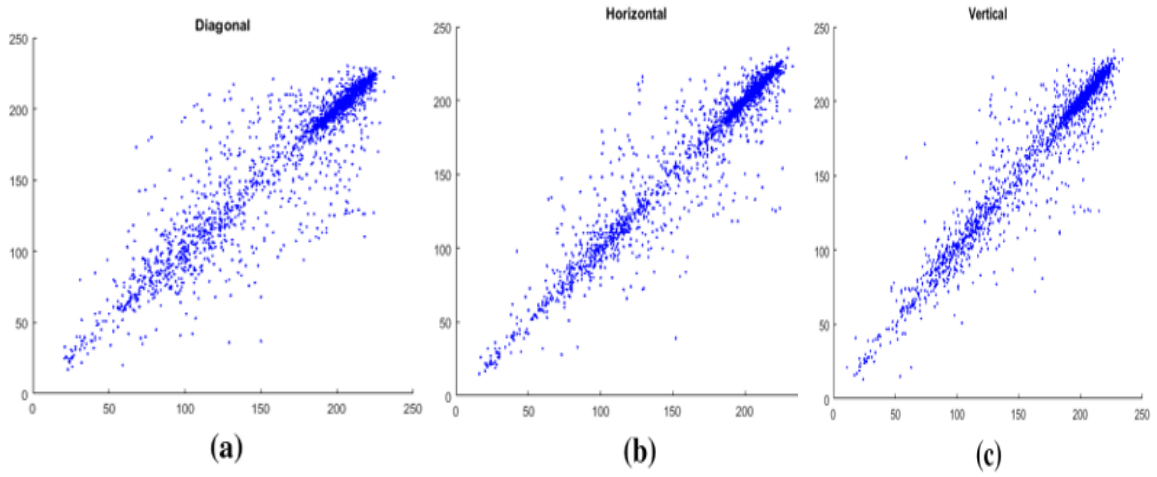


Figure 3.10: (a) Diagonal Correlation Coefficient of Original Airplane Image, (b) Horizontal Correlation Coefficient, (c) Vertical Correlation Coefficient

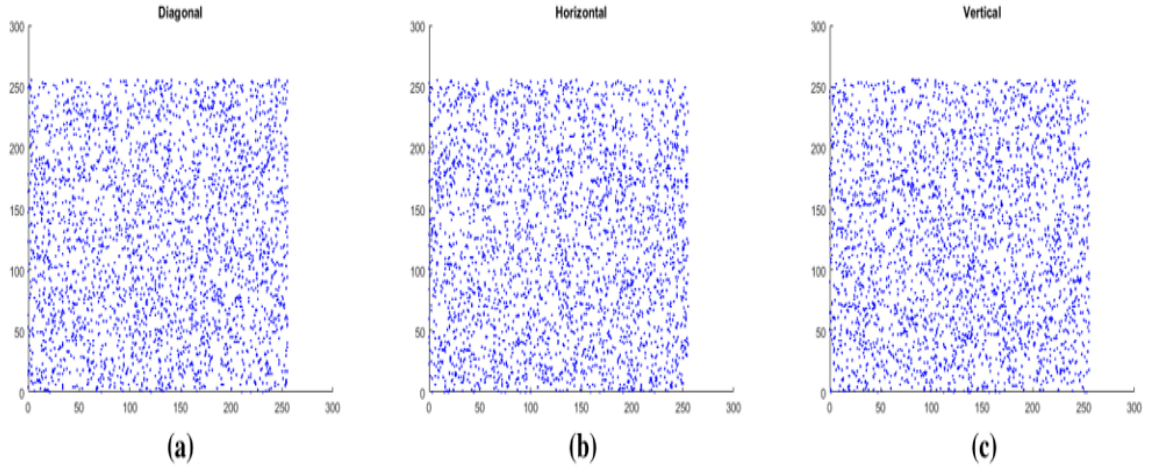


Figure 3.11: (a) Diagonal Correlation Coefficient of the Cipher Airplane image, (b) Horizontal Correlation Coefficient, (c) Vertical correlation coefficient

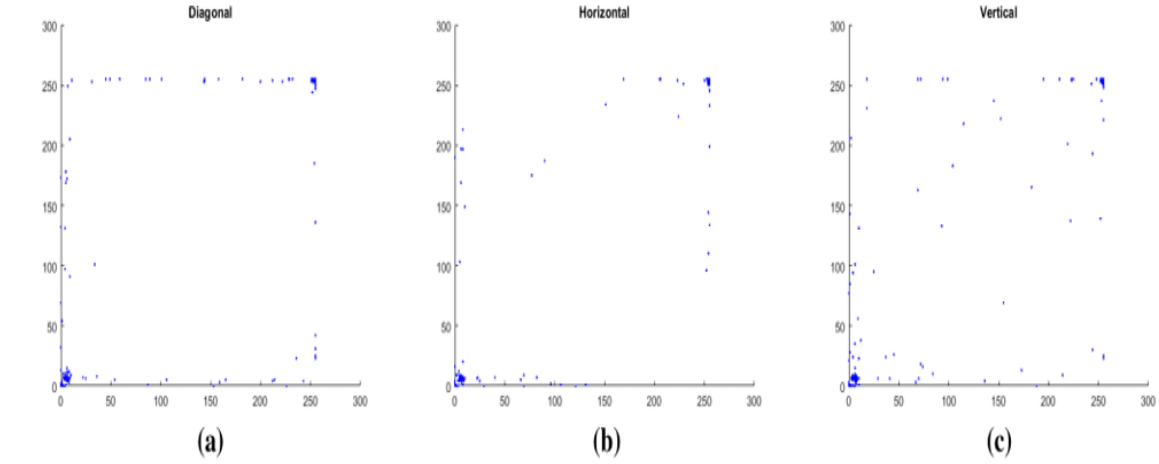


Figure 3.12: (a) Diagonal Correlation Coefficient of Original Nike Image, (b) Horizontal Correlation Coefficient of Image, (c) Vertical Correlation Coefficient of Image

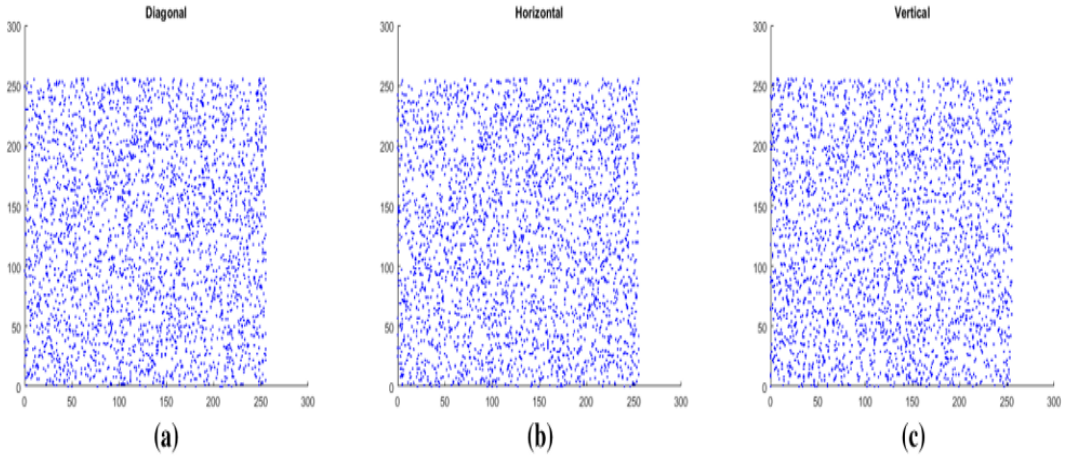


Figure 3.13: (a) Diagonal Correlation Coefficient of Cipher Nike image, (b) Horizontal Correlation Coefficient of Cipher Image, (c) vertical correlation coefficient of cipher image

Table 3.4: Correlation Coefficient between Original and Encrypted Images

Image	Lena		Pepper		Baboon		Nike		Airplane	
	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
Horizontal	0.9669	0.0008	0.9822	0.0046	0.9717	0.0047	0.9833	0.0090	0.9669	0.0016
Vertical	0.9818	0.0004	0.9856	0.0039	0.8943	-0.0001	0.9836	0.0013	0.9666	-0.0015
Diagonal	0.9521	0.0020	0.9697	-0.0018	0.9275	-0.0011	0.9596	-0.0006	-0.9395	-0.0003

Table 3.5 Lena Image Comparison

Method	Horizontal	Vertical	Diagonal
Proposed	0.0008	0.0004	0.0020
Ref. [40]	-0.0007	-0.0003	-0.0007
Ref. [39]	-0.0048	-0.0112	-0.0045
Ref. [37]	0.0015	0.0043	0.0023
Ref. [38]	-0.0008	-0.0025	0.0010

3.13 Information entropy analysis

Pixel values in any grayscale image range from 0 to 255, and the whole image requires 8 bits to represent. If the cipher image's information entropy is 8 bits or near to it, the cryptosystem is more resilient against statistical attacks. Table 3.6 is about information entropy. Table 3.7 is about comparison of information entropy of Lena image.

Table 3.6: The Results of Information Entropy

Image	Lena	Peppers	Baboon	Airplane	Nike
Entropy(original Image)	7.6112	7.1842	7.7319	6.7631	1.0027
Entropy(Encrypted Image)	7.9995	7.9889	7.9974	7.9989	7.4856

Table 3.7: Comparing the Information Entropy of Lena Image

Image	Proposed	Ref. [40]	Ref. [39]
Lena	7.9995	7.9997	7.9963

3.14 Resistance of Differential attack

Our experiment creates a new image by randomly selecting 200 pixels from the basic image and altering their values. The cipher images $C_1$and C_2 are created by encrypting the images were created using the same secret key. Table 3.8 shows the average maximum and minimum values of NPCR 99.21 and UACI 33.59, whereas Table 3.9 compares NPCR and UACI values.

