AN EFFICIENT ENCRYPTION TECHNIQUE BASED ON COUPLED MAP LATTICES

By

Rabia Riaz

NATIONAL UNIVERSITY OF MODERN LANGUAGES
ISLAMABAD

January, 2026

AN EFFICIENT ENCRYPTION TECHNIQUE BASED ON COUPLED MAP LATTICES

By

Rabia Riaz

MS MATH, NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD, 2026

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF

THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

In MATHEMATICS

TO

FACULTY OF ENGINEERING & COMPUTING

NATIONAL UNIVERSITY OF MODERN LANGUAGES ISLAMABAD

THESIS AND DEFENSE APPROVAL FORM

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

Thesis Title: An Efficient Encryption Technique Based on Coupled Map Lattices

Submitted By: Rabia Riaz **Registration #:**96 MS/MATH/F23

Master of Science in Mathematics

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

Signature of HOD

Dr. Noman Malik

Name of Dean (FES)

Signature of Dean (FEC)

January 2, 2026

AUTHOR'S DECLARATION

I Rabia Riaz

Daughter of Riaz Ahmed

Registration 96 MS/MATH/F23

Discipline Mathematics

Candidate of Master of Science in Mathematics at the National University of Modern Languages do hereby declare that the thesis An Efficient Encryption Technique Based on Coupled Map Lattices submitted by me in partial fulfillment of MS degree, is my original work and has not been submitted or published earlier. I also solemnly declare that it shall not, in the 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

Rabia Riaz

Name of Candidate

January 2, 2026

Date

ABSTRACT

Title: An Efficient Encryption Technique Based on Coupled Map Lattices

This study introduces a highly secure image encryption technique based on coupled map lattices (CMLs), a class of chaotic systems known for their sensitivity to initial conditions and spatiotemporal complexity. The CMLs offer an ideal foundation for encryption due to its ability to generate unpredictable and nonlinear transformations.

Although several chaos-based encryption methods have been explored in the past, many suffer from narrow parameter ranges, limited key spaces, or insufficient resistance to modern cryptographic attacks. To address these issues, we propose a novel two-parameter wide-range CMLs model that enhances key generation and improves chaotic behavior across a broader parameter space. The encryption process employs a dynamic key schedule, pixel permutation, and modular diffusion using CMLs-generated sequences.

Comprehensive experimental evaluations demonstrate that the proposed method ensures high entropy, minimal pixel correlation, and strong resistance to brute-force, occlusion, noise, and differential attacks. It also outperforms existing techniques in both computational efficiency and encryption strength.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

PR	-	Private Key
PU	-	Public Key
AES	-	Asymmetric Key Cryptography
DES	-	Data Encryption Standard
TCML	-	Two Way Coupled Logistic Map Lattices
2DNLCML	-	Two Dimensional Nonlinear Coupled Map Lattices
CKNR	-	Chaotic Key Number Generation
PSNR	-	Peak Signal-to-Noise Ratio
PRNG	-	Pseudorandom Number Generator
CPA	-	Chosen-Plaintext Attack
CCA	-	Chosen-Ciphertext Attack
KPA	-	Known Plaintext Attack
COA	-	Ciphertext Only Attack
MITM	-	Man in the Middle Attack
CCCM	-	Compound-Coupled Chaotic Model
LE	-	Lyapunov Exponent
KE	-	Kolmogorov Entropy
CD	-	Correlation Dimension
ApEn	-	Approximation Entropy
MSE	-	Mean Square Error
UACI	-	Unified Average Changing Intensity
NPCR	-	Number of Changing Pixels Rate
	-	

LIST OF SYMBOLS

M	-	Plaintext or Message
C	-	Ciphertext
E	-	Encryption Algorithm
D	-	Decryption Algorithm
PR	-	Private Key
PU	-	Public Key
SHA	-	Hash Function
1D	-	One Dimension
2D	-	Two Dimension
IE	-	Information Entropy

ACKNOWLEDGMENT

I would like to start by expressing profound gratitude to Almighty Allah, whose mercy supported and encouraged this research work. Without the incredible cooperation and efforts of several people, for whom I am very thankful, the work would not have been finished.

Foremost, I would like to convey my sincere gratitude to Dr.Ghulam Murtaza, my research supervisor, who gave me continuous guidance and did all in his ability to help me along on this journey. I was well-served by his unwavering support and patience. His substantial contribution to one of my life's most successful endeavours is something I will always remember. This work was made possible in a significant way by his mentoring, and it was a pleasure to learn under supervision.

I am also incredibly thankful to the teachers who have guided and supported me throughout my academic journey.I really appreciate our HOD, Dr. Anum Naseem providing us with a research environment and kind support. I really want to say thanks to our respected teachers, Dr. Shehzad Khattak, Dr. Muhammad Rizwan, Dr. Sadia Riaz , Dr. Hadia Tariq, Dr. Asia, Dr.Shabeela and other teachers, for their guidance and support.

Additionally, I would like to thank the administration of the mathematics departments for their essential help, which greatly facilitated this research process. Their collaboration made it easier for me to overcome the obstacles I faced. I want to sincerely thank everyone who has helped along the way, whether or not they are mentioned here, for their encouragement and support.

DEDICATION

"No journey worth taking is walked alone; it takes both our determination and the heartfelt support of those who truly matter."

My little effort I dedicate to my beloved

Parents

"Behind every success story is the silent sacrifice and unconditional love of parents."

CHAPTER 1

INTRODUCTION AND LITERATURE REVIEW

This chapter explores chaotic systems in contemporary cryptography, comparing them with established techniques like AES and RSA. Deterministic chaos offers advantages like erratic key streams and effective diffusion-confusion processes. Early 1D systems had limitations like limited parameter spaces and brute-force attacks. Modern systems like coupled map lattices and 3D Lorenz attractors address these shortcomings may be instead. The chapter emphasizes advancements in security claims, key lengths, formal security proofs, benchmarks, and efficient implementations for limited resources.

1.1 Cryptography and Data Security

Information shared in electronic media has increased significantly in recent years. There are threats to data transmitted through insecure channels due to technological advances. Information must be protected from unauthorized access and changes and made available to an authorized person when necessary. Secret writing hides information within ordinary files or communication channels to prevent detection [1]. The primary goal of cryptography is secret writing, or crafting the message so that only the intended person can decode it. It is essential to protect the security and confidentiality of transmitted data.

Cryptography and data security are among the most significant scientific advances of the last century. Cryptographers have proposed numerous techniques for data security. The three basic categories of these techniques are cryptography, steganography, and watermarking. In cryptography, the original information is transformed into an unreadable form before communicating on a public network [2]. We can send or store private information over unsecured networks like the Internet. It guarantees that only the intended recipient can access it [3]. The science of studying

and cracking encrypted communication is known as cryptanalysis. Cryptography, a key-based encryption process, protects information from unauthorized access. It is divided into two main categories: symmetric and asymmetric. In symmetric cryptography, the sender and recipient share the same key for encryption and decryption. In contrast, asymmetric-key cryptography uses a public key that is accessible to everyone and a key that is only known by authorized users. Traditional cryptographic techniques are successful but have drawbacks, including high computing cost, susceptibility to side channel attacks, and limited flexibility in low-resource settings such as the Internet of Things [4].

1.1.1 Purpose and Need for Cryptography

In addition to protecting messages, cryptography also solves real-world problems that require data security. Its primary goals in the modern era are [5]:

- **Confidentiality:** Two basic features of confidentiality are privacy and data confidentiality.
    a. **Privacy:** Authorization assures one's personal information won't be violated.
    b. **Data Confidentiality:** It is assured that attackers will either learn about or not be able to access confidential or personal information.
- **Integrity:** Integrity includes the following:
    a. **System Integrity:** A system aware of fulfilling the suggested concepts without interference and unauthorized exploitation.
    b. **Data Integrity:** There is a guarantee that the data are only legally recreated.
- **Authenticity:** The skill involves recognizing the individuals communicating and the source of the data.
- **Availability:** The scheme's accessibility to certified owners is modified to their specific needs.

1.2 Chaos Theory

Chaos theory studies deterministic systems that behave in seemingly random and unpredictable ways [6]. A characteristic of these systems is their extreme sensitivity to initial conditions and the "butterfly effect." This property, together with pseudo-randomness and ergodicity (uniform distribution of states), makes chaotic systems ideal for cryptography applications. Chaos theory in cryptography began in the last decades of the twentieth century when researchers

demonstrated how chaotic maps may offer secure encryption keys and diffusion processes [7]. Chaos-based encryption is a viable substitute for conventional cryptographic techniques because it provides dynamic key creation, faster computing, and resilience to statistical attacks [8].

1.2.1 Advantages of Chaotic Systems

Although chaotic systems have several benefits for encryption:

1. High Sensitivity to Initial Conditions: Chaotic sequences are extremely unpredictable because even small changes in starting values or parameters can produce distinct results.

2. Ergodicity: The uniform coverage of the phase space by chaotic systems guarantees that the sequences produced are evenly dispersed, which is essential for encryption diffusion.

3. Computational Efficiency: One-dimensional chaotic maps, such as the logistic map, are appropriate for real-time encryption since they need less processing power.

1.2.2 Drawbacks of Chaotic System

In addition, they have several drawbacks that reduce their efficacy as independent cryptography. The main disadvantages are listed below:

1. Restricted Chaotic Range: The chaotic behavior of many chaotic maps, such as the logistic map, is limited to a small parameter range (e.g., $\mu \in [3.57, 4]$), which limits the key space.

2. Periodic Windows: Non-chaotic areas are frequently included in bifurcation diagrams of chaotic maps, which lowers security and unpredictability.

3. Low-Dimensional Vulnerability: The power of standalone cryptography is limited by the vulnerability of simple 1D chaotic maps to phase space reconstruction attacks.

1.3 Need for New Chaotic Maps in Modern Cryptography

Chaotic maps, such as Tent and Logistic maps, are commonly used in encryption but have limitations [9]. They are vulnerable to brute-force attacks due to their small key spaces and non-uniform results, exploited through frequency analysis [10]. Low-dimensional chaotic maps, like 1D systems, have computing efficiency, but lack the complexity needed for strong security [11]. High-dimensional chaotic systems, such as 3D Lorenz, require substantial computing costs for real-time implementation on limited resources, making them unsuitable for modern cryptographic applications [12].

Coupled Map Lattices (CMLs) have been explored as a better option for addressing security issues [13]. CMLs offer a broader key space, improved resistance against brute-force attacks, and better chaotic behavior. They also preserve computational efficiency, making them suitable

for real-time encryption. By combining spatial coupling with nonlinear interactions, CMLs offer a balance between security, complexity, and performance.

1.4 Role of Chaotic Maps

Chaotic maps, mathematical functions with dense periodic orbits and topological mixing, have become a revolutionary tool in contemporary cryptography due to their dynamical characteristics [14]. These maps produce predictable pseudorandom sequences, providing a significant advantage over conventional techniques for encryption, ensuring secure communication systems. Chaotic maps are effective for image and video encryption because they break spatial correlations through permutation and diffusion [15]. They increase complexity, making spatiotemporal systems like coupled map lattices impervious to statistical techniques. Chaotic maps also play a role in dynamic S-box design, improving block ciphers' confusion features and enhancing resistance to differential cryptanalysis [16].

Despite their advantages, chaotic maps face challenges in formal security proofs and standardization. Unlike AES or RSA, which have strong mathematical foundations, they often require empirical validation through statistical testing [17]. Future research should focus on developing theoretical frameworks and refining hardware implementations for practical use, thereby pushing the boundaries of secure communication and post-quantum cryptography.

1.5 Chaotic Maps in Image Encryption

Because of their ergodicity, pseudo-random behaviour, and sensitivity to initial conditions, chaotic maps are very useful for image encryption. They meet cryptography requirements, offer computational efficiency, and can produce intricate sequences, making them resistant to attacks [18]. Chaotic maps also provide inherent confusion and diffusion, ensuring that even minor changes to the input image yield distinct encrypted outputs. Chaotic maps have potential security issues due to weak keys, predictable behavior, periodic sequences, lack of universal certification, and difficulty in key management due to high-precision floating-point parameters [19]. If not properly built, they are also susceptible to chosen-plaintext and known-plaintext attacks, making their use in high-security sectors less secure than established algorithms like AES.

Chaotic maps effectively encrypt images, especially in situations requiring speed and dynamic security [20]. However, their success depends on their implementation, integration with other cryptographic methods, and resolution of accuracy issues. Traditional techniques may be better for strict standards, but hybrid strategies combining chaos theory with algorithms can offer a strong security-performance balance [21].

Complex mathematical structures with complicated, unpredictable dynamics are known as chaotic systems. Creating encryption keys in cryptography is one of many uses for this characteristic. From their chaotic trajectories, chaotic systems may also be used to derive genuine randomness [22]. It is possible to generate samples and modify high-quality random numbers appropriate for a range of cryptographic applications. Using chaotic trajectories and their sensitivity to initial conditions, we can develop security techniques resistant to specific attacks, thus improving the strength of encryption [23]. Chaotic maps require careful implementation and analysis, even if they might be a valuable source of unpredictability for key creation [24]. The efficacy of the key generation process depends on several factors, including parameter selection, map choice, and security concerns [25]. Furthermore, preventing prospective attackers from knowing the beginning state and other characteristics is essential to the system's security [26]. Generating a chaotic map key is crucial to improving data protection and advancing cryptography in the communication sector. Like mathematical riddles, chaotic systems demonstrate how even little adjustments may have unexpected and startling effects [27]. There are practical applications for this unpredictability, such as creating secure messaging secret codes and assisting in comprehending weather patterns [28]. Chaos serves as a reminder that, despite the complexity, there may be a hidden order that has applications in everything from science to protecting our digital world [29].

Because of its unpredictable pseudo-randomness and sensitivity to initial values, a chaotic system is frequently utilized in digital image encryption. Examples of chaotic systems are one-dimensional, multidimensional, spatiotemporal, and other types of chaotic maps. Spatial-temporal chaotic systems exhibit more complicated chaotic behaviours, a broader chaotic area, and lower computer overhead when compared to other chaotic systems. Applications for chaos include secure communication, cryptography, and random number generation, where the capacity to generate highly complicated and unpredictable pseudo-random sequences is essential [30]. Researchers can investigate and utilize the rich dynamics of chaotic systems for functional goals while guaranteeing robustness and security in digital systems by carefully managing the digital perturbations.