Table 3.8: Average NPCR and UACI values for different plain images.

Image	Lena	Pepper	Baboon	Airplane	Nike
NPCR (%)	99.2157	99.2130	99.2252	99.6128	99.2272
UACI (%)	33.590	32.6708	32.8760	32.5345	33.5607

Table 3.9: Comparison of NPCR and UACI Results for Lena Image

Algorithm	Proposed	Ref. [40]	Ref. [39]	Ref. [37]	Ref. [38]
NPCR (%)	99.21	99.6193	99.6228	99.60	99.60
UACI (%)	33.59	33.4286	37.7041	33.46	33.50

3.15 Encryption quality

Peak signal to noise ratio (PSNR) values increase as mean square error (MSE) values decrease, showing that the plain and decrypted images are more similar. Lossless encryption is accomplished by the suggested image encryption method.

3.16 Speed and Computational complexity

It is critical to evaluate the encryption or decryption time and complexity of the algorithm. Table 3.10 displays the encryption time used by the algorithm.

Table 3.10: Suggested Algorithm's Encryption/Decryption Time (in seconds)

Image	Lena	Peppers	Baboon	Airplane	Nike
speed	0.139008	0.139435	0.139999	0.137665	0.196549

Chapter 4

A NEW MULTIPLE IMAGE ENCRYPTION SCHEME BASED ON CHAOTIC SYSTEMS

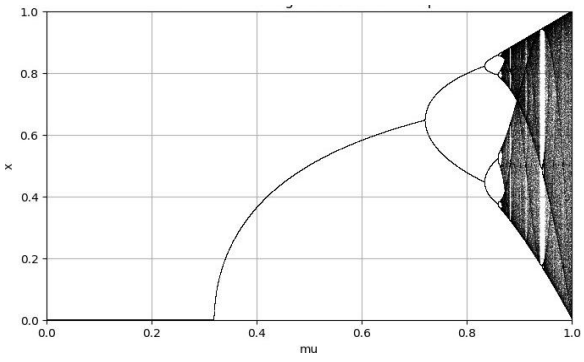
The chaotic behavior of the map has shown great promise in a variety of chaos-based encryption schemes. However, its narrow parameter space and non-uniform probability density distribution make it less useful for cryptography applications. The modified map, a novel method that combines sine, cosine and tangent functions, is proposed in this research to improve chaotic performance and provide a more uniform distribution. A more resilient and adaptable chaotic system that is appropriate for uses like encryption that demand a high degree of randomness is the primary result.

4.1 Formulation of New Map

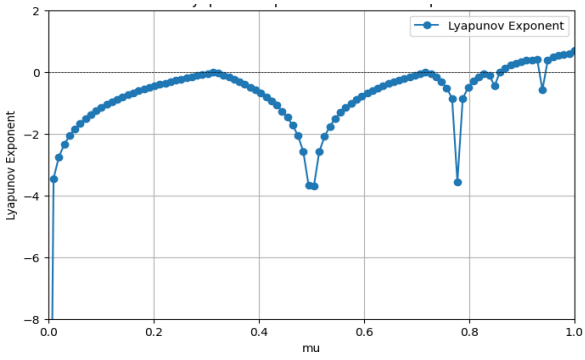
The Sin map is a classic one-dimensional chaotic system with high speed that has been used in a variety of chaos-based encryption techniques. Equation 4.1 defines the control parameter μ, which ranges from 0 to 1, and the iteration state x_i.

$$x_{i+1} = \mu \sin(\pi x_i) \qquad 0 < \mu \leq 1 \qquad 4.1)$$

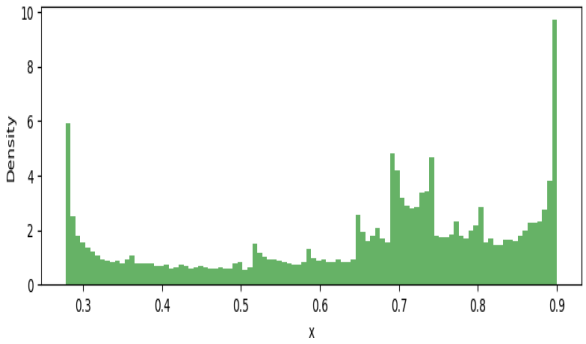
When the Lyapunov exponent is not always positive, the system becomes insufficiently complicated. Figures 4.1(a) and (b) show that the sine map becomes chaotic only when the parameter μ is between [0.87, 1]. Figures 4.1 (c) and (d) show the density probability distribution of a sine map at μ = 0.9 and μ = 1. The sine map is clearly distributed unevenly. Despite being commonly utilized, the sine map is less appropriate for secure cryptography applications due to its uneven density distribution and lack of complexity. Improving the chaotic performance and attaining a consistent distribution to improve security are the challenges.



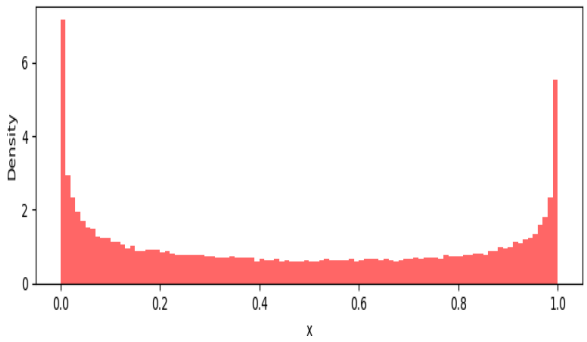
(a)



(b)



(c)



(d)

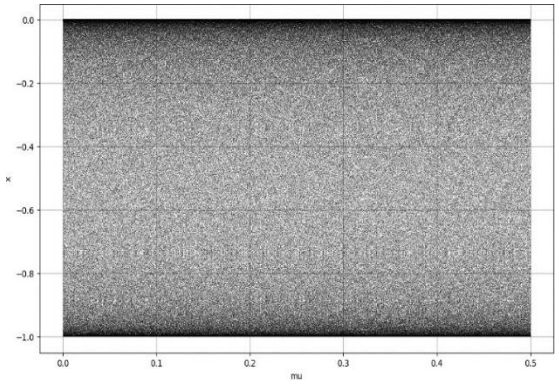
Figure 4.1: (a**)** Bifurcation, (b**)** Lyapunov exponent,

(c) and (d)Probability Distribution of Sin map (μ=0.9, μ=1)

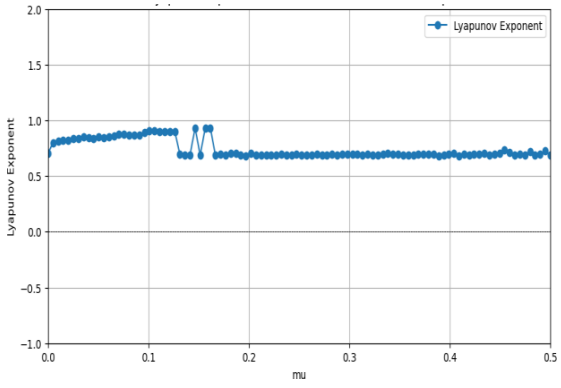
We suggest a piecewise chaotic map to enhance the chaotic performance of the sine map. We changed the sine map to use the sin, cos, and tan functions to enhance more chaotic performance. The segment intervals are calculated using the parameter μ ∈ (0, 0.5). Figures 4.2 (a) and (b) show the Lyapunov exponent and the bifurcation diagram. The bifurcation diagram is more complicated than the sine map, and the Lyapunov exponents are always positive. As a result, the new chaotic map improves chaotic performance and shows more sophisticated dynamic behavior. Figures 4.2 (c) and (d) show the map's density probability distribution for different parameter values. The new map's density probability distribution is relatively uniform for μ ∈ (0, 0.1), with less than 0.3% difference between the highest and lowest values. To achieve good ergodicity and unpredictability, set the value of μ in the interval (0, 0.1), as given in equation 4.2.

$$x_{i+1} = MPCM(x_i)$$

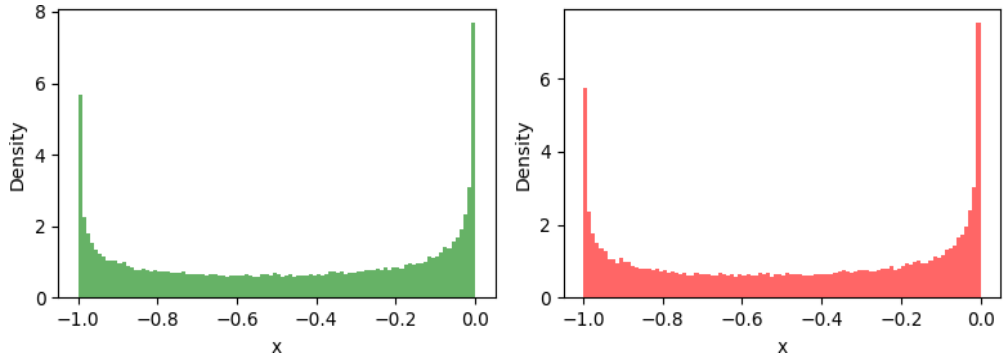
$$x_{i+1} = \begin{cases} sin(\pi x_i) & if\ x_i \le \mu\ or\ x_i > 1-\mu \\ cos\left(\frac{2\mu(x_i-\mu)}{1-2\mu}\pi\right) & if\ \mu < x_i \le 0.5 \\ tan\left[\left(1-\mu+\frac{(2x_i-1)\mu}{1-2\mu}\right)\pi\right] & if\ 0.5 < x_i \le 1-\mu \end{cases} \quad 4.2)$$



(a)



(b)



(c) (d)

Figure 4.2 (a) Bifurcation and (b) lyapunov exponent
(c) and (d) Probability Distribution of MPCM

4.2 Lyapunov Exponent Equation

It is computed as follows equation 4.3.

$$\mu = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} log \left| \frac{df^i(x)}{dx} \right| \quad 4.3)$$

Where μ is the lyapunov exponent, n is the number of iterations and $f^i(x)$ is the i^{th} rate of map.

1. $\boldsymbol{For\ x_i \le \mu\ or\ x_i \ge 1-\mu}$

$$f(x_i) = \sin(\pi x_i)$$

$$\frac{d}{dx_i}(\sin(\pi x_i)) = \pi cos \pi x_i$$

2. For $\boldsymbol{\mu < x_i \le 0.5}$

$$f(x_i) = cos\left(\frac{2\mu(x_i-\mu)}{1-2\mu}\pi\right)$$

Let $t = \frac{2\mu(x_i-\mu)}{1-2\mu}\pi$

$$f(x_i) = cost$$

$$\frac{d}{dx_i}(cost) = -\sin t \frac{dt}{dx}$$

$$\frac{dt}{dx} = \frac{2\mu\,\pi}{1-2\mu}$$

$$f'(x_i) = -\sin\left(\frac{2\mu(x_i-\mu)}{1-2\mu}\pi\right)\frac{2\mu\,\pi}{1-2\mu}$$

3. $\boldsymbol{For\ 0.5 < x_i \le 1-\mu}$

$$f(x_i) = \tan\left(1-\mu+\frac{(2x_i-1)\mu}{1-2\mu}\pi\right)$$

Let $v = 1-\mu+\frac{(2x_i-1)\mu}{1-2\mu}\pi$

$$\frac{d}{dx_i}(tanv) = sec^2(v)\frac{dv}{dx_i}$$

$$\frac{dv}{dx_i} = \frac{2\mu\,\pi}{1-2\mu}$$

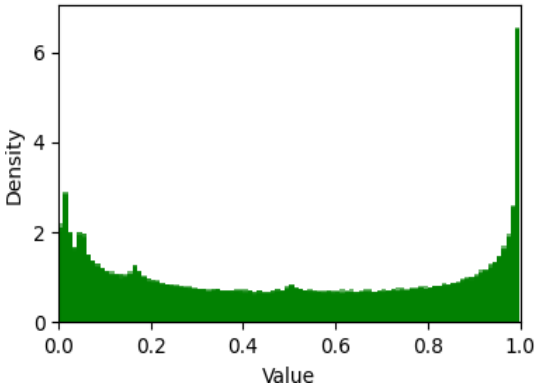
$$f'(x_i) = sec^2\left(1-\mu+\frac{(2x_i-1)\mu}{1-2\mu}\pi\right)\frac{2\mu\,\pi}{1-2\mu}$$

4.3 The Chaotic System that is Being Shown

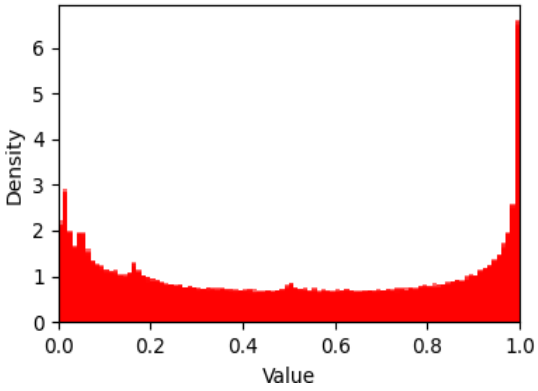
This method reduces the μ parameter space, but when μ is fixed in the interval (0, 0.1) distribution, the chaotic map can produce chaotic sequences with uniform probability density. The security of the encryption approach is compromised when the value of parameter μ is limited because parameters are typically utilized as secret keys in chaos-based encryption systems. The Coupled Chaotic Map is intended to solve this issue and further complicate chaotic systems. By linking parameters, the one-dimensional chaotic map can become multi-dimensional. Examine the definition of "four-dimensional" in equation 4.4 below.

$$\begin{cases} x = MPCM(\lambda x + (1-\lambda)y), \\ y = MPCM(\lambda y + (1-\lambda)z), \\ z = MPCM(\lambda z + (1-\lambda)w), \\ w = MPCM(\lambda w + (1-\lambda)x), \end{cases} \quad 4.4)$$

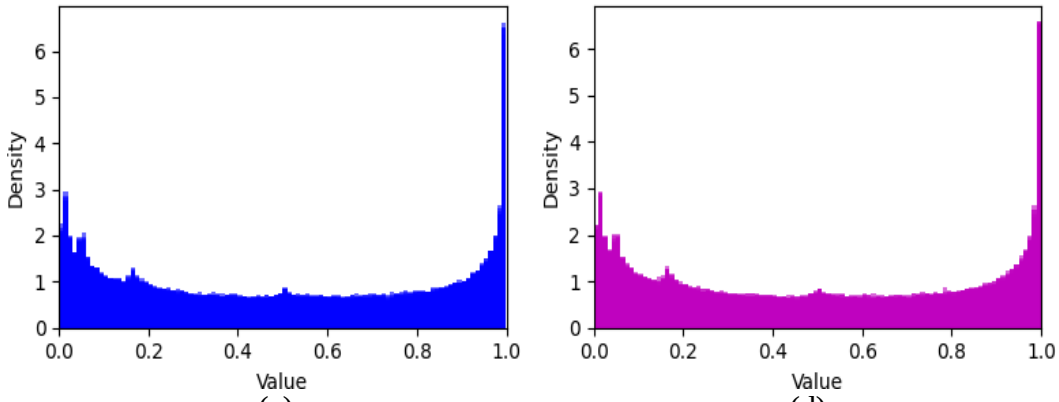
The coupling parameter in this equation is λ, and its value ranges from 0 to 1. The MPCM total parameter space is expanded with more distinct dimensional variables and control parameters for each dimensional variable. The experiment shows that the MPCM can generate chaotic sequences with a uniform probability density distribution for $\lambda \in [0,1]$ and $\mu \in (0,0.1]$. Figures 4.3 (a) to (d)) illustrate the density probability distributions of each MPCM dimension variable at $\mu = 0.05$ and $\lambda = 0.995$. The density probability's maximum and minimum values are calculated to be less than 0.3%. Because of its high-dimensional chaotic nature and uniform probability density distribution, the MPCM exhibits complex dynamic behavior and elaborate structures, providing a solid foundation for the development of encryption methods.



(a)



(b)

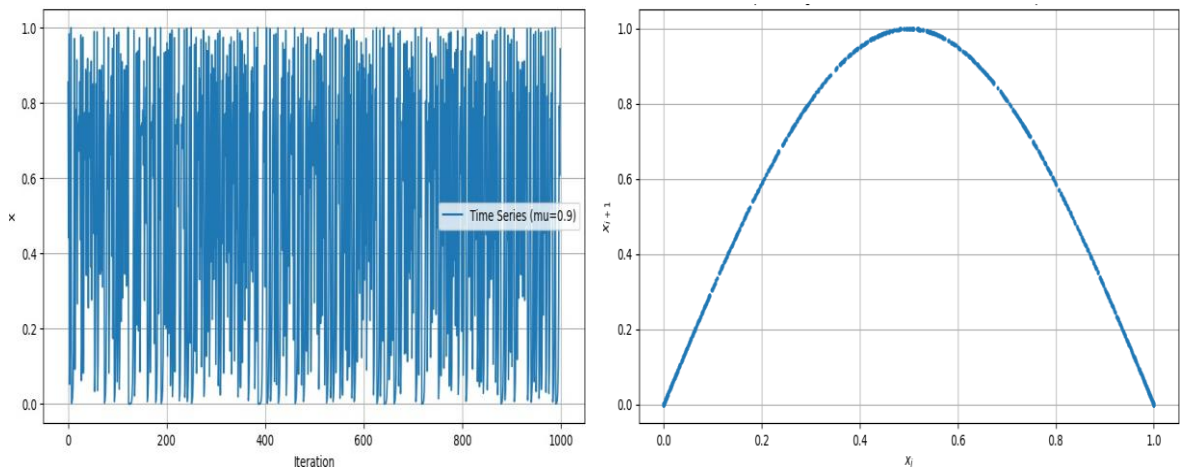


(c) (d)

Figure 4.3: Displays the density probability distribution μ=1 and λ=0.995 (a) vary =w, (b) vary=x, (c) vary=y and (d) vary=z

4.4 Time Series and Phase Diagrams

The chaotic map's performance is assessed using time series and a phase diagram.The proposed map spans the entire region indicated by the Figure 4.4 (a) and (b), which shows that the data distribution covers considerably greater territory. The lack of localization implies that the pseudo random sequence is uniformly distributed and random in order to attain a high diffusion capacity. The phase diagram shows that at μ=0.9, the system is chaotic and ergodic.



(a) (b)

Figure 4.4: (a) Time series and (b) Phase Space diagram.

4.5 Image Encryption Scheme Using MPCM

In the modern digital era, image encryption is crucial for securing multimedia content during storage and transmission. Traditional cryptographic methods may not offer the computational efficiency or complexity needed for high-dimensional image data. This work presents a robust image encryption algorithm based on chaotic sequences generated using the Modified Piecewise Chaotic Map (MPCM). The system utilizes multi-dimensional coupling

of chaotic maps to maximize unpredictability, and it divides the encryption process into two core stages: confusion (permutation of pixels) and diffusion (modification of pixel values).

4.5.1 Parameters

Upload the image. If the image *I* is in *RGB*, *I* convert it to grayscale. Choose $\mu \in [0,0.5]$ is the control parameter of Modified Chaotic Map and $\lambda \in [0.99,1]$ is the coupling strength of map. Initial values of Modified Chaotic Map are $x_0, y_0, z_0, w_0 \in [0,1]$.