1.5.1 Chaotic Image Encryption Using Block Cipher

Block ciphers divide plaintext into equal-sized blocks, encrypting each separately [31]. Chaotic image encryption ensures high security using a chaotic map. Scharinger proposed a technique based on Kolmogorov flows, processing full images as complete blocks.

The image-encryption approach uses logistic mapping and a discrete 3D Cat map to distribute XOR and shuffle cubes, obtaining an encrypted image after reorganization and restoration to two dimensions, as shown in Figure 1.1. Because of the association between the red (R), green (G),

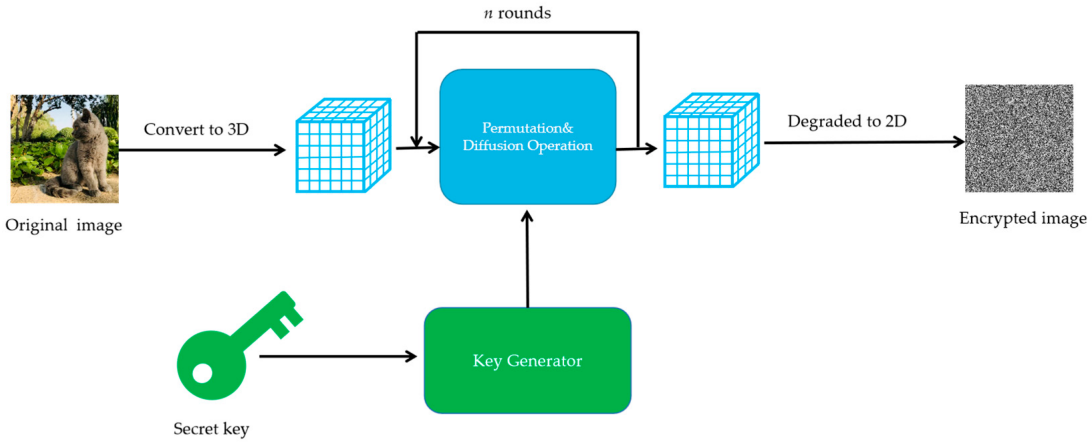


Figure 1.1: The Algorithm of the Image-Encryption Process

and blue (B) channels, color image encryption has to be improved in a few areas. Controlling these channels throughout the encryption process is essential to guaranteeing data integrity and confidentiality. More studies are required to create practical encryption algorithms for color image. Using a 2D standard map and a 1D logistic map, Vinod Patidar and N. K. Pareek [32] presented a symmetric image-encryption scheme that recovers the blue, red, and green channels for XOR confusion and diffusion operations.

1.5.2 Chaos-Based Image Encryption Using Stream Ciphers

Because of their speed and security, stream ciphers are frequently utilized in cryptographic fields. The method's security is directly affected by the keystream generator's performance. Combining chaotic systems with stream ciphers requires the integration of chaotic maps and keystream generators, with the primary technique being the construction of keystream generators with chaotic systems [33].

Stream ciphers are used in traditional chaotic image encryption systems, although they have limitations such as limited key spaces and low security. The coupling of low-dimensional chaotic maps provides a novel method for image encryption based on stream ciphers. Shubo Liu and Jing Sun [34] introduced a linked logistic map as a keystream generator, while Sahar Mazloom and Amir Masud Eftekhari-Moghadam [35] suggested a chaos-based symmetric streaming method for encrypting color images.

Researchers are developing new image-encryption methods by combining chaotic and frequency-

domain encryption. Preprocessing is required, as seen in Figure 1.2.

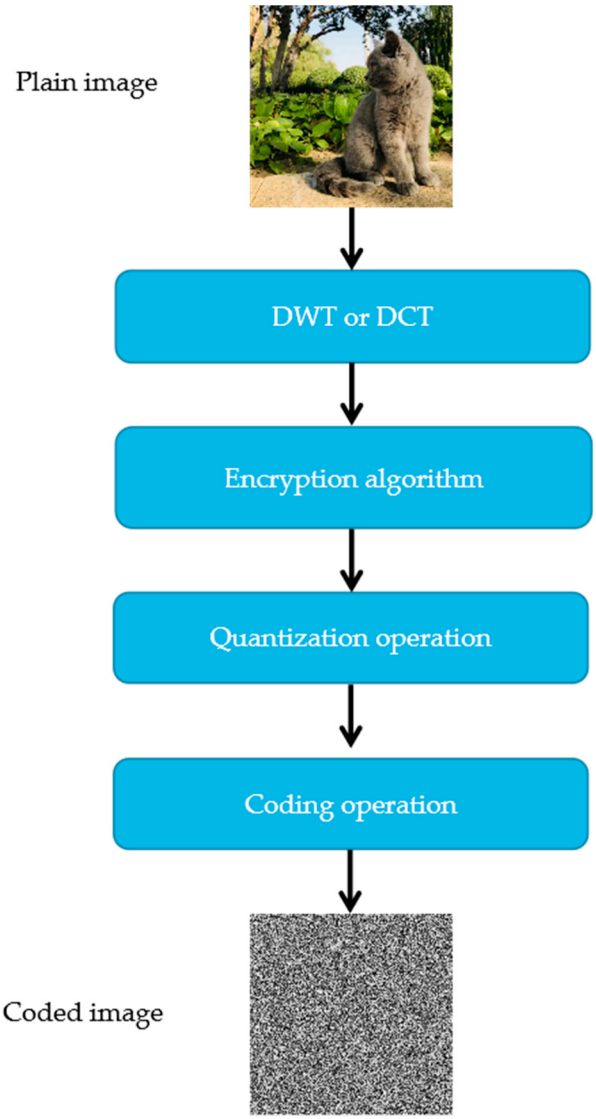


Figure 1.2: Frequency-Domain Image Encryption Process

1.6 CML-Based Image Encryption

The early chaotic systems, such as low-dimensional systems, suffered from the drawback of small key spaces. They were easily resistant to brute-force attacks, leading to the use of high-dimensional systems such as Coupled Map Lattices (CMLs), which offered a much larger key space and higher complexity, hence making them better suited to resist cryptanalytic methods than the low-dimensional systems. In [36], the author introduced the first coupled map lattices (CMLs) in 1982, a high-dimensional chaotic system. CML and other coupled map lattices have very complex spatiotemporal behaviour and are also good candidates for image encryption because of their chaotic behaviour. Researchers are still enhancing the chaotic properties of

CMLs [37] to improve the encryption process. In [38], the authors proposed the two-way coupled logistic map lattices (TCMLs) that increases the chaotic range, which leads to an increase in the security of the encryption process. The authors in [39] proposed another system, the nonlinear coupled map lattices model, that combines the system's linear dynamics and nonlinear dynamics, increasing the unpredictability of the chaotic system.

Kapral modelled [40] chemical spatial phenomena using CMLs, by creating a renormalisation group technique. In [41], the author attempted to apply CMLs to electrical circuits. Although Kaneko's concentration was broader, he remains the most active researcher in this field. The study in [42] proposed a novel dynamical chaotic system to produce random numbers. In [43], the authors proposed cryptosystems based on S-boxes generated by chaotic maps. Researchers in [44] used a new approach that differed from standard chaotic maps to create chaos-based S-boxes.

According to [45], the system has a large parameter space compared to traditional CMLs, and each lattice phase is more efficient. The approach is appropriate for both secured communications and chaotic encryption. In [46], the author suggests an alternative image encryption method that uses CMLs spatially.

1.7 Applications of Image Encryption Based on Chaos Theory

The worldwide Internet of Things, satellites, and medical devices extensively use chaos-based image encryption technologies. Techniques like bifurcation, open loop, and delayed feedback control manage chaotic systems such as robotics, cryptography, mechanical engineering, electrical engineering, and aeronautical engineering. These methods are crucial for stabilizing the inputs and parameters of the system, which makes them applicable in various fields [47].

1.7.1 Chaos-Based Medical Image Encryption

In [48], mammography image encryption uses the Hill cypher and a chaotic system. An FPGA-based encryption processor may be designed using the suggested method's symmetric algorithm. In [49], a logistic-map-based technique was presented for the safe online transfer of medical images over public networks. Akram Belazi and Muhammad Talha [50] used DNA technology, a hash function, and chaotic systems to create a medical image encryption method. To safeguard the confidentiality of patients and medical data, the paper's authors proposed a medical image encryption system [51] that uses chaotic maps and dynamic replacement boxes. Behrouz and Saleh [52] have presented a dynamic terminal mode sliding tracking technique for sender-receiver synchronisation. Medical image encryption uses synchronized chaotic systems

to increase storage or transmission protection. The study demonstrates chaos theory's security in medical image encryption, outperforming traditional algorithms due to its robustness and effectiveness through various analysis methods.

1.7.2 Chaos Image Encryption for Internet of Things Devices

The IoT expands the network of Internet-based devices, enabling the interconnectedness of people, machines, and objects anytime and anywhere. Despite steady development in the past decade, technology, administration, and security issues remain. To enhance security, academics have attempted to implement chaotic encryption techniques, addressing the need for improved security measures in the IoT. Chaotic systems like Cat and logistic maps are used to improve multimedia data encryption [53, 54]. Jaishree and Arpit emphasize the importance of 6G technological advances in securing multimedia data transfer across 6G networks in the IoT. They introduce a hybrid image encryption method.

In [55], a safe technique was presented to improve the dynamics of chaotic maps generated on microcontrollers, enabling secure wireless transmission on M2M systems and demonstrating that chaotic maps offer adequate security performance.

1.7.3 Satellite Image Encryption Using Chaos

M. Usama [56] presented chaotic images from a satellite cryptosystem in that combines several chaotic systems to enhance key space and security. Bentoutou and Bensikaddour [57] presented a method for encrypting satellite images resistant to transmission errors and SEU. Behrouz and Seyedeh [58] presented a finite-time synchronizing of chaos satellite image encryption technique that employs chaotic oscillators at the transmitter and receiving ends by fusing the idea of finite-time synchronizing with Lyapunov stability theory.

1.8 Defence Against Cryptanalysis and Attacks

Chaos-based image encryption technology rapidly evolves, with various schemes enhancing security, resilience, efficiency, and key space [59]. Researchers are exploring ways to undermine and enhance these methods. Safeguarding image-encryption algorithms from attacks is a significant challenge in image encryption. There is no completely safe encryption method [60].

Nonlinear functions for system parameters, along with time and state variables, can safeguard chaos-based image encryption systems from attacks that utilize constant keys [61]. The authors in [62, 63] provide guidelines for the security evaluation of chaotic encryption.

Rhouma and Safya's [64] study on image-encryption techniques in hyperchaos revealed that

encryption in CPA and CCA can be broken with just three plaintext/ciphertext pairs. By disclosing the secret permutation mechanism, the algorithm in [65], among the earliest chaos-based image-encryption methods, also demonstrated its insecurity against CCA in [66]. Later on, the plan was refined in [67].

Yushu Zhang and Di Xiao [68] proposed the CPA method for chaotic image encryption that focuses on S-Boxes, noting that the computational complexity is only O(128L), where L represents the total number of pixels in the image. A chaotic image-encryption technique based on information entropy was also analyzed in [69], revealing its vulnerability to differential attacks [70]. Zhen Li's plaintext-related hyperchaotic encryption technique [71] has two significant shortcomings. Lidong Liu and Zhaolun Zhang [72] pointed out that this method is reversible in its structure and fails to change the grey value of a specific pixel during the diffusion process.

1.9 Literature Review

This section reviews several works that addressed the creation of random cryptographic keys using chaotic maps. The study will comprehensively understand the applicability and effectiveness of chaotic maps as a significant generating technique.

Researchers have been increasingly interested in dynamical systems in recent decades, especially in chaotic maps, a kind of classical dynamical system [73]. We can generate new chaos sequences by changing the parameters or initial values. These distinguishing features make chaotic maps excellent tools in computer science and engineering. The high performance of chaotic maps is particularly beneficial for pseudo-random number generators (PRNGs), image encryption, and security applications. In [73], the authors use chaotic systems in cryptography, being the first to encrypt digital information using chaotic maps. This work brought the use of central properties of chaotic systems to the forefront as essential factors in securing an encryption system. Encryption algorithms utilize one-dimensional and multidimensional chaotic systems [74]. Due to their complex structure and various features, MD chaotic maps are increasingly used in image security. However, the computational complexity and difficulty of their software/hardware implementations increase with the number of parameters. In contrast, one-dimensional chaotic systems are simple to design and have a clear structure. However, they face three issues: (1) The limited or discontinuous variation in chaotic behaviours; (2) The sensitivity to low-priced evaluation using correlation and iteration functions; (3) The non-uniform distribution of data about the chaotic sequences that are produced. Therefore, it is necessary to build new chaotic systems with improved chaotic performance.

As shown in Table 1.1, recent research shows that different chaotic encryption algorithms have different key strengths. A novel chaotic map cryptography technique is presented in [75]. This method focuses on the discrete cosine transform coefficients to achieve rapid encryption through confusion and diffusion processes in the spectral domain. It utilises a random number generator and Baker's map to generate a Gaussian distribution diffusion pattern, allowing for key encryption up to 128 bits.

The authors of [76] present a novel approach to image encryption that utilizes affine transformations and chaotic maps. This method eliminates pixel correlations, producing the final encoded image through an affine transformation. The security of this approach is validated by various factors, including histogram analysis, contrast, PSNR (Peak Signal-to-Noise Ratio), entropy, correlations, key space, key sensitivity, and resistance to differential attacks. It offers a robust, practical, and reliable solution for secure communication applications.

The study in [77] uses a chaotic map to implement a system based on a digital speech signal. The map's discrete-time parameterization allows for adaptability and multiple dimensions, providing powerful encryption capabilities.

A new technique for creating keystreams by combining the 3D Hénon and Cat maps is given in [78]. The fundamental idea behind this approach is to generate random numbers using the 3D Hénon map, which is subsequently converted into a binary sequence. Security analysis also highlights its high initial condition sensitivity and vast key space.