4.5.2 Chaotic Sequence Generation MPCM

4.5.2.1 MPCM Function

$$x_{i+1} = \begin{cases} sin(\pi x_i) & if\ x_i \le \mu\ or\ x_i > 1-\mu \\ cos\left(\frac{2\mu(x_i-\mu)}{1-2\mu}\pi\right) & if\ \mu < x_i < 0.5 \\ tan\left[\left(1-\mu+\frac{(2x_i-1)\mu}{1-2\mu}\right)\pi\right] & if\ 0.5 < x_i \le 1-\mu \end{cases}$$

4.5.2.2 Coupled MPCM

$$\begin{aligned} x &\leftarrow MPCM(\lambda x + (1-\lambda)y), \\ y &\leftarrow MPCM(\lambda y + (1-\lambda)z), \\ z &\leftarrow MPCM(\lambda z + (1-\lambda)w), \\ w &\leftarrow MPCM(\lambda w + (1-\lambda)x), \end{aligned}$$

The system evolves for a total of $2 \times (M \times N)$ iterations, where *M* and *N* are the dimensions of the image. The first half of the generated chaotic values are utilized for permutation, while the second half is used for diffusion.

4.5.3 Confusion Phase (Permutation)

Flatten image I to 1D vector V of length and generate chaotic sequence of length $L = M \times N$. Convert each chaotic value to an Integer index $P = mod(floor(S.L), L) + 1$, sort the sequence to get the permutation order. Rearrange vector V using permutation indices and reshape back to matrix form to get permuted image I_p.

4.5.4 Diffusion Phase (Pixel Modification)

Use the second half of the chaotic sequence and convert values to the integer. D is the diffusion key $D_i = mod\ (floor\lfloor(S_i.10^{10}), 256\rfloor)$. For each pixel $I_p(i,j)$ compute that is $I_{enc}(i,j) = mod\big(I_p(i,j) + D(i,j), 256\big)$ or use XOR: $I_{enc}(i,j) = bitxor\ (I_p(i,j), D(i,j))$

4.5.5 Out Put Encrypted Image

Output the final encrypted image I_{enc} and Optionally compute.

4.5.6 Encryption Algorithm

Algorithm 4 Image Encryption using MPCM

Input: Grayscale image I of size $M \times N$
Initialize Parameters
Set MPCM control parameter $\mu \in [0,0.5]$
Set MPCM coupling strength $\lambda \in [0,1]$
Initial chaotic values $x_0, y_0, z_0, w_0 \in [0,1]$
Read Input image I and convert to grayscale if necessary
$L = M \times N$ represents the total number of pixels.
Flatten the image I into a one-dimensional vector V of length L
Chaotic sequence generation
Initialize the chaotic variables x_0, y_0, z_0, w_0
$For\ i = 1\ to\ 2L$
$x' = MPCM(x),\ y' = MPCM(y),\ z' = MPCM(z),$
$w' = MPCM(w)$
Apply Couple Map system:
$$x \leftarrow MPCM\big(\lambda x' + (1-\lambda)y\big)$$
$$y \leftarrow MPCM(\lambda y' + (1-\lambda)z)$$
$$z \leftarrow MPCM(\lambda z' + (1-\lambda)w)$$
$$w \leftarrow MPCM(\lambda w' + (1-\lambda)x)$$
$S_i = mod\ (x, 1)\ as\ the$ i-th element of the chaotic sequence S
CONFUSE$(image, chaotic\ Sequence)\ S_{perm} = S(1:L)$
$L \leftarrow$ length($image$)
for $i = 1$ to L **do**
$P\ (i) \leftarrow mod(\lfloor S(i).L \rfloor, L) + 1$
end for
$permuted \leftarrow image(P)$
Return *Permuted*
DIFFUSE $(image, chaotic\ Sequence)\ S_{diff} = S(L+1:2L)$
Convert each value to an 8bit diffusion key:
$$D_i = mod\ (\lfloor (S_{diff}(i).10^{10}) \rfloor, 256)$$
$I_{enc}(i,j) = mod\big(I_p(i,j) + D(i,j), 256\big)$
Reshape: $V_{enc} \rightarrow\ M \times N\ matrix$
Out Put $\rightarrow$ *Encrypted Image*
end

4.5.7 General Example of Encryption

Let's assume we have a small 4×4 grayscale image:

$$\text{Original image}=\begin{bmatrix}12 & 45 & 78 & 34\\ 56 & 89 & 23 & 67\\ 90 & 123 & 150 & 200\\ 34 & 66 & 99 & 111\end{bmatrix}$$

Step 1: Permutation

Original image (flattened to 1D):

$$Flat\ image = [12, 45, 78, 34, 56, 89, 23, 67, 90,123,150,200,34,66,99,111]$$

Generated permutation vector:

$$P = [5, 1, 16,9,12,3,7,2,10,4,6,11,13,14,8,15]$$

Apply Permutation:

$$Permuted\ image\ vector = [56, 12, 111, 90, 200, 78, 23, 45, 123,34,89,150,34,66,67,99]$$

Step 2: Diffusion

$$Diffusion\ Key = [13,21,15,77,101,33,9,60,1,14,42,55,3,10,7,6]$$

Apply diffusion using XOR

$$Encrypted\ vector = bitxor\ (Permuted\ Vector, Diffusion\ Key)$$

For example:

$$Bitxor\ (56, 13) = 53$$

$$Bitxor\ (12, 21) = 25$$

$$Bitxor(\ 111, 5) = 106\ and\ so\ on$$

$$Encrypted\ vector = [53, 25, 106, 23, 173, 111, 30, 17, 122, 44, 115, 173, 33, 72, 68, 101]$$

Reshape into 4×4:

$$Encrypted\ image = \begin{bmatrix}53 & 25 & 106 & 23\\ 173 & 111 & 30 & 17\\ 122 & 44 & 115 & 173\\ 33 & 72 & 68 & 101\end{bmatrix}$$

4.6 Flowchart of the Encryption Process

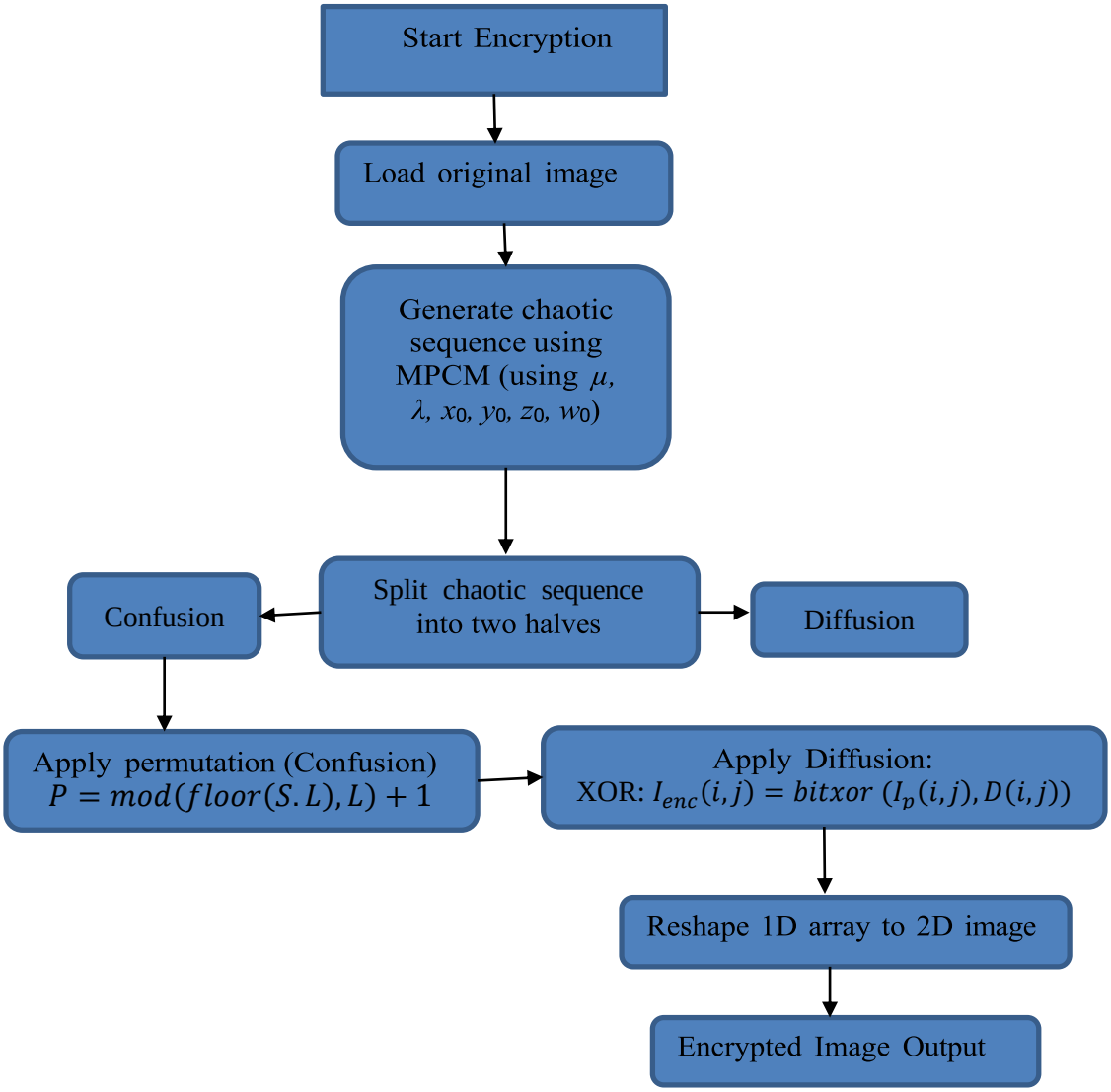


Figure 4.5: Flowchart of the Encryption Process

4.7 Image Decryption Scheme

Flatten the encrypted image I_{enc} in to 1D vector V_{enc} of length L. For decryption regenerate the chaotic sequence using same parameters. Initialize the chaotic variables x, y, z, w using the same values x_0, y_0, z_0, w_0 as used in encryption. Generate chaotic sequence length S of length $2L$ using the MPCM and same coupling parameter.

4.7.1 Inverse the Diffusion Process

For each $i \in [1, L]$ compute the diffusion key:

$$D_i = mod(\lfloor S_{diff}(i).10^{10} \rfloor \times 256$$

For each pixel $i \in [1, L]$ reverse the diffusion operation.

$$V_p(i) = mod(v_{enc}(i) - D(i) + 256,256) \text{ Or}$$

$$\text{XOR: } I_p(i,j) = bitxor\left(I_{enc}(i,j), D(i,j)\right)$$

The result is permuted image vector.

4.7.2 Inverse Permutation

For each $i \in [1, L]$ calculate permutation index $P_i = mod(\lfloor S_{perm}(i.L) \rfloor, L + 1)$

Determine the inverse permutation by finding the original position of each pixel:

$$\pi^{-1}(P) = argsort(P)$$

Apply the inverse permutation to V_p to obtain the original pixel order vector V Reshape the vector into matrix form and get the decrypted image.

4.7.3 Image Decryption Algorithm

Algorithm 4 Image Decryption Using MPCM

1: Input Encrypted Image I_{enc} , same chaotic parameter used in encryption
2: Flatten I_{enc}into 1D vector V_{enc}
2: Generate chaotic sequence S of length $2L$ using MPCM
3: Split sequence:
$$S_{diff} = S[L: 2L - 1]$$
$$S_{perm} = S[\emptyset: L - 1]$$
4: **For $i =$ 1 to L do**
5: Reverse diffusion:
$$D_i \leftarrow mod(\lfloor S_{diff}(i).10^{10} \rfloor \times 256$$
$$V_p(i) \leftarrow mod(v_{enc}(i) - D(i) + 256,256)$$
6: **End for**
7: **For $i = 1$ to L do**
8: $$P_i \leftarrow mod(\lfloor S_{perm}(i.L) \rfloor, L + 1)$$
9: **End for**
10: $\pi^{-1}(P) = argsort(P)$ inverse Purmutaion
11 **For $i = 1$ to L do**
12: $$\boldsymbol{V[i] \leftarrow v_p[\pi^{-1}(i)]}$$
13: **End for**
14: Reshape V into $M \times N \rightarrow I_{dec}$
15: **Return I_{dec}**

4.7.4 Example of Decryption Process

$$Encrypted\ image = \begin{bmatrix} 53 & 25 & 106 & 23 \\ 173 & 111 & 30 & 17 \\ 122 & 44 & 115 & 173 \\ 33 & 72 & 68 & 101 \end{bmatrix}$$

Flatten it:

$$Encrypted\ vector = [53, 25, 106, 23, 173, 111, 30, 17, 122, 44, 115, 173, 33, 72, 68, 101]$$

Step 1: Reverse Diffusion (XOR with same key)

$$Diffusion\ Key = [13, 21, 15, 77, 101, 33, 9, 60, 1{,}14, 42, 55, 3, 10, 7, 6]$$

Apply XOR again:

$$\text{Permuted vector} = \text{bitxor (Encrypted Vector, Diffusion Key)}$$
$$= [56, 12, 111, 90, 200, 78, 23, 45, 123, 34, 89, 150, 34, 66, 67, 99]$$

Reshape into Matrix:

$$Permuted\ image = \begin{bmatrix} 56 & 12 & 111 & 90 \\ 200 & 78 & 23 & 45 \\ 123 & 34 & 89 & 150 \\ 34 & 66 & 67 & 99 \end{bmatrix}$$

Step 2: Reverse Permutation

$$\boldsymbol{Permutation\ index} = [\mathbf{5, 1, 16, 9, 12, 3, 7, 2, 10, 4, 46, 11, 13, 14, 8, 15}]$$

$$\boldsymbol{Reverse\ Index} = [\mathbf{2, 8, 6, 10, 1, 11, 7, 15, 4, 9, 12, 5, 13, 14, 16, 3}]$$

Now apply it:

$$\text{Original vector = Permuted Vector (Reverse Index)}$$
$$= [12, 45, 78, 34, 56, 89, 23, 67, 90, 123, 150, 200, 34, 66, 99, 111]$$

Reshape into original 4×4 matrix:

$$Recovered\ Original\ Image = \begin{bmatrix} 12 & 45 & 78 & 34 \\ 56 & 89 & 23 & 67 \\ 90 & 123 & 150 & 200 \\ 34 & 66 & 99 & 111 \end{bmatrix}$$

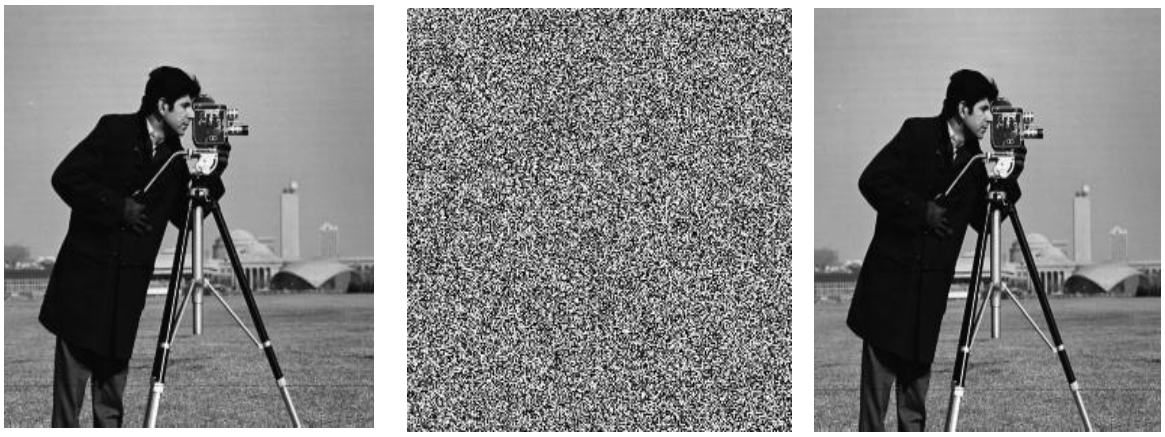
4.8 Experiment Results and Security Analysis

The experiment uses following keys:

$x = 0.226598532502152,\ y = 0.715260198702623,$

$z = 0.0.271238570940165, w = 0.619035721685213,$

$\lambda = 0.434214444,\ \mu = 0.9819349999.$ We test the suggested encryption scheme's performance and security features using MATLAB (R2018b) on a standard images "Cameramen", "Airplane", "Nik logo", "Peppers" and "Baboon" are used to test the result. The encryption and decryption result shown in Figure 4.6 (a), (b) and (c). All of the information in the plaintext images is effectively hidden by the ciphertext images, which resemble random noise and lack any visual cues. Furthermore, the cipher and plaintext images are identical. Consequently, the experimental findings confirm that the method is accurate.



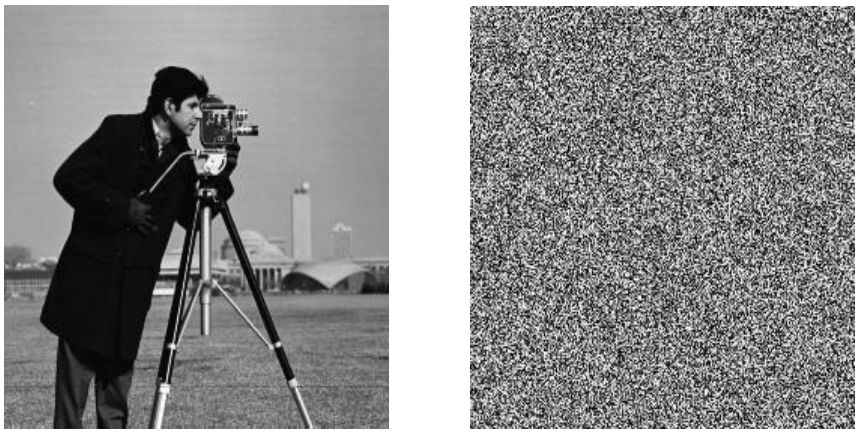
(a) (b) (c)

Figure 4.6: (a) Plaintext of Cameraman Image (b) Encrypted Image (c) Decrypted image

4.9 Statistical Analysis

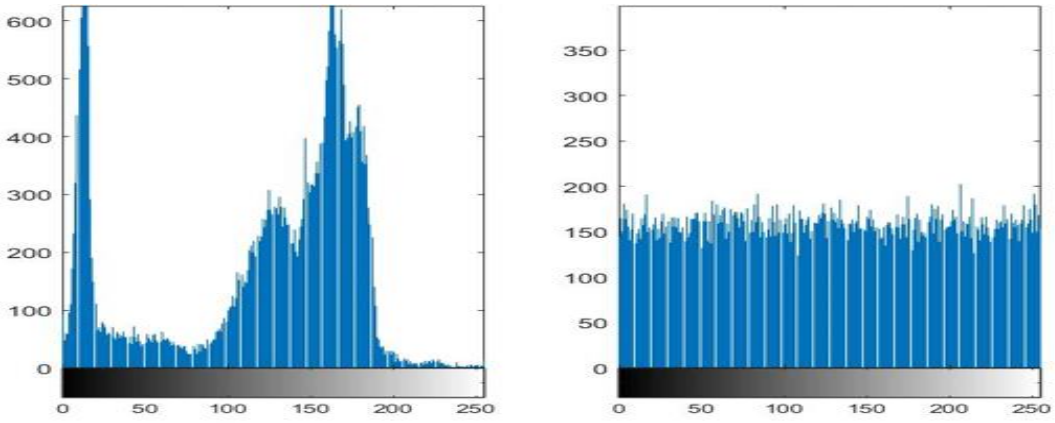
4.9.1 Analyzing the Histogram

The histogram depicts the distribution of the image's pixel values from 0 to 255. Because the pixel values are not evenly distributed and clustered within a preset interval, a high diffusion capacity image encryption system encrypts the plain image by changing the pixel values to achieve a uniform distribution. If the encryption is not uniform, an attacker can use statistical analysis to recover the original image. Figures 4.7 (a), (b), 4.8 (a), (b), 4.9 (a), (b) 4.10 (a), (b), 4.11 (a), (b), 4.12 (a), (b), 4.13(a), (b), 4.14 (a), (b), 4.15 (a), (b) 4.16 (a), (b) show plaintext images coupled with encrypted images and aslo illustrate histograms for both plain and cipher images. The findings indicate that the pixel values in each encryption image's histogram have a uniform distribution.