This study [79] proposes a chaotic framework that is extremely sensitive to initial values and system variables by combining the image encryption method with a secret key. Chaos adds to the durability of this system due to its intrinsic unpredictability. They used the inherent unpredictability of chaotic approaches, particularly the Hénon and Arnold cat maps. The Hénon map generates the encryption key, while the Arnold cat map shuffles pixels, ensuring data protection by limiting unauthorized access.

This work uses initial key and chaos theory to create a secure key generation mechanism [80]. The first stage involves a 2048-bit sequence using chaotic equations. The second stage involves a multi-phase procedure, creating 64 symbols or 512 bits for the key. The output is then passed through a crude table and an XOR operation, resulting in a 3584-bit key. The chaotic key number generator (CKNG), a pseudorandom number generator [81], is created using a two-dimensional rational map and a two-dimensional Hénon map. CKNG has a long key length, sensitivity to input values, and robust resistance against brute-force and differential attacks. It has passed strin-

gent NIST testing and is suitable for various encryption applications due to its unpredictability. The paper cited in [82] introduces a chaotic key generation technique that uses the 2D Hénon map and the 3D Lorenz system. This method might generate numerous key sequences appropriate for cryptographic applications by using floating-point integers and emphasizing the first two digits to increase unpredictability. A two-dimensional improved hyperchaotic Hénon sine map (2D-EHSHM) was developed using the remainder-after-division function to improve uniformity and unpredictability in a two-dimensional hyperchaotic map [83]. The enhanced map has better pseudorandom properties than the original version. The study also introduced a unique pseudo-random number generator (PRNG) technique for generating highly random 8-bit pseudorandom numbers. Positive results suggest PRNG may be helpful in cryptography, especially in low-cost processor-based embedded security systems.

The study [84] presents an optical cryptosystem that enhances the Hénon chaotic map and the gyrator transformation for color images. It offers three layers of protection: content, analysis, and appearance security. The cryptosystem uses electro-optical techniques that help with polarisation to work well. It is resistant to statistical and traditional attacks and is sensitive to minor modifications in the secret key. The cryptosystem outperforms other recently created cryptosystems in durability and visual security [85].

Table 1.1: A Comparative Analysis of Recent Studies.

Reference No.	**Technique**	**Number of key in bits**	**Performance**
[75]	Affine transformation and Chaotic maps	128 bits	The secret key provides a robust level of security, further bolstered by its powerful security mechanisms.
[76]	Affine transformation and Chaotic maps	128 bits	The findings indicate a consistent level of security, supported by the strong attributes of the secret key.
[77]	Hénon map	256 bits	The system guarantees security integrity by protecting against various attacks.
[78]	3D Hénon map and Cat map	128 bits	The system maintains its security integrity despite various attacks.
[79]	The Arnold Cat map and Hénon map	2320 bits	The positive evaluations suggest that this PRNG could benefit cryptography.
[80]	Initial key and Chaos theory	3584 bits	The study demonstrates a high level of security, which is further strengthened by the secret key's dependable security characteristics.
[81]	Two-dimensional rational map and Hénon map	2213 bits	The tool is helpful for various encryption applications since it generates an infinite number of pseudo-random sequences.

CHAPTER 2

PERLIMINARIES

A thorough overview of the main concepts behind this study is given in this chapter. It starts with cryptography before moving on to crucial processing techniques like representation and improvement. With a focus on cryptographic keys, the chapter looks at cryptanalysis and attacks. Furthermore, chaotic systems are used in multimedia encryption and pseudo-random number generation, discussing their basic characteristics and behavior tests, emphasizing the need for a comprehensive review of image encryption techniques based on chaos theory.

2.1 Cryptology

Cryptology is a concept that encompasses both cryptography and cryptanalysis [86]. The classification of cryptology is summarized in Figure 2.1.

2.2 Cryptography

The study of secure communication between two parties via a public channel that keeps private messages safe from hackers is known as cryptography. The five components of a

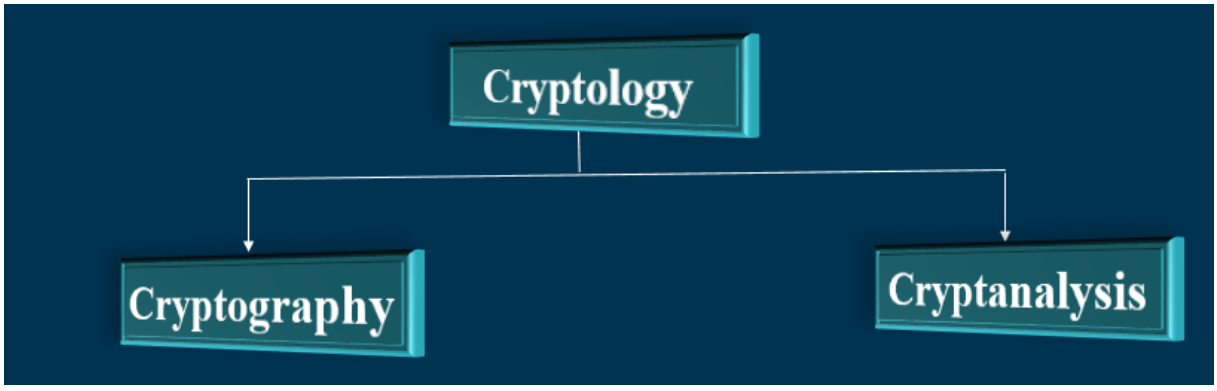


Figure 2.1: Classificaion of Cryptology

cryptosystem—plaintext, encryption, ciphertext, decryption, and key, are used to create and analyze techniques [87] shown in Figure 2.2.

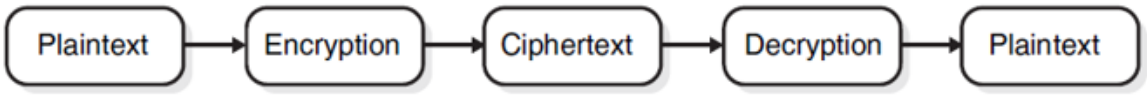


Figure 2.2: Component of Cryptography

1. **Plaintext:** Plaintext refers to the original message.
2. **Encryption:** Encryption converts a readable message into an unreadable form, preventing unauthorized parties from accessing it.
3. **Ciphertext:** Ciphertext is the term used to describe encrypted communication.
4. **Decryption:** Decryption is converting an encrypted message back to its plaintext format, which is the original message.
5. **Key:** The private key is used secretly by authorized users, and the public key is disclosed to everyone. Both keys are used for encryption and decryption.

2.2.1 Types of Cryptography

The flow diagram in Figure 2.3 demonstrates that cryptography can be categorized into three categories based on key distribution.

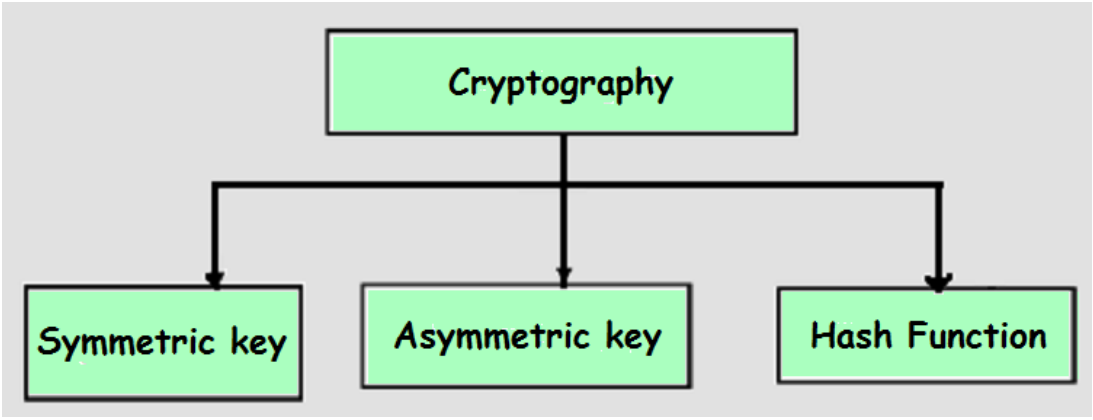


Figure 2.3: Types of Crpytography

1. Symmetric Key Cryptography

2. Asymmetric Key Cryptography

3. Hash Function

1. Symmetric Key Cryptography

Symmetric key cryptography [88], also known as secret key cryptography, has been used in public networks since 1976 for transmitting confidential messages. This method relies on a single key for encryption and decryption, as Figure 2.4 illustrates. Notable examples of symmetric key algorithms include the Advanced Encryption Standard (AES) [89], the Data Encryption Standard (DES) [90], and Blowfish [91]. Block and stream ciphers are the two main categories of symmetric encryption techniques. While stream ciphers handle encryption and decryption, one byte of plaintext is decrypted at a time, and block ciphers encode and decode fixed-length blocks of data.

Depending on the transform domain used during the encryption process, symmetric encryption

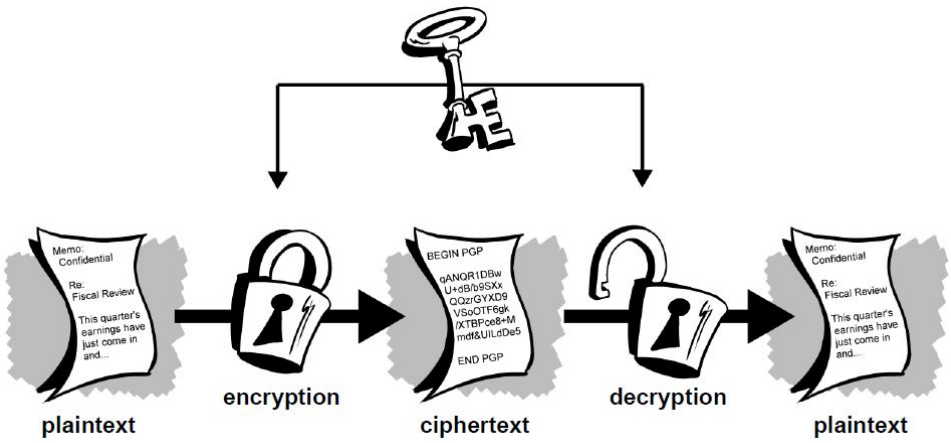


Figure 2.4: Symmetric Key Cryptography

methods can be categorized into spatial-domain chaotic image encryption and frequency-domain chaotic image encryption. Image encryption involves altering the position, value, or location of pixels in digital images. The permutation-diffusion architecture uses two iterative stages: permutation and diffusion. During permutation, pixels are rearranged, while diffusion gradually changes pixels, as shown in Figure 2.5.

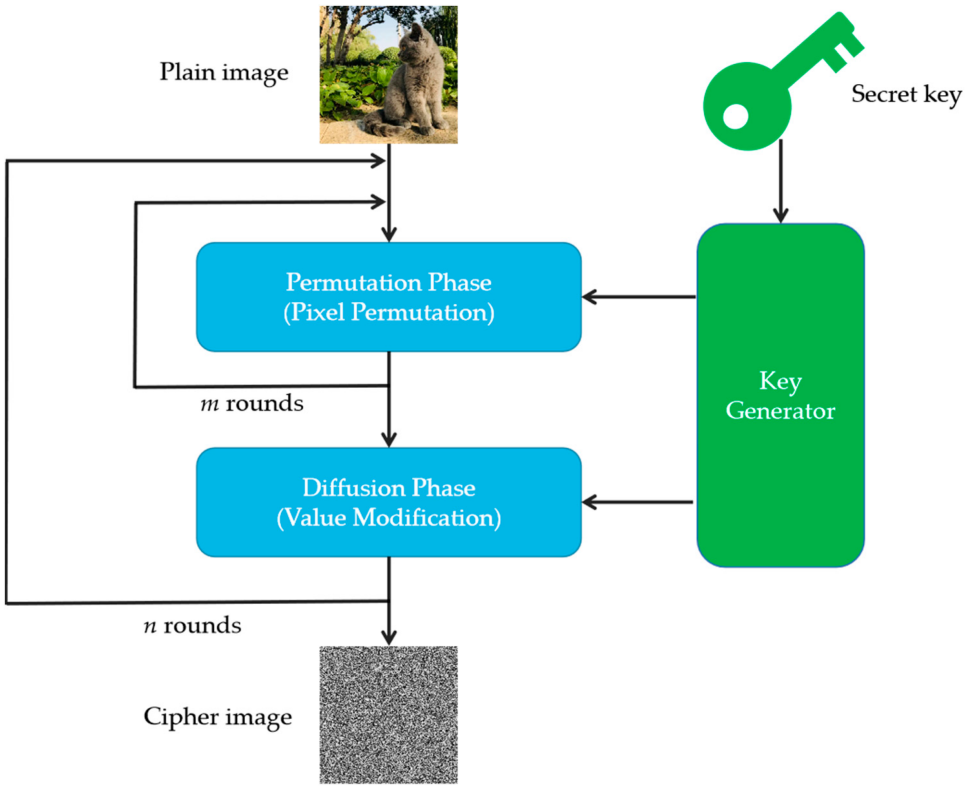


Figure 2.5: The Design of Permutation-Diffusion Chaotic Image Encryption

2. Asymmetric Key Cryptography

Whitfield Diffie and Martin Hellman [92] proposed asymmetric key cryptography in 1976 to solve crucial security issues. Two keys are used in asymmetric cryptosystems, commonly called public key algorithms: a private key for decryption and a public key for encryption. While the private key is used to transmit sensitive data, the public key is used for sender authentication. This technique, which is based on a mathematical function similar to substitution and permutation, employs a one-way trapdoor function for key transmission between parties. Figure 2.6 demonstrates using private and public keys for data encryption and decryption. The primary elements of public key encryption are ciphertext (C), decryption using the recipient's private key and plaintext (M), encryption using an encryption algorithm $(\mathscr{E})$, and the public key of the beneficiary (PU) [93]. The structure provided is as follows:

$$C = \mathscr{E}(PU, M), \tag{2.1}$$

$$M = \mathscr{D}(PR, C) \tag{2.2}$$

The RSA cryptosystem [94], the ElGamal cryptosystem [95], and the elliptic curve cryptosystem [96] are examples of asymmetric key cryptography [97].