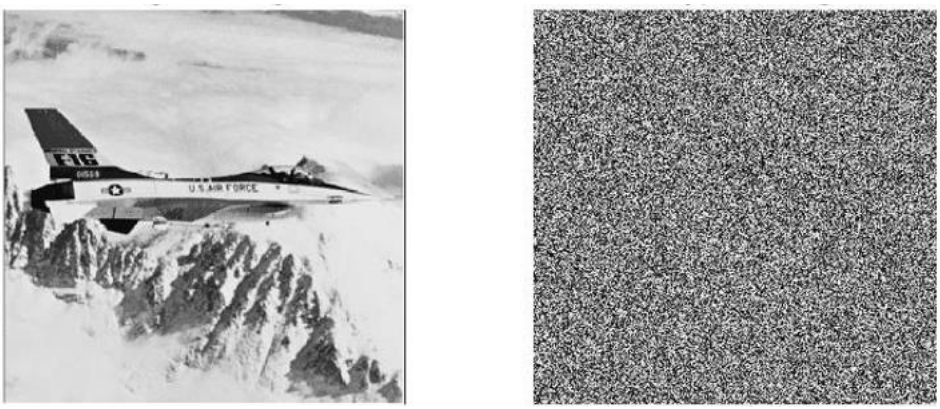
(a) (b)

Figure 4.7: (a) Cameraman (b) Encrypted Image



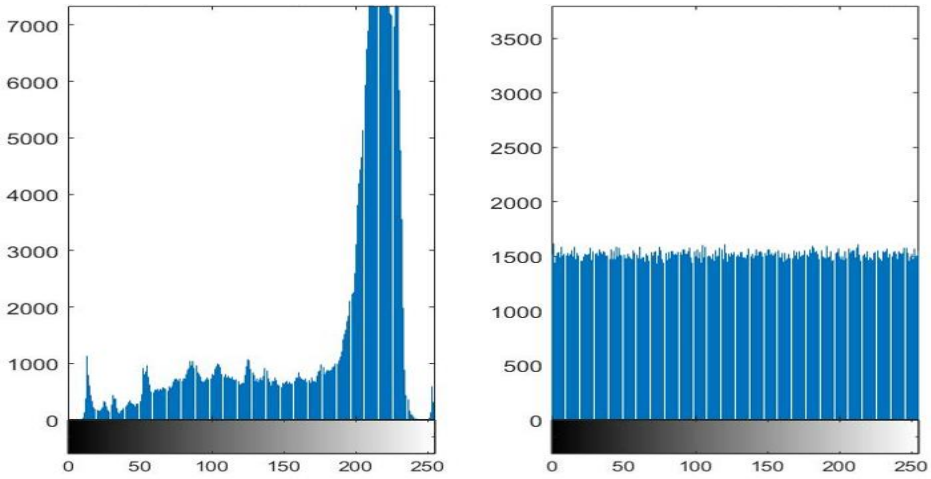
(a) (b)

Figure 4.8: Histogram (a) Plaintext Cameraman Image (b) Encrypted Image



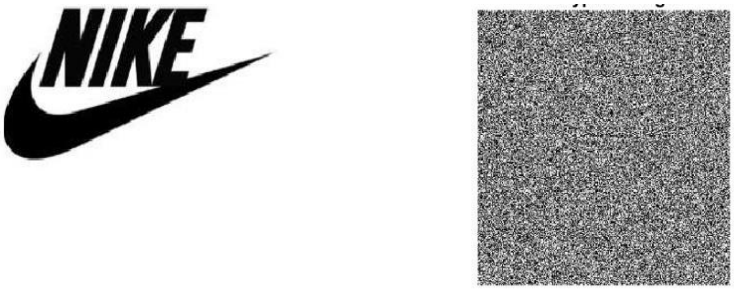
(a) (b)

Figure 4.9: (a) Plaintext Image of Airplane (b) Encrypted Image



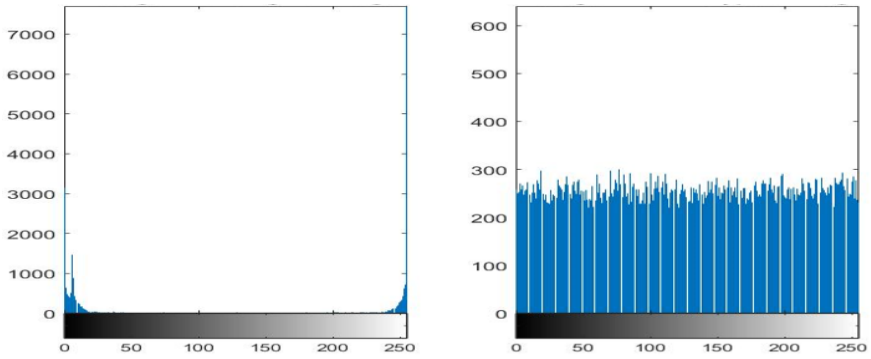
(a) (b)

Figure 4.10: Histogram (a) Plaintext Airplane Image (b) Encrypted Image



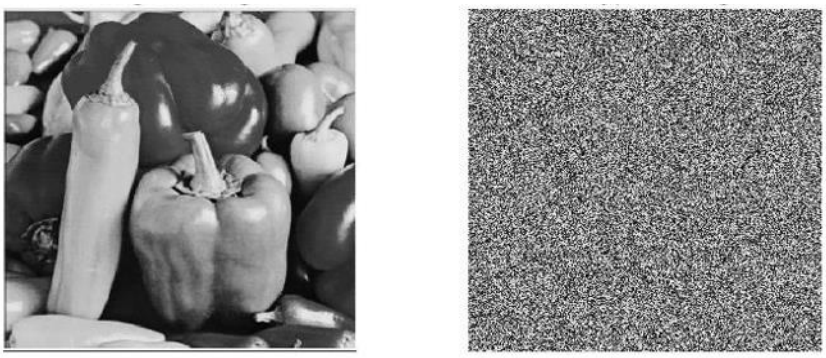
(a) (b)

Figure 4.11: (a) Plaintext Nike logo (b) Encrypted Image of Nike logo



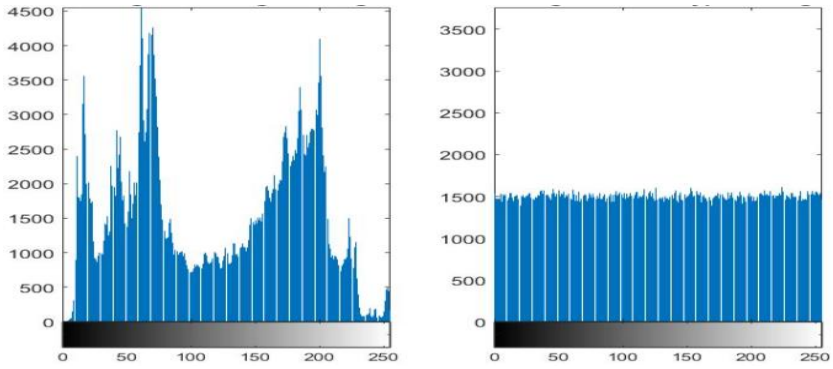
(a) (b)

Figure 4.12: Histogram (a) Plaintext Nike logo (b) Encrypted Image



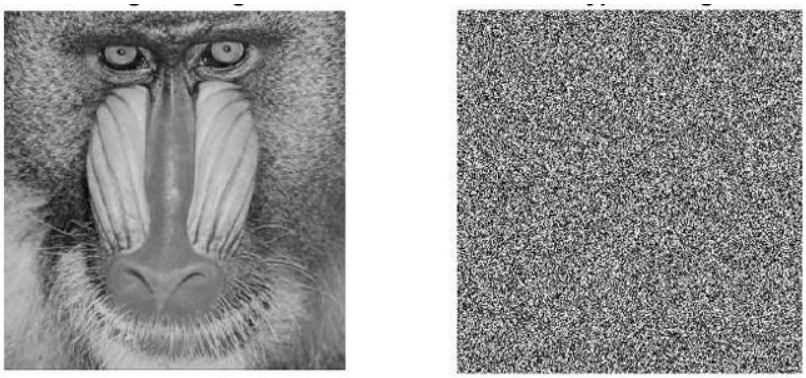
(a) (b)

Figure 4.13: (a) Plaintext Peppers Image (b) Encrypted Image



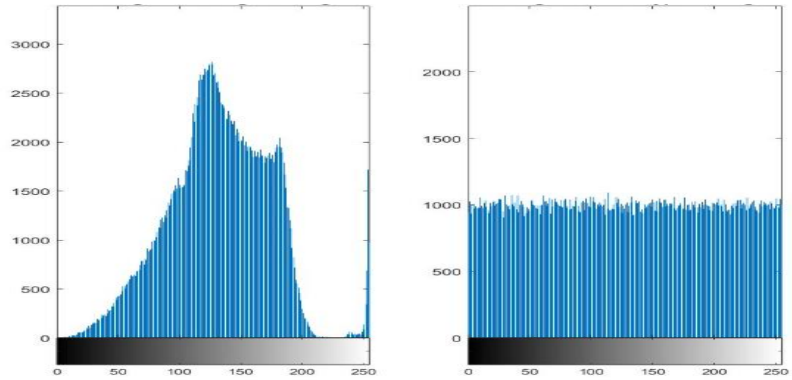
(a) (b)

Figure 4.14: Histogram Peppers Image (a) Plaintext (b) Encrypted Image



(a) (b)

Figure 4.15: (a) Baboon image (b) Encrypted Image of Baboon



(a) (b)

Figure 4.16: Histogram of Baboon Image (a) Plaintext (b) Encrypted image

4.9.2 Adjacent Pixel Correlation and Information Entropy

The computation equation of information entropy is given in equation 2.9 and adjacent pixel correlation are given in equation 2.10. Table 4.3 displays the information entropy for both plaintext and encrypted images. Table 4.4 compares the entropy of the "Airplane image". The correlation test method computes the plain image's distribution and coefficient of correlation in the horizontal, vertical, and diagonal directions by randomly selecting 4,000 nearby pixels from images and their corresponding cipher images. Table 4.1 displays the findings of the correlation coefficient computation, and Table 4.2 displays the comparison of the Airplane image.

4.10 Ability of Defending Differential Attack

Our experiment creates a new image by randomly selecting 200 pixels from the basic image and altering their values. A variety of image types are calculated with expected values using the encrypted NPCR and UACI. The UACI and NPCR for "Airplane image 512" are 34.7622% and 99.6221 percent, respectively. Table 4.5 contains NPCR and UACI results for all images. Table 4.6 compares the "Airplane Image" results by UACI and NPCR. The average NPCR and $UACI$ values for encrypted images are extremely close to the expected values.

Table 4.1: Correlation for all Three Directions for an Encrypted Images

Image	Horizontal		Vertical		Diagonal	
	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
Camera man	0.9339	0.0074	0.9646	-0.0058	0.9089	0.0011
Airplane	0.9721	-0.0039	0.9819	-0.0023	0.9561	-0.0015
Nike	0.9754	-0.0020	0.9772	0.0077	0.9422	0.0020
Peppers	0.9901	-0.0004	0.9781	0.0003	0.9686	0.0006
Baboon	0.9556	-0.0028	0.9249	0.0002	0.8881	0.0003

Table 4.2: Comparison of Airplane Image

Method	Proposed	Ref.[41]	Ref. [39]	Ref. [37]	Ref. [38]
Horizontal	-0.0039	0.0008	− 0.0048	0.0015	− 0.0008
Vertical	-0.0023	0.0004	− 0.0112	0.0043	− 0.0025
Diagonal	-0.0015	0.0020	− 0.0045	0.0023	0.0010

Table 4.3: Entropy Information for Original and Encrypted Images

Image	Entropy(Original image)	Entropy(Encrypted image)
Lena	7.4939	7.9995
Cameraman	7.1078	7.9958
Airplane	6.8092	7.9996
Nike	2.1719	7.9964
Peppers	7.6557	7.9995
Baboon	7.2890	7.9993

Table 4.4: Comparison of Information of Entropy for Airplane Image

Image	New Map	Ref.[41]	Ref. [39]	Ref. [38]
Airplane	7.9996	7.9995	7.9963	7.9992

Table 4.5: Average NPCR and UACI values for Different Plain Image

Image	*NPCR (%)*	*UACI (%)*
Cameraman	99.5995	31.0926
Airplane	99.6221	34.7622
Nike	99.5876	48.7516
Peppers	99.6037	32.0029
Baboon	99.6075	27.6983

Table 4.6: Comparison of NPCR and UACI Results for Airplane Image

Algorithm	*NPCR%*	*UACI%*
New Map	99.6221	34.7622
Ref.[41]	99.2100	33.5900
Ref. [40]	99.6193	33.4286

4.11 High Quality Encryption

Lossless encryption is achieved by the proposed image encryption method when the plain and decrypted images are identical. When the root mean square error (RMSE) becomes zero, the images are identical. It is impossible to differentiate the image when the peak signal noise ratio (PSNR) is higher than 30 db. Table 4.7 shows the irregular mean squared error (RMSE) and peak signal noise ratio (PSNR) values for each image.

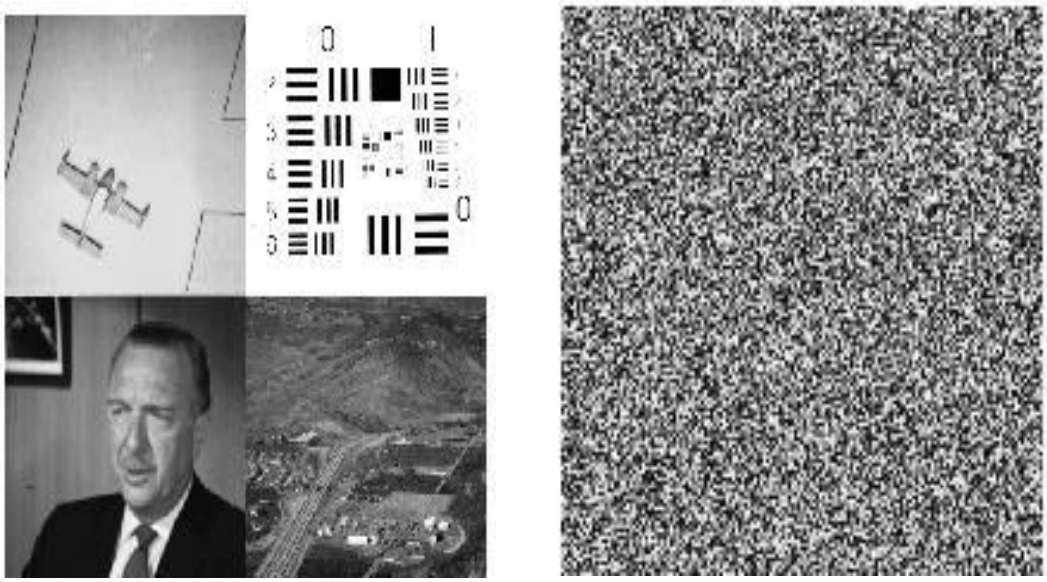
Table 4.7: RMSE and PSNR values

Image	RMSE	PSNR
Cameraman	97.1562	8.3814
Airplane	108.5322	7.4196
Nike	144.8709	4.9112
Peppers	99.7535	8.1522
Baboon	84.6889	9.5743

4.12 Multiple Image Encryption

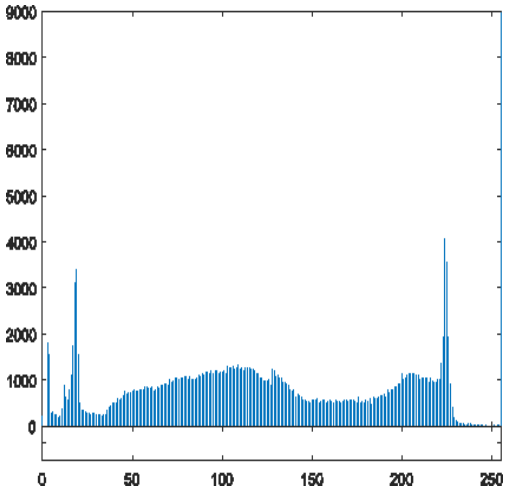
This study proposes a novel multiple-image encryption (MIE) approach based on modified piecewise chaotic mappings (MPCM) to improve encryption efficiency and allow for the secure transmission of large amounts of images. Alice (the sender) first merges original images into a single, huge image, then splits into several pure image parts to generate mixed image elements. The mixed images parts are then combined to create a big-scrambled image, which is then divided into smaller images of the same size as the originals. Finally, uses filenames generated by a different MPCM system to name these tiny, encrypted images as shown in Figure 4.17 (a) and (b). In the meantime, a comparative analysis is conducted with an existing algorithm that is similar.

The new algorithm is highly secure and efficient, according to algorithm analysis and experimental results. Figure 4.18 (a) and (b) is about histogram analysis of multiple images and Table 4.6 is correlation of all three direction of encrypted images. Comparison for Information of entropy image is shown in Table 4.7 and Table 4.8 is about NPCR and UACI comparison. RMSE and PSNR value are shown in Table 4.9.

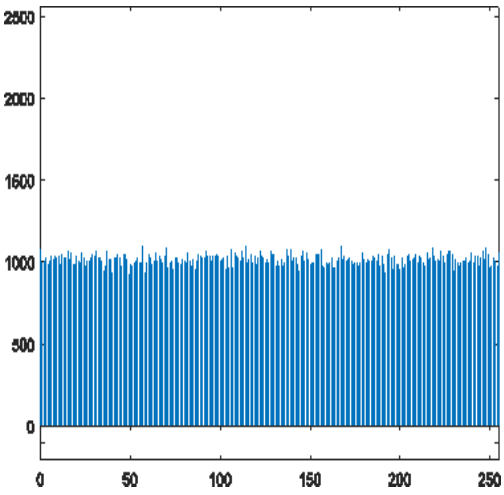


(a) (b)

Figure 4.17 (a) Multiple Images (b) Encrypted Images



(a)



(b)

Fig 4.18 (a) Histogram of original image and (b) Encrypted multiple images

Table 4.6: Correlation Comparison for all Three Directions of an Encrypted Image

Multiple Image	Plain Image	Cipher Image	Ref.[41]
Horizontal	0.9669	0.0015	-0.0014
Vertical	0.9818	-0.0001	-0.0013
Diagonal	0.9521	0.0014	0.0184

Table 4.7: Comparison of Information Entropy for Multiple Image

Image	New Map	Ref.[42]	Ref.[39]
Multiple image	7.9955	7.9952	7.9963

Table 4.8: Comparison between Multiple Image NPCR and UACI

Multiple Image	NPCR%	UACI%
New Map	99.6168	36.3132
Ref.[41]	99.2100	33.5900
Ref. [40]	99.6193	33.4286
Ref.[42]	99.6078	33.4741

Table 4.9: RMSE and PSNR values of Multiple Images

Image	RMSE	PSNR
Multiple images	90.2239	90.0223

CHAPTER 5

CONCLUSION AND FUTURE WORK

5.1 Conclusion

The proposed image encryption scheme leveraging the modified piecewise chaotic map (MPCM) and the Coupled MPCM (CMPCM) demonstrates strong potential in providing robust and sensitive image encryption. The proposed scheme offers a promising foundation for secure image encryption using chaotic systems. With the aforementioned extensions, the system can evolve into a comprehensive solution capable of addressing modern data security challenges in multimedia and communication technologies.