By combining the unpredictability of chaotic systems with the security of public-key cryp-

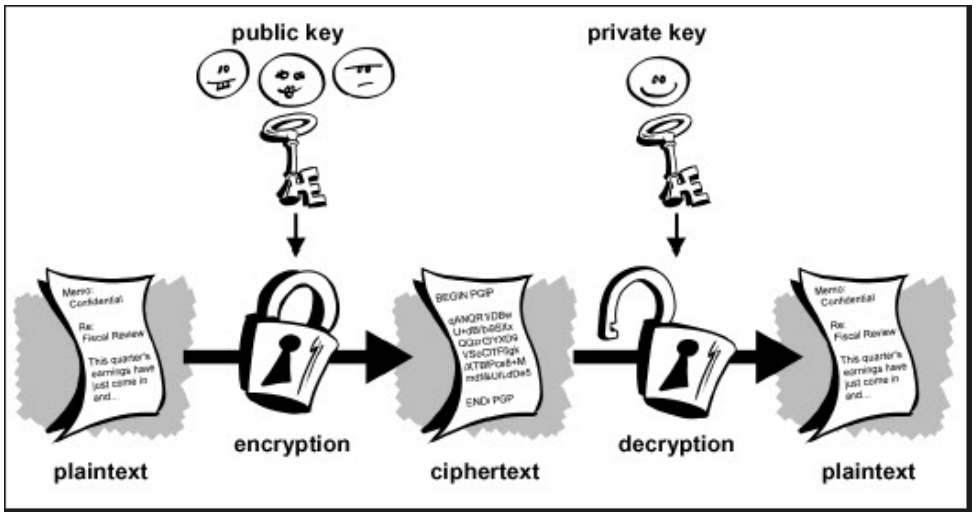


Figure 2.6: Asymmetric Key Cryptography

tography, asymmetric chaos-based encryption improves attack resistance and eliminates key distribution problems. Future research should concentrate on speed optimization and protocol standardization for practical implementation. Figure 2.7 depicts the typical flow of image encryption based on a public key.

In 2013, Cheng and Cheng [98] introduced an asymmetric cryptosystem for chaos-based image

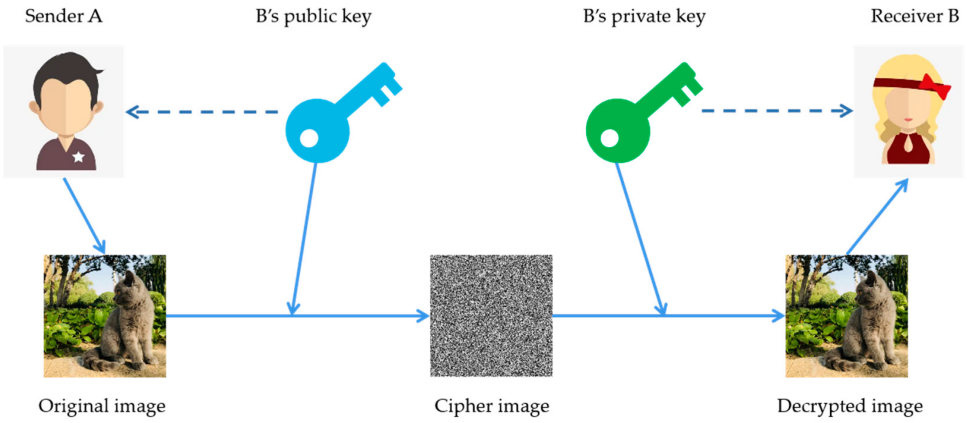


Figure 2.7: Public-Key Transfer of Image Encryption

encryption using a cellular neural network and adaptive synchronization of two chaotic systems. During the process, they generated a pair of asymmetric keys for encryption and decryption.

3. Hash Function

A hash function, as illustrated in Figure 2.8, is a cryptographic method that generates a fixed-length output from an input of any length. It is a one-way device that produces a hash code with two binary data streams of fixed-length blocks [99]. Common hash functions include MD5, SHA, RIPEMD, and Whirlpool. MD5 is the most widely used hashing algorithm for encrypting passwords and other sensitive information, making it a crucial tool in cryptographic systems.

Figure 2.8: Hash Function

2.3 Cryptanalysis

Cryptanalysis studies ciphertext, ciphers, and cryptosystems to understand their workings and develop strategies to tackle them. Cryptanalysts decode ciphertexts without knowing the source, encryption key, or algorithm [100]. They also target secure hashing and digital signatures. Cryptographers use the results of the cryptanalysis to improve, reinforce, or replace flawed algorithms [101].

There are a variety of cryptanalysis attacks, which differ depending on how much knowledge the researcher has about the ciphertext being analyzed.

2.3.1 Ciphertext Only Attacks

Ciphertext-only attacks (COA) involve attackers accessing encrypted messages without knowledge of plaintext data, encryption algorithms, or cryptographic keys, which poses a challenge for intelligence agencies intercepting encrypted messages [102].

2.3.2 Known Plaintext Attack

A known plaintext attack (KPA) involves obtaining access to the ciphertext of a plaintext to discover a key to encrypt a file [103]. If found, an intruder can decrypt all encrypted messages,

such as a message addressed to a specific person [104].

2.3.3 Chosen Plaintext Attack

In a chosen plaintext attack (CPA), the analyst knows how the data were encrypted or has access to the computer that did it [105]. The analyst will encrypt the CPA with the attacked algorithm to learn more about the key.

2.4 Chaotic Map

A secret key cryptosystem uses a one-dimensional chaotic map, demonstrating how chaos affects cryptography. The sensitivity of the system to parameters and the unpredictability of the sequence form its basis [106]. Chaos-generating mechanisms, such as one-dimensional difference equations, have been studied in various disciplines [107].

Definition: Dynamic systems generate a state of randomness that is entirely disorganized and seems irregular. In the mathematical study of chaotic maps, the initial seed conditions govern this state. Chaos theory explains the connection between entirely random chaotic outcomes and the basic patterns that generate them [108]. Understanding how a generator is linked makes a detailed examination of these patterns possible. These generators often rely on feedback loops, self-similarity, repeatability, and the chaotic nature of the system [109].

The features of chaotic solutions consist of the following:

1. Sensitivity of parameters: Due to parameter sensitivity, a slight change in one parameter, like the shape of F, might result in a considerable difference between two sequences from multiple computations on a chaotic map.

2. Sensitivity of initial points: The sensitivity of initial points in a chaotic map can cause two sequences to differ significantly if the initial point X slightly changes.

2.4.1 Types of Chaotic Map

There are two types of chaotic map, i.e. continuous and discrete, can use actual values or be complex, with some having up to four dimensions. Most are three measurements with seed points ranging from 0 to 18 parameters, with the type C polynomial fractal map being the most complex [110].

1. **Continuous Chaotic Map:**

   Continuous chaotic systems exhibit intricate, erratic behavior over time, characterized by differential equations controlling state variables [111]. These systems represent specific

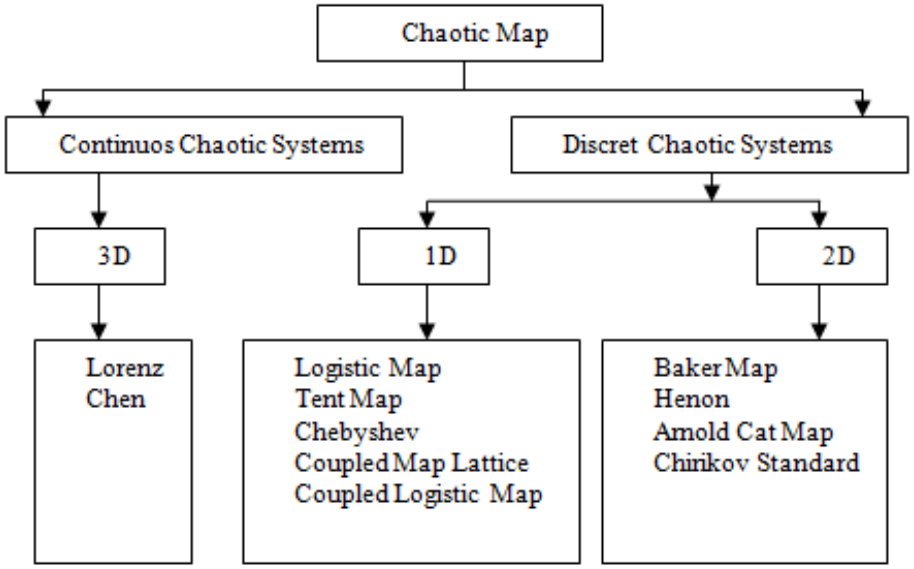


Figure 2.9: Types of Chaotic Map

physical parameters like pressure, temperature, location, or velocity, and they are often studied using three-dimensional chaotic systems like Lorenz and Chen systems.

2. **Discrete Chaotic Map:**

   Due to its sensitivity to initial conditions and changes in system state parameters over time, a discrete chaotic map is a nonlinear equation that exhibits period multiplication and nonlinearity, generating random patterns [112]. Based on their applications, structure, and dimensionality, discrete maps may be broadly classified into one-dimensional (1D) and two-dimensional (2D) categories.

   One-dimensional (1D) maps, such as the logistic and tent maps, are defined by a single variable and exhibit fundamental chaotic properties, including sensitivity to initial conditions and period-doubling bifurcations. Due to their simplicity and well-studied behavior, they are widely used in population dynamics and cryptography.

   Logistic map: A chaotic function that produces pseudo-random sequences is called a logistic map [113].

$$x_{n+1} = r x_n (1 - x_n) \tag{2.3}$$

   The control parameter, denoted by r, is usually in the range $3.57 < r \leq 4$ for chaotic behavior. At iteration n, the sequence value is indicated by x_n. The logistic map is particularly well-suited for use in cryptography due to its extreme sensitivity to initial conditions.

Coupled Logistic Map

It connects many logistics systems to extend the logistics map and increases complexity, strengthening its resistance against cryptographic attacks [114].

Sine Map

A sine map is a deformation of the sine function, which transforms its inputs from $[0, \pi]$ into $[0, 1]$ and retains the range of the original outputs is $[0, 1]$ [115].

$$x_{n+1} = S(x_n) = \mu \sin(\pi x_n) \tag{2.4}$$

where, μ is the control parameter. The bifurcation and Lyapunov exponent diagram of sine map are shown in Figure 2.10.

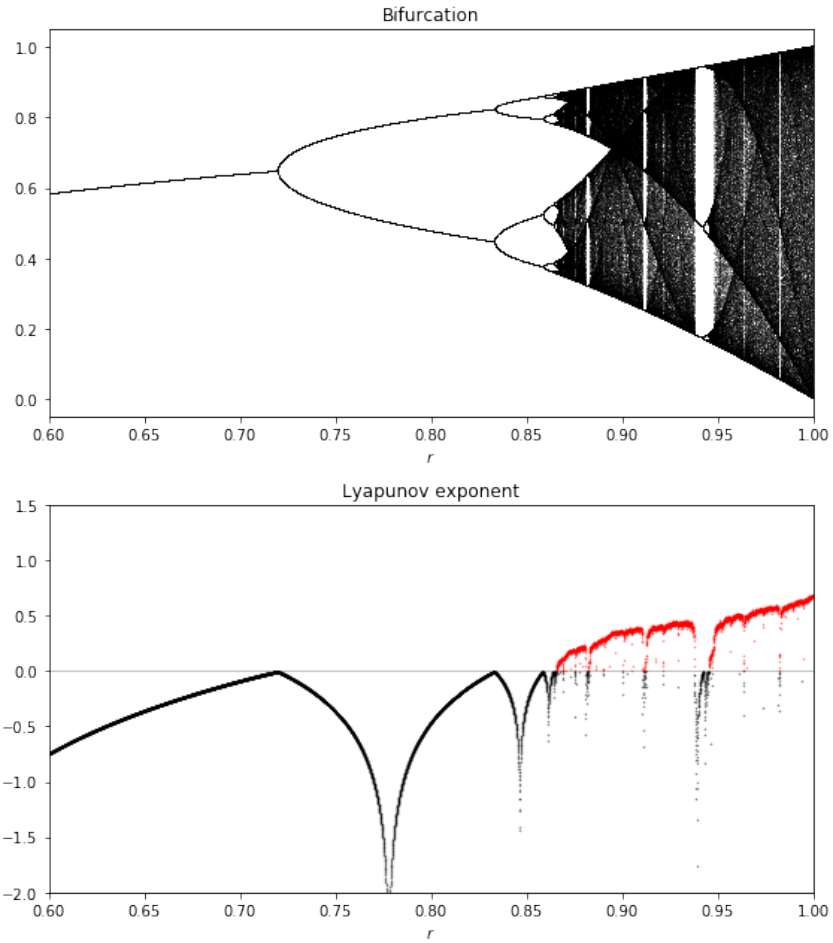


Figure 2.10: Sine Map

Logistic Sine Map (2D-LSCM)

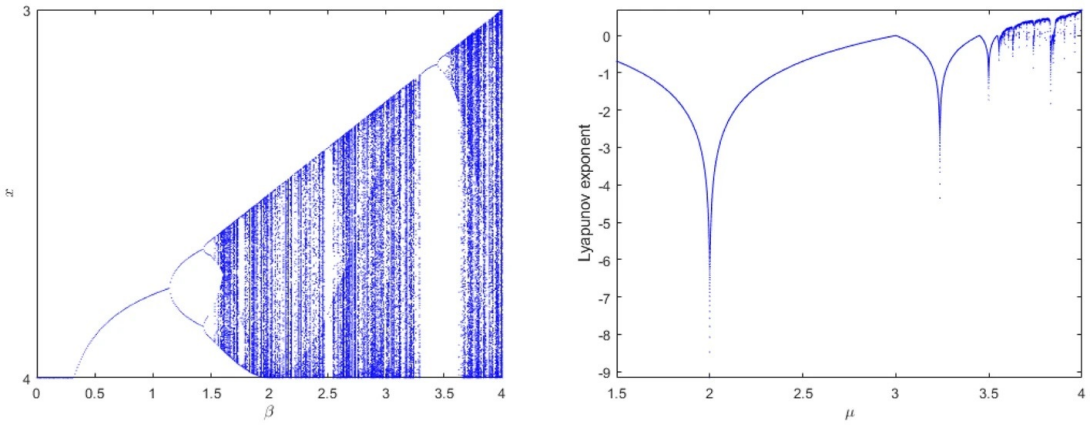
The 2D-LSCM combines the logistic and sine map in a coupled manner [116]. We employ modulation and coupling approaches to construct a new chaotic system using the logistic

map and a sine map, as shown in Eq. (2.4).

$$\begin{cases} x_{n+1} = sin(\pi(4\mu x(n)(1-x(n)) + (1-\mu)sin(\pi y(n)))) \\ y_{n+1} = sin(\pi(4\mu y(n)(1-y(n)) + (1-\mu)sin(\pi x(n+1)))) \end{cases} \tag{2.5}$$

μ is the control parameter, and $x(n)$ and $y(n)$ are the state variables.This coupling creates a more complex and robust chaotic system.

As can be observed from Eq . (2.4), we first use the Logistic map to modulate the Sine map. Then, we couple the Logistic map and the Sine map together and use control parameters to restrict the outputs of LSMCL. Finally, we extend the dimension from 1D to 2D to improve the chaotic behaviors. The bifurcation and Lyapunov exponent diagram of sine map are shown in Figure 2.11.



(a) Bifurcation Diagram **(b)** Lyapunov exponent

Figure 2.11: Logistic Sine Map

A two-dimensional $(2D)$ discrete map, such as the Baker, Henon, and Arnold Cat Map, is a dynamic system defined by a pair of recurrence relations describing the evolution of two variables, x_n and y_n, over discrete time steps. These maps exhibit rich nonlinear behavior, including chaos, bifurcations, and the emergence of fractal attractors.

2.5 Coupled Map Lattices: Theory and Applications

2.5.1 Mathematical Representation

A discrete-time dynamical system described on a spatial lattices is called a coupled map lattices (CMLs) [117]. The state of a 1D lattice of size L fluctuates as follows:

$$x_{n+1}(i) = (1-\varepsilon)f(x_n(i)) + \frac{\varepsilon}{2}[f(x_n(i-1)) + f(x_n(i+1))] \tag{2.6}$$

Components:

1. **Lattices Site** $(i = 1, 2, \ldots, L)$

   A one-dimensional lattices of L identical spots represents the discretization of the system. A state variable $x(i) \in R$, representing local dynamics (such as temperature in a thermal rod or neuron activity in neural tissue), is present at each site i [118]. The spatial backbone of interactions is the lattices.

2. **Local Map** $(f : \mathbb{R} \to \mathbb{R})$

   The logistic map $f(x) = rx(1-x)$ is a nonlinear chaotic map that controls the uncoupled dynamics at each site. By applying this Map at each time step, the state space becomes enlarged and folded to produce complicated behaviour [119]. Initial conditions impact chaotic maps (Lyapunov exponent $lambda > 0$).

3. **Coupling Strength** $(\varepsilon \in [0, 1])$

   Determines the influence of neighbouring sites. The evolution combines local dynamics and neighbour contributions:

   $$x_{n+1}(i) = (1-\varepsilon) f(x_n(i)) + \frac{\varepsilon}{2} \left[f(x_n(i-1)) + f(x_n(i+1)) \right]$$

   $\varepsilon = 0$: Sites evolve independently (decoupled)

   $\varepsilon = 1$: Dominant neighbour influence (maximal coupling)

4. **Boundary Conditions (Periodic)**

   The spatial closure is enforced via:

   $$x^{(0)} \equiv x^{(L)}, \quad x^{(L+1)} \equiv x^{(1)}$$

   This framework has infinite/extended systems and eliminates edge effects, preserving translational symmetry.

Important Features

1. **Phase Space** $([0, 1]^L)$

   The collective state can be found in a hypercube of L dimensions. According to standard chaotic maps (such as logistic map outputs $\subset [0, 1]$), each dimension corresponds to a site's state $x(i) \in [0, 1]$. Under the coupled equations, trajectories change, creating complex manifolds controlled by the bifurcation parameters (r, ε).

2. **Lyapunov Spectrum**

   The stability is described by the L exponents $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_L$:

   $\lambda_1 > 0$: Chaos in space and time

   $\lambda_k = 0$: Neutral modes (such as pattern drift)

   $\lambda_k < 0$: Stable Directions

   The greatest exponent for diffusive coupling is as follows:

$$\lambda_{\max} \approx \lambda_f + \ln|1-\varepsilon|$$

   where λ_f is the Lyapunov exponent of the local map f.

3. **Measure Invariance**

   Examines the statistical distribution of states over a lengthy period [120]. For CMLs that are chaotic:

   Uncoupled scenario$(\varepsilon = 0)$**:** Measure of the product $\mu = \prod_{i=1}^{L} \mu_f$ (independent sites)

   Coupled scenario$(\varepsilon > 0)$**:** Factorizability is broken by emergent spatial correlations. The measurement μ_ε satisfies

$$\mu_\varepsilon \circ \Phi = \mu_\varepsilon$$

   where Φ is the CMLs evolution operator [121]. For weak coupling, μ_ε is singular with fractal support.

2.6 Chaotic Behaviour Tests

- **Definition 1 (Bifurcation Diagram):** A bifurcation diagram graphically represents the chaotic behaviour of a dynamical system, displaying values obtained or entered in terms of its bifurcated parameters [122]. This diagram connects chaotic features to control settings, allowing for analysis of how system performance varies with specific factors, especially when values suddenly change. The bifurcation map is seen in Figure 2.12.

- **Definition 2 (Lyapunov Exponent):** The Lyapunov exponent (LE) measures the divergence rate of infinitely proximal trajectories starting from close beginning states in a dynamical system. It measures the exponential divergence between orbits with near beginning states after a finite number of repetitions [123]. LE may be expressed as follows, considering that $X_{N+1} = G(X_N)$ is a one dimensional map:

$$LE = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} \ln\left|G'(X_i)\right| \tag{2.7}$$

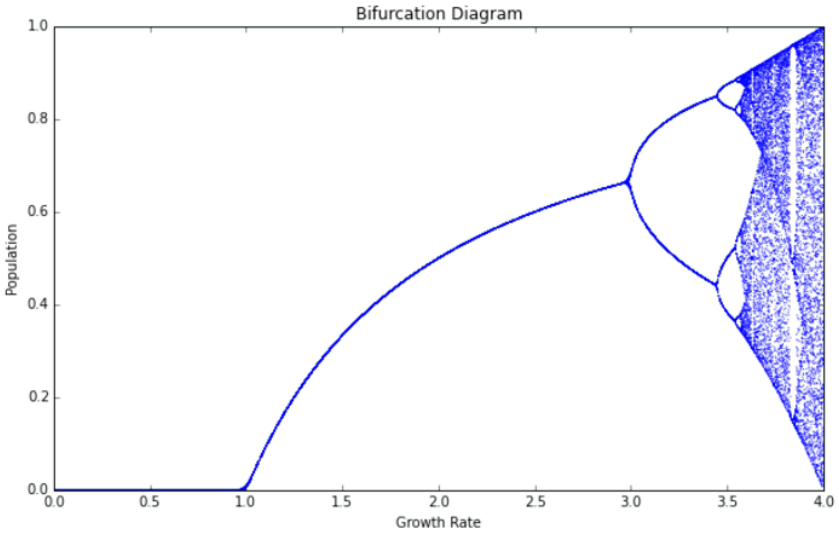


Figure 2.12: Bifurcation Diagram of logistic map

When LE < 0, neighbouring points are more stable, indicating periodic motion or stable fixed points. When LE > 0, an exponential divergence occurs. Chaotic systems have at least one positive LE, determining their chaotic nature. Chaotic features become more apparent as LE value increases. Hyperchaotic systems have two or more positive Lyapunov exponents. Figure 2.13 displays the Lyapunov exponent of a logistic map.

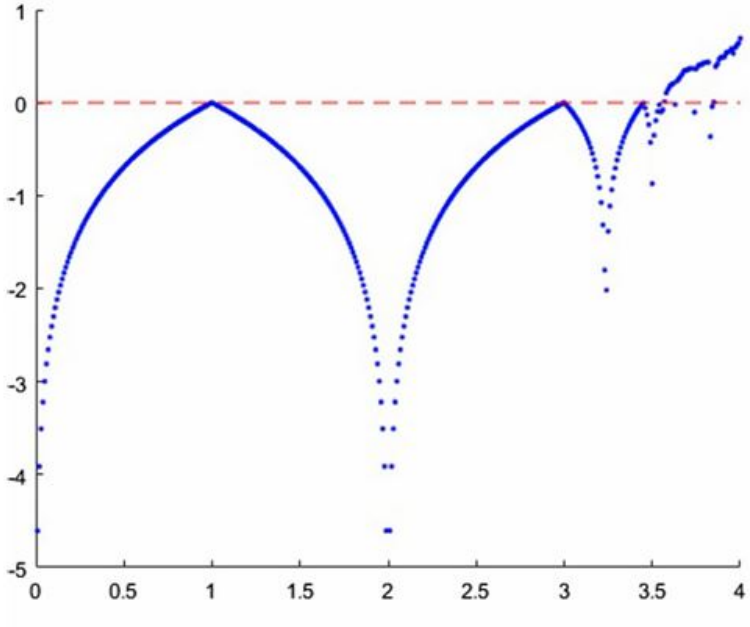


Figure 2.13: Lyapunov exponent of logistic map

- **Definition 3 (Correlation Dimension):**The correlation coefficients are computed and

quantified to show how the correlation of neighboring pixels changes after encryption [124]. As correlation increases, the coefficient approaches 1, while as correlation decreases, it approaches 0. One way to explain the calculation equation would be

$$\gamma = \frac{\sum_{i=1}^{M_0} (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{M_0} (x_i - \bar{x})^2 \sum_{i=1}^{M_0} (y_i - \bar{y})^2}} \tag{2.8}$$

- **Definition 4 (Information Entropy):** Information entropy is a key performance indicator in sequence randomization, determining each grey-level pixel's diffusion level and quantifying the image's unpredictability [125]. The optimal entropy value for encrypted messages is 8, and better encryption algorithm security performance is linked to greater resilience to statistical attacks [126]. The following is the calculating formula:

$$H(x) = -\sum_{i=1}^{M} P(x_i) \log_2 P(x_i) \tag{2.9}$$

in which $P(x_i)$ is the likelihood that a point in the sequence with the value of pixels of x_i will occur.

- **Definition 5 (Approximate Entropy):** Approximate Entropy (ApEn) is a metric for measuring the complexity of time series [127]. It indicates the series's irregularity and intricacy. The likelihood of a variation pattern being preceded by comparable ones is inversely linked to ApEn. Positive ApEn levels suggest a lack of redundancy patterns, but higher ApEn values indicate more complex and surprising systems.

- **Definition 6 (The Trajectory):** The trajectory diagram shows the existence of cycles and the ergodic characteristics of a chaotic system. The trajectory of a perfect one-dimensional discontinuous chaotic map system should be free of periodic cycles and structure.

2.6.1 Occulusion Attack

The mean squared error (MSE) is used to determine the PSNR for grayscale images in the following way:

- The average squared difference between matching pixels in the original and decrypted images is measured by MSE, which is determined by:

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(I_1(i,j) - I_2(i,j)\right)^2 \tag{2.10}$$

The numbers M and N in the images represent the number of rows and columns. The pixel value at a particular point in the original image is represented by $I_1(i,j)$. The pixel value in the encoded or encrypted image is denoted by $I_2(i,j)$.

- The PSNR is computed as follows:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{\text{MSE}}\right) \tag{2.11}$$

Higher PSNR values suggest greater resemblance between the original and decrypted images, even after occlusion.

2.6.2 Histogram Analysis

The variability of the tonal value of the encrypted image histogram is quantitatively assessed using variance and chi-square tests χ^2 [128]. The definition of a grey-level image is as follows:

$$\chi^2 = \sum_{i=0}^{255} \frac{(n_i - n/256)^2}{n/256} \tag{2.12}$$

$$\text{var}(Y) = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n}\frac{1}{2}(y_i - y_j)^2 \tag{2.13}$$

Where n is the total number of pixels, n_i is the recurrence density of pixel value i, and $n/256$ is the projected recurrence density of each pixel value. Its vector is $Y = \{y_1, y_2, \cdots, y_{256}\}$. The corresponding pixel values for i and j are denoted by Y_i and Y_J, respectively [129].

2.6.3 Robustness Analysis

During image transmission, digital images are frequently impacted by noise or partial data loss. A robust encryption method should retain its decoding capabilities even in such unfavorable circumstances. The suggested approach was examined in terms of data loss and noise interference attacks to assess its effectiveness. Image encryption techniques undergo robustness tests to evaluate their resilience against various attacks. Table 2.1 illustrates the robustness behavior under attack scenarios.

2.6.4 Statistical Tests by NIST

An encrypted image's pixels should be evenly distributed to withstand statistical attacks. Applying the statistical test suite created by NIST, the suggested encryption scheme's resilience to such attacks is further examined. It consists of 15 tests that discuss various aspects of randomness in large binary sequences. The purpose of this test set is to find any patterns of non-randomness in these sequences.

Table 2.1: Robustness Metrics and Their Desired Behaviour Under Attack Scenarios

Metric	**Robustness Role**	**Desired Behavior Under Attack**
Correlation	Shows encryption effectiveness in randomizing spatial data	Should remain close to 0
Entropy	Indicates resistance to statistical/predictive attacks	Should stay close to 8
MSE	Measures decryption accuracy under noisy/partial input	Should be low after decryption
PSNR	Reflects image recovery quality from attack/occlusion	Should be high (>30 dB if robust)

With a significance threshold of 0.01 and 16 statistical verification processes, the NIST Statistical Suite verifies the randomness of binary sequences. A sequence is considered valid when its p-value is ≥ 0.01, and current random testing standards are NIST statistical tests.