5.2 Future direction

There are several important directions in which this research can be extended to further enhance its performance, applicability and security.

5.2.1 Full-Color Image Encryption

At present, the encryption scheme converts RGB images into grayscale before processing. To maintain color fidelity and increase the complexity of the cipher, future extensions can involve the separate or joint encryption of the red, green, and blue channels. This would not only preserve image quality but also enhance security due to the higher dimensionality of the input data.

5.2.2 Adaptive Chaos Control Parameters

Currently, the control parameters μ and λ used in the chaotic map are static. A more dynamic approach could involve making these parameters adaptive or image-dependent. For example, control parameters can be generated based on a cryptographic hash of the image content or an external secure key. This would improve key sensitivity and bolster resistance against known-plaintext and chosen-plaintext attacks.

5.2.3 Extension to Video and Volumetric Data Encryption

The methodology can be extended to encrypt video sequences or three-dimensional data such as medical imaging (e.g., MRI, CT scans). This would

involve the use of temporal and spatial chaos synchronization to preserve frame-to-frame consistency while maintaining security.

5.2.4 Hybrid Cryptographic Models

Combining chaos-based encryption with other cryptographic paradigms such as DNA computing, elliptic curve cryptography, or lattice-based encryption could lead to the development of hybrid models. These models can exploit the advantages of both approaches to create systems that are highly secure, computationally efficient, and adaptable to various data types.

The proposed scheme offers a promising foundation for secure image encryption using chaotic systems. With the aforementioned extensions, the system can evolve into a comprehensive solution capable of addressing modern data security challenges in multimedia and communication technologies.

References

[1] J. Fridrich, "Image encryption based on chaotic maps," in *1997 IEEE International Conference on Systems, Man, and Cybernetics. Computational Cybernetics and Simulation*, vol. 2, pp. 1105–1110, Oct. 1997.

[2] I. Yasser, F. Khalifa, M. A. Mohamed, and A. S. Samrah, "A new image encryption scheme based on hybrid chaotic maps," *Complexity*, 2020.

[3] A. S. Menon and K. S. Sarila, "Image encryption based on chaotic algorithms: An overview," *International Journal of Science, Engineering and Technology Research*, vol. 2, no. 6, pp. 1328–1332, 2013.

[4] E. Yavuz, R. Yazıcı, M. C. Kasapbaşı, and E. Yamaç, "A chaos-based image encryption algorithm with simple logical functions," *Computers & Electrical Engineering*, vol. 54, pp. 471–483, 2016.

[5] L. Kocarev, "Chaos-based cryptography: a brief overview," *IEEE Circuits and Systems Magazine*, vol. 1, no. 3, pp. 6–21, 2001.

[6] I. Hussain and T. Shah, "Literature survey on nonlinear components and chaotic nonlinear components of block ciphers," *Nonlinear Dynamics*, vol. 74, no. 4, pp. 869–904, 2013.

[7] N. McDonald, "Past, present, and future methods of cryptography and data encryption. A Research Review," 2009. [Online]. Available: http://www.eng.utah.edu/~nmcdonal/Tutorials/EncryptionResearchReview.pdf

[8] D. Pointcheval, "Asymmetric cryptography and practical security," *Journal of Telecommunications and Information Technology*, pp. 41–56, 2002.

[9] S. K. Rakeshkumar, "Performance analysis of data encryption standard algorithm & proposed data encryption standard algorithm," *International Journal of Engineering Research and Development*, vol. 7, no. 10, pp. 11–20, 2013.

[10] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[11] Y. Wu, Y. Gelan, H. Jin, and J. P. Noonan, "Image encryption using the two-dimensional logistic chaotic map," *Journal of Electronic Imaging*, vol. 21, no. 1, p. 013014, 2012.

[12] Z. Hua, Y. Zhou, C. M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.

[13] A. Ullah, S. S. Jamal, and T. Shah, "A novel construction of substitution box using a combination of chaotic maps with improved chaotic range," *Nonlinear Dynamics*, 2017.

[14] G. P. Williams, *Chaos Theory Tamed*, Joseph Henry Press, 1997. https://books.google.com/books/about/Chaos_Theory_Tamed.html?id=G6ePyAEACAAJ

[15] W. Trappe, *Introduction to Cryptography with Coding Theory*, Pearson Education India, 2006. https://www.math.umd.edu/~lcw/book.html

[16] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324–332, 2017.

[17] H. W. Safi and A. Y. Maghari, "Image encryption using double chaotic logistic map," in *2017 International Conference on Promising Electronic Technologies (ICPET)*, IEEE, pp. 66–70, Oct. 2017.

[18] K. R. Radhika and M. K. Nalini, "Biometric image encryption using DNA sequences and chaotic systems," in *2017 International Conference on Recent Advances in Electronics and Communication Technology (ICRAECT)*, IEEE, pp. 164–168, Mar. 2017.

[19] M. S. Khrisat, Z. Alqadi, and S. A. Khawatreh, "Improving WPT color image decomposition," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 18, no. 7, 2020.

[20] Y. Eltous, A. M. Hamarchi, M. S. Khrisat, S. A. Khawatreh, and Z. Alqadi, "Color image encryption-decryption using random noise and PMT."

[21] J. Zhang and D. Huo, "Image encryption algorithm based on quantum chaotic map and DNA coding," *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 15605–15621, 2019.

[22] H. Liu and C. Jin, "A novel color image encryption algorithm based on quantum chaos sequence," *3D Research*, vol. 8, no. 1, p. 4, 2017.

[23] T. Sivakumar and R. Venkatesan, "A new image encryption method based on knight's travel path and true random number," *Journal of Information Science & Engineering*, vol. 32, no. 1, 2016.

[24] N. Masuda and K. Aihara, "Cryptosystems with discretized chaotic maps," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 49, no. 1, pp. 28–40, 2002.

[25] W. K. S. Tang and Y. Liu, "Formation of high-dimensional chaotic maps and their uses in cryptography," in *Chaos-based Cryptography: Theory, Algorithms and Applications*, Springer Berlin Heidelberg, 2011, pp. 99–136.

[26] E. W. Weisstein, "Logistic map," *MathWorld—A Wolfram Web Resource*, 2001. [Online]. Available: https://mathworld.wolfram.com/LogisticMap.html

[27] A. Biryukov and D. Wagner, "Advanced slide attacks," in *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, pp. 589–606, May 2000.

[28] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," *IEEE Transactions on Image Processing*, vol. 13, no. 4, pp. 600–612, 2004.

[29] Z. Tang, J. Cui, H. Zhong, and M. Yu, "A random PRESENT encryption algorithm based on dynamic S-BOX," *International Journal of Security and Its Applications*, vol. 10, no. 3, pp. 383–392, 2016.

[30] M. Elhoseny et al., "A survey on chaotic encryption algorithms for secure image transmission," *Future Generation Computer Systems*, vol. 79, pp. 58–75, 2018.

[31] A. Mishra, "Advances in chaos-based image encryption systems," *Information Security Journal: A Global Perspective*, vol. 27, no. 3, pp. 149–167, 2018.

[32] Z. Chen and C. Liu, "A novel image encryption algorithm based on chaotic system," *International Journal of Computer Applications*, vol. 171, no. 9, pp. 34–40, 2017.

[33] S. Padhy et al., "A review of image encryption techniques based on chaotic maps," *Procedia Computer Science*, vol. 171, pp. 2210–2217, 2020.

[34] W. F. Al-Shameri, "Dynamical properties of the Hénon mapping," *International Journal of Mathematical Analysis*, vol. 6, no. 49, pp. 2419–2430, 2012.

[35] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution–permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[36] J. Chen, Z. L. Zhu, L. B. Zhang, Y. Zhang, and B. Q. Yang, "Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption," *Signal Processing*, vol. 142, pp. 340–353, 2018.

[37] Z. Hua and Y. Zhou, "Image encryption using 2D logistic-adjusted sine map," *Information Sciences*, vol. 339, pp. 237–253, 2016.

[38] P. Ping, J. Fan, Y. Mao, F. Xu, and J. Gao, "A chaos based image encryption scheme using digit-level permutation and block diffusion," *IEEE Access*, vol. 6, pp. 67581–67593, 2018.

[39] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution–permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[40] K. Panwar, R. K. Purwar, and A. Jain, "Cryptanalysis and improvement of a color image encryption scheme based on DNA sequences and multiple 1D chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 29, no. 8, p. 1950103, 2019.

[41] "A secure image encryption scheme based on a novel 2D sine–cosine cross-chaotic (SC3) map," *Journal of Real-Time Image Processing*, vol. 18, no. 1, pp. 1–18, 2021. doi: 10.1007/s11554-019-00940.

[42] J. Wei, M. Zhang, and X. Tong, "Multi-Image Compression–Encryption Algorithm Based on Compressed Sensing and Optical Encryption," Entropy, vol. 24, no. 6, p. 784, Jun. 2022, doi: 10.3390/e24060784