CHAPTER 3

A NOVEL IMAGE ENCRYPTION ALGORITHM BASED ON COMPOUND-COUPLED LOGISTIC CHAOTIC MAP

This chapter introduces a compounding coupling approach to enhance the complexity of chaotic systems, addressing the lack of safety and complexity in original chaotic systems. The approach is universal and demonstrated through numerical tests on the 1D logistic map. The enhanced map has more dynamic complexity than the original one. The enhanced chaotic map is used in an image encryption technique, outperforming current security, attack resistance, and computing efficiency techniques.

3.1 Formulation

For real-world cryptography applications, this research attempts to increase the complexity and security of low-dimensional chaotic systems, such as logistic maps. It aims to create a modified chaotic model that enhances their cryptographic performance, security, and unpredictability, making them suitable for image encryption while maintaining efficiency and universality.

3.2 Exploring the Dynamics and Characteristics of the Compound-Coupled Logistic Chaotic Map

3.2.1 The Compound-Coupled Logistic Chaotic Map

The paper suggests a universal N-dimensional compound-linked chaotic model, which is described mathematically, to increase the complexity of chaotic maps.

$$\begin{cases} x_1^{(i+1)} = f_2(f_1(x_1^{(i)}, p_1, p_2)) \\ x_2^{(i+1)} = f_3(f_2(x_2^{(i)}, p_2, p_3)) \\ \quad \vdots \\ x_j^{(i+1)} = f_{j+1}(f_j(x_j^{(i)}, p_j, p_{j+1})) \\ \quad \vdots \\ x_N^{(i+1)} = f_1(f_N(x_N^{(i)}, p_N, p_1)) \end{cases} \tag{3.1}$$

The CCCM is linked with state variables of each dimension being governed by the compounding of two chaotic maps, as shown in Eq. (3.1), where $x(N)$ represents the N-dimensional state variable.

The CCCM restricts $Eq.(3.1)$ to the chaos zone, requiring its magnitude to be in the chaotic region of f_{j+1}, which can be removed if the maps are equivalent.

The technique is further implemented using a two-dimensional CC logistic map, with its mathematical model expressed as follows.

$$\begin{cases} x_{i+1} = f(f(y_i, p_1), a) \\ y_{i+1} = f(f(x_i, p_2), b) \end{cases} \tag{3.2}$$

The logistic map, denoted by f, is defined as

$$f(x, p) = p(1 - x) \tag{3.3}$$

The control coefficient, denoted by p, causes the region map f to become chaotic. The parameters p_1 and p_2, associated with variables x_i and y_i, increase the complexity of the CC logistic map. In this study, simple linear functions are used.

$$p_1(x_i) = 3.6 + 0.4x_i \tag{3.4}$$

$$p_2(y_i) = 4 - 0.4y_i \tag{3.5}$$

It should be mentioned that in order to guarantee that the map is chaotic, the values of parametric functions p_1 p_2 must fall within [3.6, 4]. The compound-coupled logistic chaotic map can be expressed as follows:

$$\begin{cases} x_{i+1} = af(y_i, p_1)(1 - f(y_i, p_1)) = a(3.6 + 0.4x_i)y_i(1 - y_i)(1 - (3.6 + 0.4x_i)y_i(1 - y_i)) \\ y_{i+1} = bf(x_i, p_2)(1 - f(x_i, p_2)) = b(4 - 0.4y_i)x_i(1 - x_i)(1 - (4 - 0.4y_i))x_i(1 - x_i) \end{cases} \tag{3.6}$$

Flowchart of the model (6) can be described in Figure 3.1.

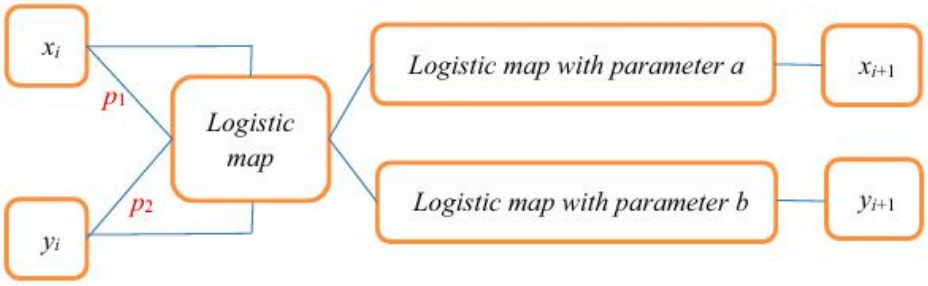


Figure 3.1: The Compound-Coupled Logistic Chaotic Model's Flowchart

3.2.2 Performance Dynamics of the CC Logistic Chaotic Model

This section presents a number of simulation tests that assess the dynamic performances of the CC Logistic map that CCCM enhanced. If no further instructions are provided, the parameters for these tests are chosen as follows: $x_0 = 0.25489, y_0 = 0.36987$ and a = b = 4.

The Trajectory

Chaotic maps produce value changes that are reflected in trajectory diagrams, indicating unpredictability, as shown in Figure 3.2. The 2D CC logistic map's orbits show good randomness and no discernible structure. The enhanced map has strong ergodicity, as its points are dispersed throughout the $[0,1] \times [0,1]$ area.

Bifurcation Diagram

Chaotic maps visit bifurcation diagrams, revealing the parameter ranges causing the map's chaotic behavior and the periodic window. When b = 4, the value of a shifts from 0 to 4. The bifurcation diagram in Figure 3.3 of the chaotic sequence produced by the dimension x of the 2D CC logistic map shows that the range of parameters causing chaos has been expanded after improvement.

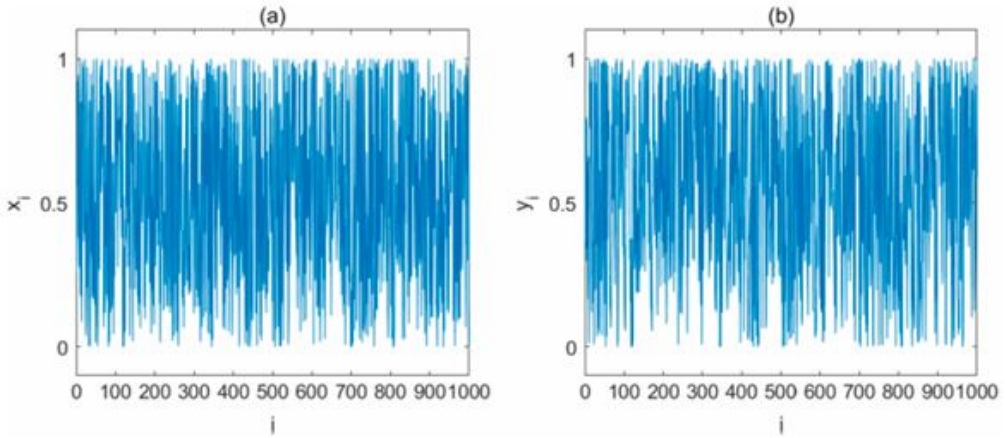


Figure 3.2: 2D CC Logistic Map's (a) x-dimensional and (b) y-dimensional Trajectory Diagrams

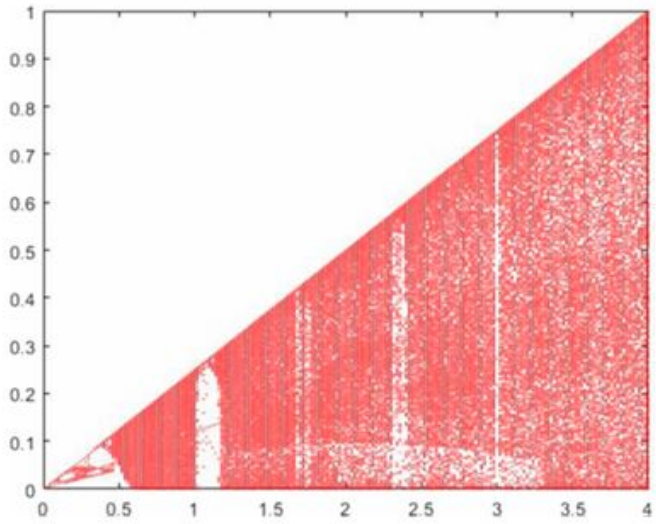


Figure 3.3: Bifurcation Diagram of x-dimensional of 2D CC Logistic Map

Lyapunov Exponent

The Lyapunov exponent is a measure for describing a system's dynamic properties, with a chaotic system requiring a positive one [130]. It can be determined if a system is chaotic by its maximum Lyapunov exponent values, which are higher than 0. The diagram of maximum Lyapunov exponent values shows that as variables improve, the range of variables allowing the map to display chaos increases, is shown in Figure 3.4.

Dimension of Correlation

Chaotic systems in integer dimensions are often described using the fractal and correlation dimensions [131]. This section calculates the correlation dimension to assess the performance of

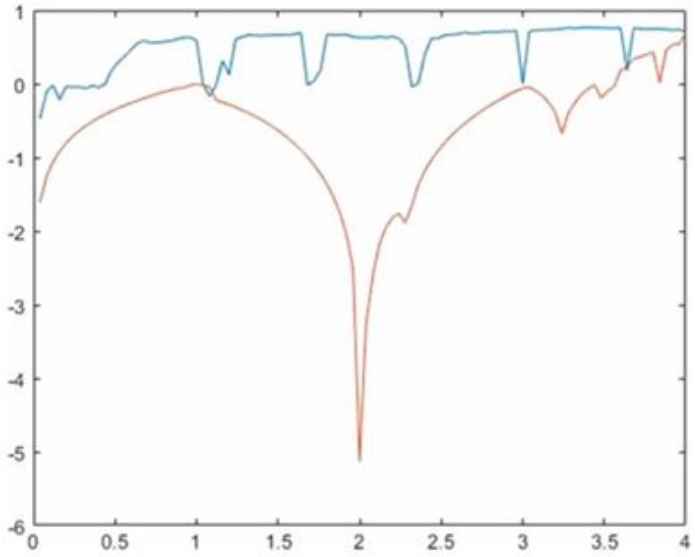


Figure 3.4: Lyapunov Exponent Diagram

the 2D CC Logistic map. The enhanced map's correlation dimensional value is primarily greater than the original map's, indicating improved performance following CCCM's enhancement; it is simple to see from Figure 3.5. The blue line shows the enhanced map's correlation dimensional value for all values, demonstrating the effectiveness of the CCCM.

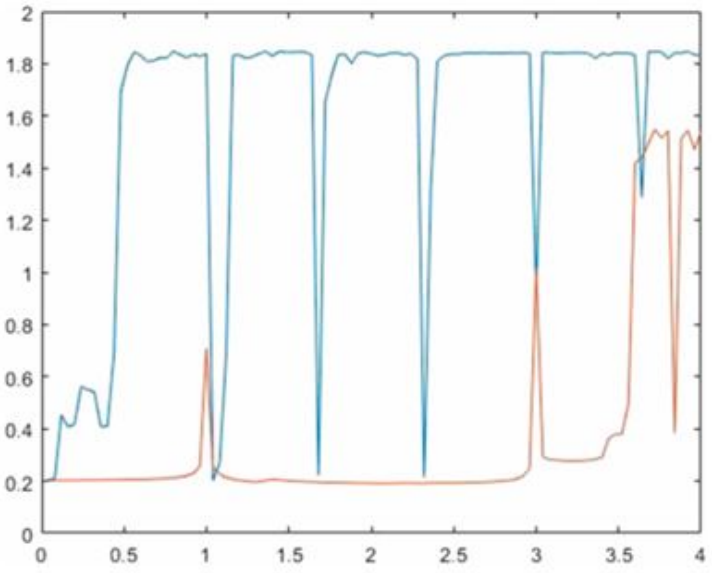


Figure 3.5: Correlation Dimension Analysis Diagram

3.3 A Complexity Image Encryption Technique Using the CC Logistic Chaotic Map

3.3.1 Algorithmic Framework for Encryption

The model's validity is demonstrated through numerical experiments and a simple image encryption technique using the chaotic logistic map of CC. The CCCM has enhanced the security of the algorithm by focusing on its simple map structure. The technique is highly secure and resistant to various attacks.

This study uses a disruption and diffusion approach for image encryption, employing three chaotic sequences from the logistic CC map. Two sequences are used in the disruption stage and one in the diffusion stage. The inverse process is used to decrypt a received cipher image. Figure 3.6 shows the flowchart of the encryption and decryption process.

3.4 Performance Evaluation of the Encryption-Decryption Process

In this part, we utilize grey 256×256 images as an example. While $x_{10} = 0.2148$, $y_{10} = 0.4789$, $x_{20} = 0.6574$, $y_{20} = 0.3657$,$x_{30} = 0.2048$, $y_{30} = 0.9843$ are the initial values in that order. Figure 3.7 show the outcomes of various chaotic encryption algorithms with the system parameters set to a = b = 4. The success of the encryption approach is demonstrated by the fact that the decrypted image is identical to the encrypted image, which lacks any important information.

3.5 Security Analysis and Experiment Testing

Simulation tests are conducted to validate and secure the encryption algorithm, focusing on ensuring accuracy of chaotic sequences using a generic algorithm performance of 105 and replicating every experiment using PyCharm 2021.1.

3.5.1 Analysis of Key Spaces

An encryption technique's key space should be sufficiently large to resist intensive attacks. This techniques uses six starting values and Table 3.1 to display key-space computation results for various encryption techniques. The key space is significantly greater than 2^{128} and wider than some other chaos-based encryption algorithms, indicating the algorithm's ability to withstand various brute-force attacks.

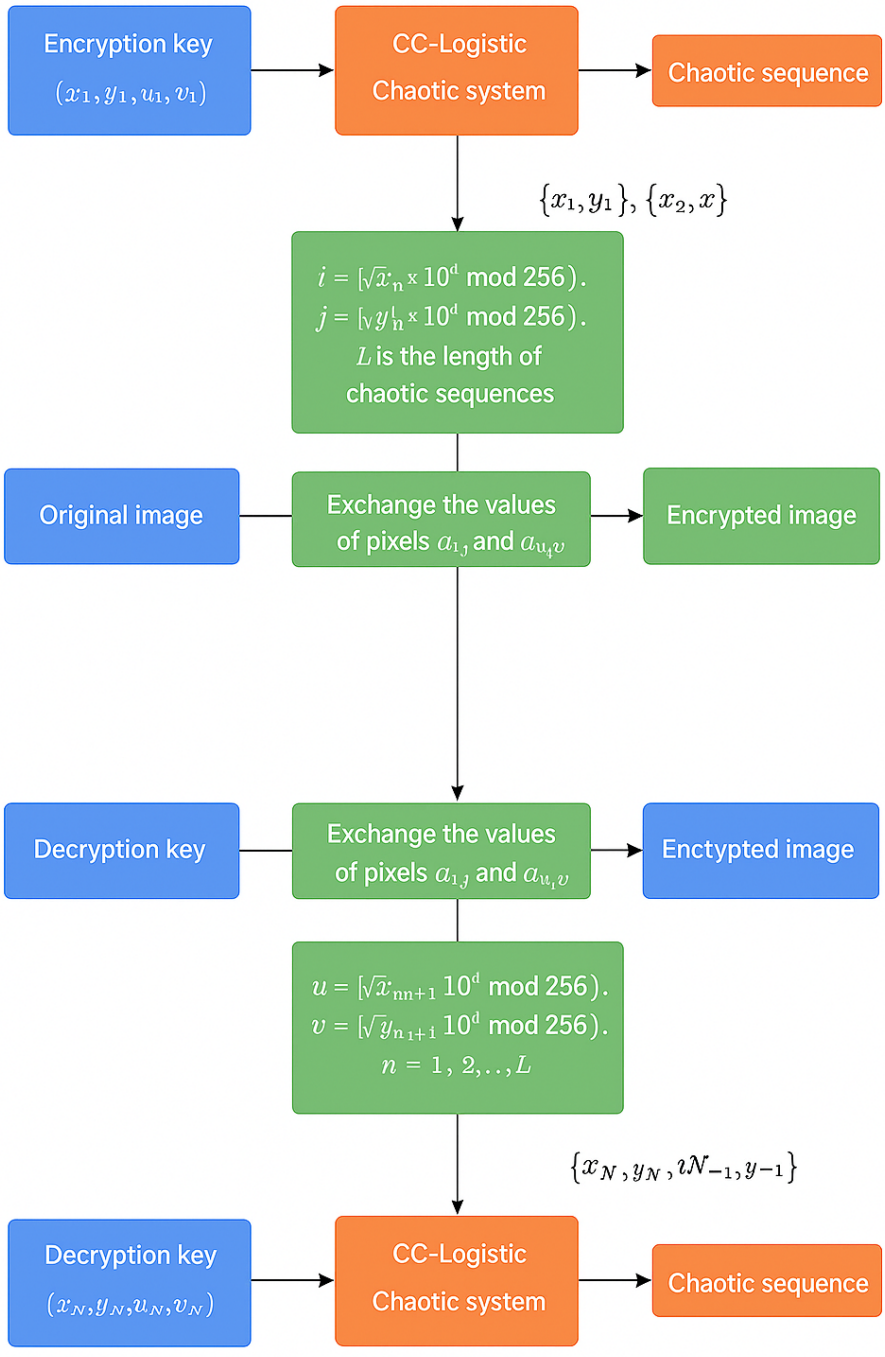


Figure 3.6: Encryption and Decryption Process

Figure 3.7: Visual Demonstration of Chaotic Encryption Process (a) Original Image (b) Encrypted Image (c) Decrypted Image

3.5.2 Analysis of Key Sensitivities

A good cypher algorithm should be susceptible to key changes to provide different representations of the ciphertext and decoding results for the same cypher image. Different decoding results should also be obtained with two slightly different encryption keys. Figure 3.8 indicates that, although there is a slight difference between the correct and decrypted keys, the decrypted image is entirely different from the original. The recommended method for image encryption is susceptible to changes in secret keys, since even a slight alteration can prevent decryption. Calculating the mean square error (MSE), or the difference between two encrypted images using various keys, may help one better understand the algorithm's primary sensitivity. The supplied

Table 3.1: Keyspace Evaluation in Testing Outcomes

Algorithms	**Keyspace**
Ref. [132]	10^{84}
Ref. [133]	10^{56}
Ref. [134]	10^{56}
Ref. [135]	10^{56}
Ref. [136]	10^{6}

Figure 3.8: Key Sensitivity Evaluation (a) Correct Decrypted Image. (b) Error-Decrypted Image

data may be used to calculate the pixel values at position (i, j), which are denoted as $P(i, j)$.

$$MSE = \frac{1}{MN} \sum_{i=1}^{M} \sum_{j=1}^{N} \left(P_{i,j} - P'_{i,j} \right)^2 \tag{3.7}$$

The MSE score of two images varies with different factors, indicating that the encryption method is highly sensitive to secret keys, as shown in Figure 3.9.

3.5.3 Analysis of Correlation

Digital images have strong correlations between neighbouring pixels, making it easier to obtain original image information. Reducing this correlation in all directions is crucial to ensuring security in image encryption. The relationship between the encrypted and original Lena images can be graphically shown in Figure 3.10. The encryption method's ciphertext's correlation coefficient is close to zero, lower than that of previous studies, indicating its competitiveness in this area, as shown in Table 3.2, which shows results in three different orientations.

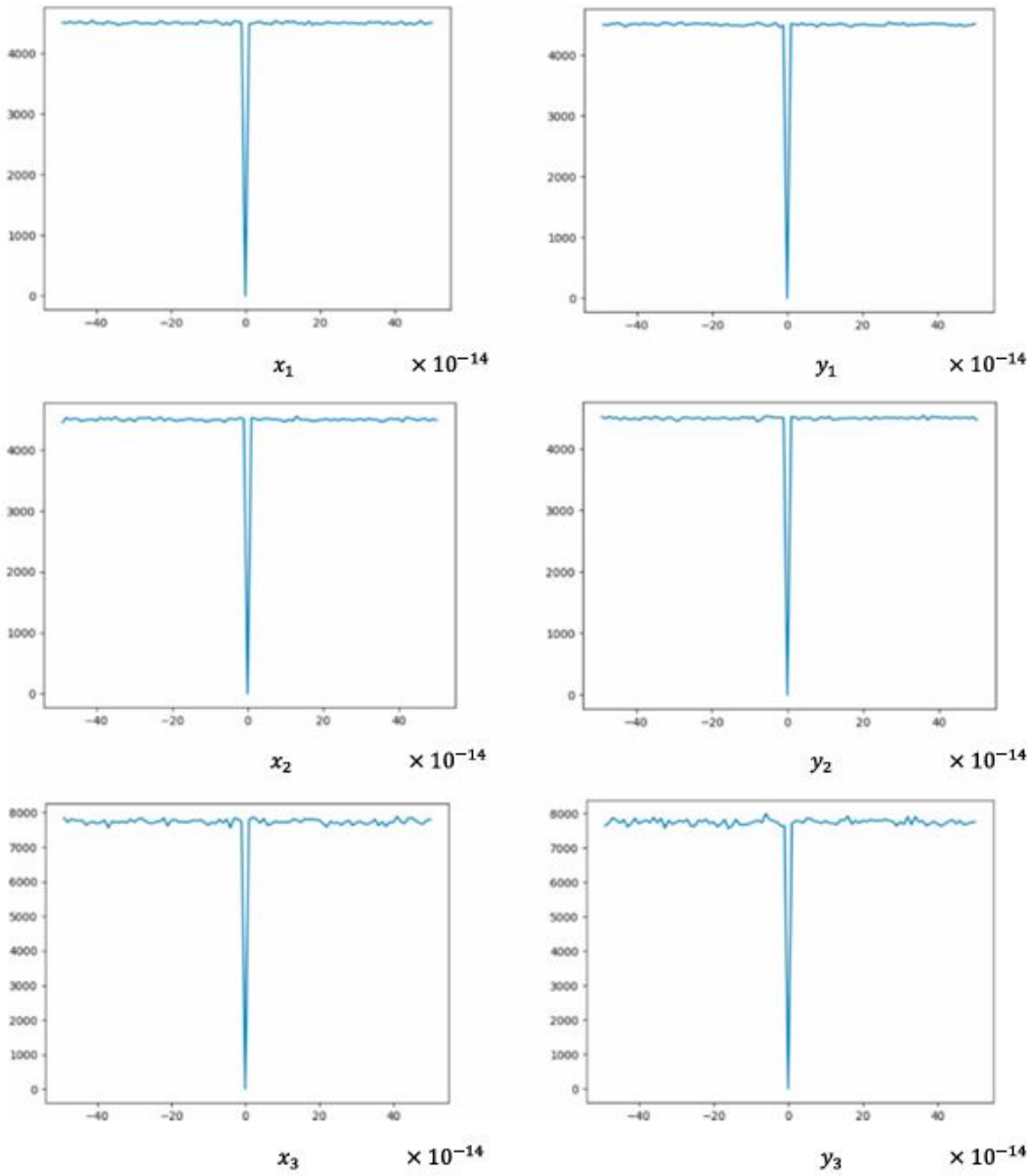


Figure 3.9: Key sensitivity Analysis in Decryption

3.5.4 Analysis of Histograms

One method for showing the distribution of pixels in an image is a histogram. In an ideal encrypted image, attackers cannot uncover any information. The histogram should be uniform, and the ciphertext image's values are pseudorandom, while the original image's values are widely dispersed. This technique effectively prevents attacks based on statistical analysis on encrypted images as shown in Figure 3.11.

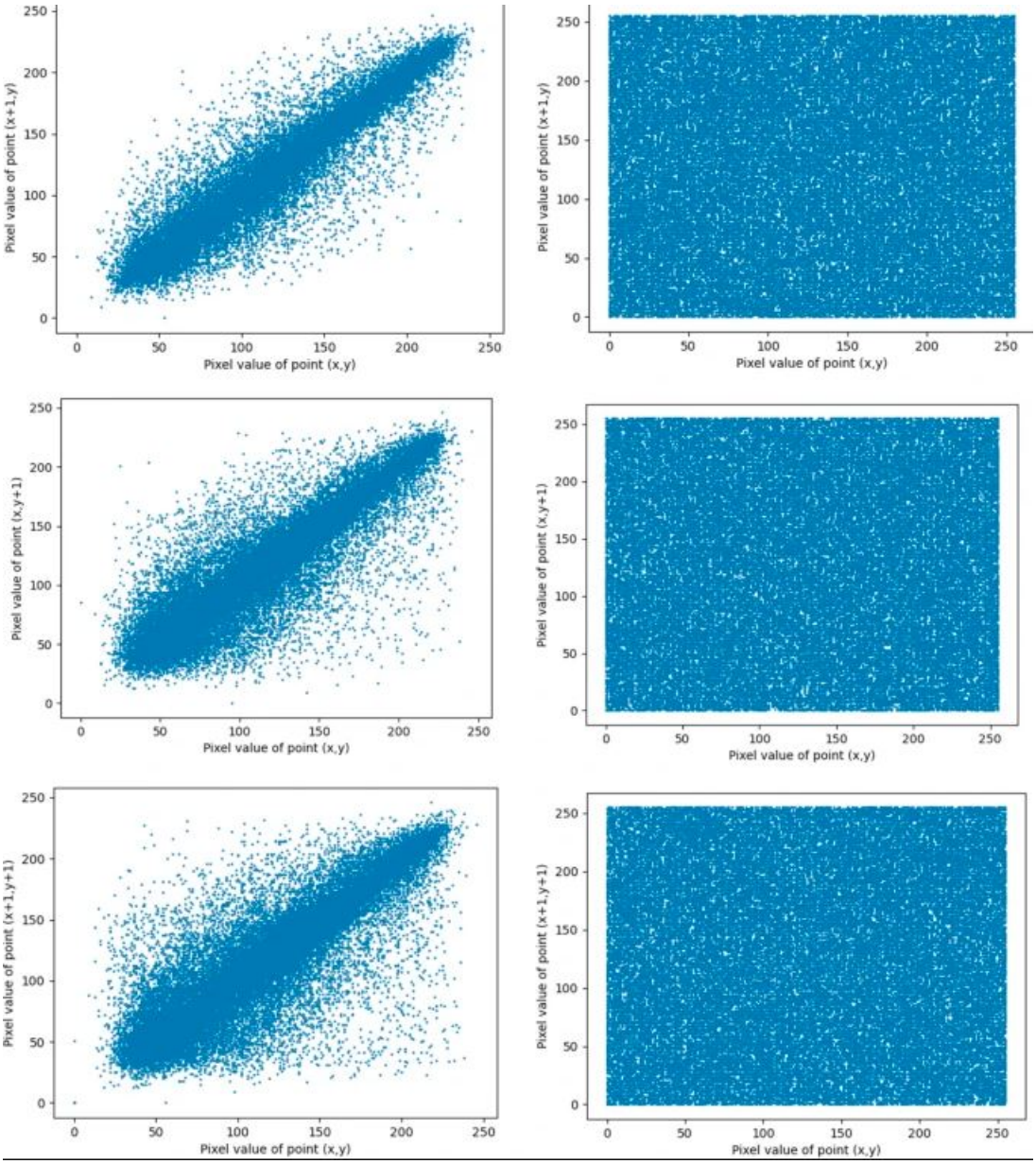


Figure 3.10: Two-Dimensional Pixel Correlation Mapping

3.5.5 Information Entropy

Information entropy is a key performance indicator in sequence randomization, determining the diffusion level of each grey-level pixel and quantifying the unpredictability of the image. The image. The optimal entropy value for encrypted messages is 8, and better encryption algorithm security performance is linked to greater resilience to statistical attacks. The following is the calculating formula:

$$H(x) = -\sum_{i=1}^{M} P(x_i) \log_2 P(x_i) \tag{3.8}$$

Table 3.2: Adjacent Pixel Correlation Analysis

Direction	**Images**	**Horizontal**	**Vertical**	**Diagonal**
Original Image	Lena	0.96896	0.93654	0.91390
	Boat	0.94761	0.93374	0.88732
	Camera	0.97309	0.96133	0.93481
Encrypted Image	Lena	-0.00199	-0.00189	0.00616
	Boat	0.00162	-0.00063	0.00055
	Camera	0.00116	0.00514	-0.00872
Ref. [137]	Lena	-0.01589	-0.06538	-0.03231
Ref.[133]	Lena	-0.09742	0.04844	-0.07068
Ref. [138]	Lena	0.0024	-0.0017	0.0011
Ref. [135]	Lena	0.000488	-0.000549	0.004539
Ref. [139]	Lena	-0.0005	0.0057	0.0032
Ref. [136]	Lena	-0.0084	-0.0018	0.0002
	Boat	-0.00067	-0.03736	-0.00075
	Camera	0.00466	0.00868	-0.0084

in which $P(x_i)$ is the likelihood that a point in the sequence with the value of pixels of x_i will occur. Table 3.3 displays the computed outcomes. The results indicate that the encrypted picture is chaotic and random-like, as the information entropy of this approach is bigger than the results of some other research and is quite near to the optimal value of 8.

3.5.6 Defending Against Distinct Attacks

Algorithms for image encryption need to be resilient to several kinds of attacks. Resistance to differential attack is measured using two indices: the unified average change intensity (UACI) and the number of pixels change rate (NPCR). Ideal values for NPCR and UACI are 0.9991 and 0.3346, respectively. Table 3.4 show that NPCR and UACI are around the optimal values, indicating the algorithm's ability to withstand differential attacks.

3.5.7 Robust Analysis

Digital images will unavoidably be impacted by various disruptions or data loss during the transfer process. An effective cryptographic system should be resilient to attacks that result in data loss and noise. The test shows how effectively the proposed method handles attacks,

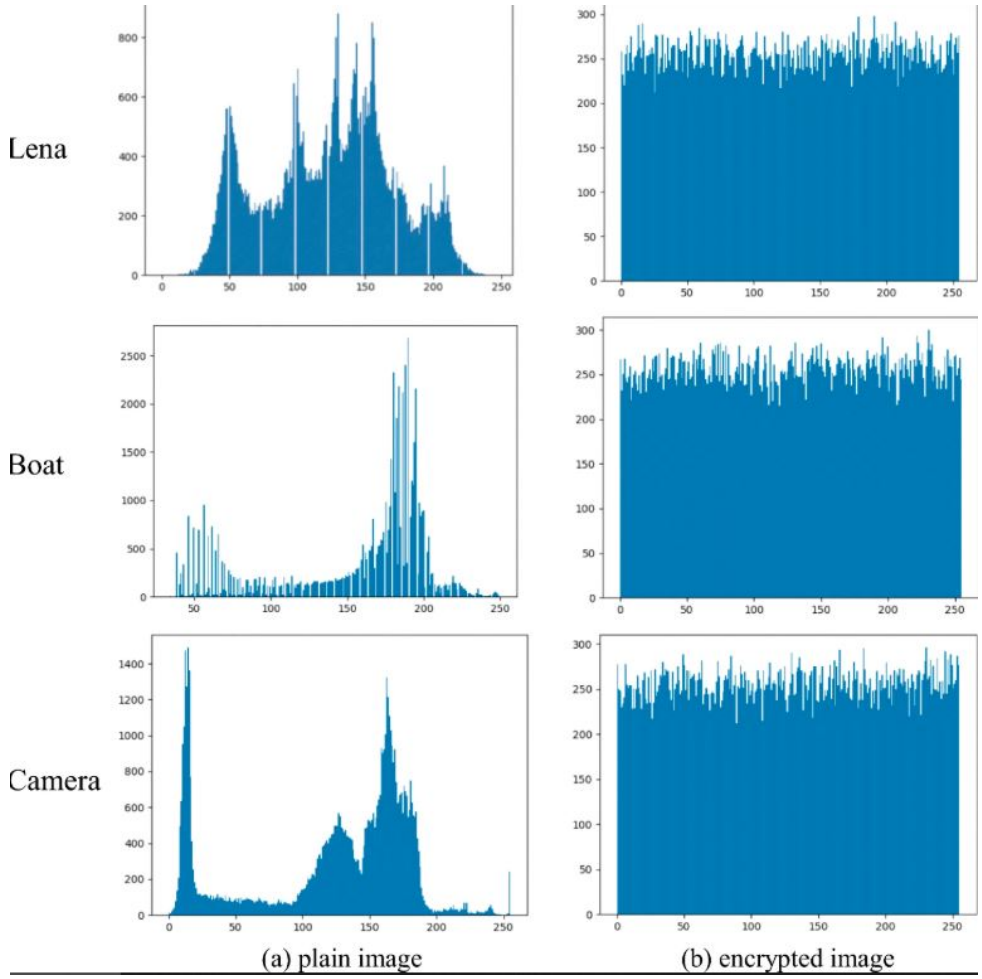


Figure 3.11: Histogram Evaluation (a) Plain image (b) Encrypted image

including data loss and noise interference. The Figure 3.12 illustrates the strong robustness of our encryption system by showing that the decrypted images can still be correctly identified even in the face of noise and data loss attacks.

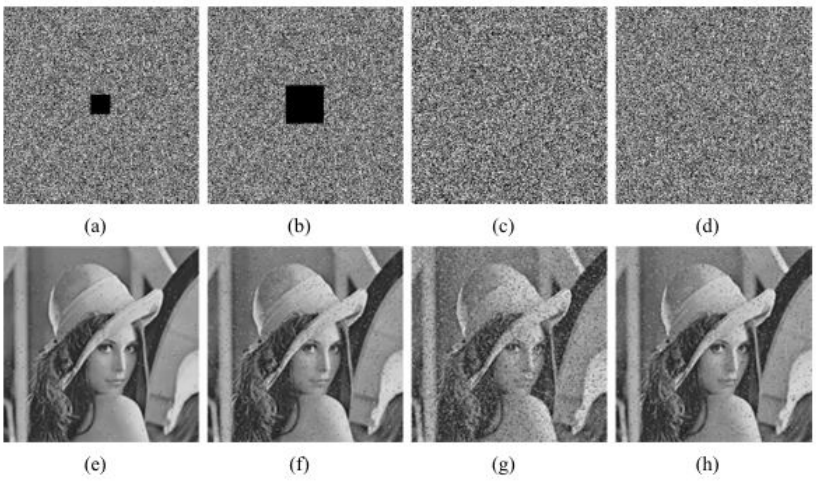


Figure 3.12: Robustness Analysis

Table 3.3: Information Entropy Measurements Across Test Datasets

Algorithms	**Images**	**Information Entropy**
Ref. [132]	Lena	7.9982
	Boat	7.9938
	Camera	7.9957
Ref.[140]	Lena	7.9977
Ref.[134]	Lena	7.9970
Ref.[139]	Lena	7.9975

Table 3.4: Differential Attack Resistance Metrics

Algorithms	**Images**	**NPCR**	**UACI**
Ref.[132]	Lena	0.995971	0.332476
	Boat	0.996185	0.332210
	Camera	0.996154	0.333230
Ref.[133]	Lena	0.996840	0.334390
Ref. [140]	Lena	0.996692	0.335051
Ref.[138]	Lena	0.996094	0.334653
Ref.[135]	Lena	0.996094	0.334215
Ref.[136]	Lena	0.996418	0.335581
	Boat	0.996278	0.336004
	Camera	0.996015	0.335737

3.5.8 Analysis of Speed

Another crucial metric for image encryption techniques is computational speed. In this test, a 3.2 GHz CPU and 8.00 GB of RAM replicate the encryption process using VC++. After hundreds of tests, the average time for the suggested image encryption algorithm for a 256×256 image is around 0.6933 s, making it very effective for real-world uses.

3.6 Transition to the Next Chapter

The findings of this study demonstrate how researchers have difficulties utilizing chaotic maps because of their limited parameter set, which leaves them open to attack by outside parties. New maps with additional parameters and wide ranges are required to address this. Balancing

computing effectiveness with cryptographic strength can be difficult when creating high-entropy random numbers. Another difficulty is creating new encryption methods that are both highly secure and computationally inexpensive. Using highly non-linear strings of random integers produced by chaotic maps may be helpful.

CHAPTER 4

AN EFFICIENT ENCRYPTION TECHNIQUE BASED ON A COUPLED MAP LATTICES

4.1 Introduction

This research aims to fill gaps in the field of efficient encryption techniques based on coupled map lattices despite significant progress made. However, CMLs-based encryption methods lack practical efficacy, necessitating future research on their application in real-world scenarios like healthcare or financial industries. Current research may not fully cover the scalability of CMLs-based encryption algorithms, so further studies could explore their effectiveness and safety under various data and user loads. The study aims to improve the effectiveness of chaotic map models, improve randomness, and develop secure encryption methods for digital applications. There are four phases in the research methodology. The first is the construction of a novel coupled map lattices. The second step analyzes the efficacy of the coupled map lattice (CMLs), in which we calculate the Lyapunov exponent, approximation entropy, etc. The third step describes the construction of an encryption algorithm based on the new CMLs system. The last step describes the implementation of the algorithm in MATLAB and tests its validity and functionality.

4.2 Contribution of the Research

This chapter introduces a new encryption method using coupled map lattices (CMLs), which improves chaotic behavior and security properties. This technology overcomes the limitations of previous chaos-based systems and conventional cryptographic techniques, generating dynamic and unpredictable keys suitable for digital communications and multimedia protection. The proposed encryption strategy, which features advanced features such as non-linear and two-way

coupled logistic map lattices, is validated through performance assessments and simulation findings. This study advances chaos-based cryptography, paving the way for further research in machine learning and quantum cryptography.

4.3 Proposed CMLs Map

The CMLs system has been widely used in encryption methods due to its good chaotic features [13]. The CMLs system may be defined using Eq. (4.1):

$$x_{n+1}^{(i)} = (1-\varepsilon) f\left(x_n^{(i)}\right) + \frac{\varepsilon}{2}\left[f\left(x_n^{(i-1)}\right) + f\left(x_n^{(i+1)}\right)\right] \tag{4.1}$$

i is the lattices number, n is the time component, and $\varepsilon \in (0,1)$ is the coupling coefficient. $f(x_n)$ is any chaotic map.

To tackle the shortcomings in classical CMLs, we try to construct a new CMLs with a wide range and more initial parameters. In the new CMLs, we used logistic map $x_{n+1} = r \cdot (1-x_n)$ and a unique sine map. The new map is given in Eq.(4.3).

$$f(x_n) = \mod\left(ux_n(i)(1-x_n) + e^t(10-u)\sin\left(\frac{\pi x_n(i)}{10}\right), 1\right) \tag{4.2}$$

$$\begin{aligned} x_{n+1} = (1-\varepsilon)\cdot & \mod\left(ux_n(i)(1-x_n) + e^t(10-u)\sin\left(\frac{\pi x_n(i)}{10}\right), 1\right) \\ + \frac{\varepsilon}{2}\Bigg(& \mod\left(ux_{n-1}(i)(1-x_{n-1}) + e^t(10-u)\sin\left(\frac{\pi x_{n-1}(i)}{10}\right), 1\right) \\ + & \mod\left(ux_{n+1}(i)(1-x_{n+1}) + e^t(10-u)\sin\left(\frac{\pi x_{n+1}(i)}{10}\right), 1\right)\Bigg) \end{aligned} \tag{4.3}$$

4.4 Analysis of New Map

4.4.1 Bifurcation Diagram

After setting ranges for ε and u, a grid of every possible combination is generated. The system iterates from an initial condition $(x = 0.5)$ for every pair (ε, u). First, temporary iterations are eliminated to give the system time to settle. After reaching a steady state, the values of (ε, u, x) are stored. A three-dimensional scatter plot is produced, with the $z-axis$ showing the appropriate steady-state x values and the x and y axes representing ε and u, respectively.

The resulting graph in Figure 4.1 provides a bifurcation diagram of the new map. It displays the effects of changing ε and u, raising ε can cause bifurcation thresholds to change or generate new stable states.

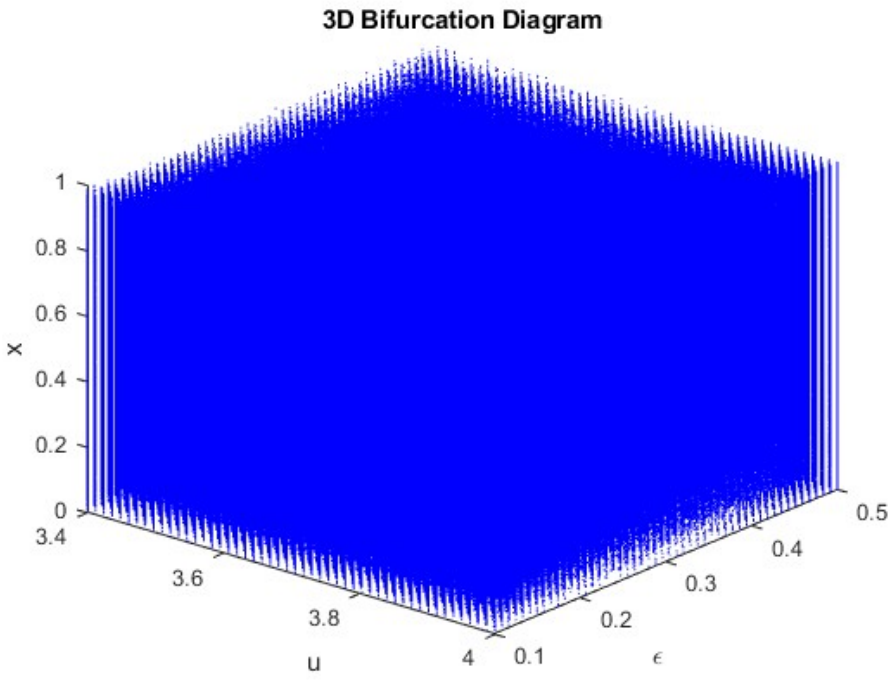


Figure 4.1: Bifurcation Diagram

4.4.2 Lyapunov Exponent

To calculate the Lyapunov exponent (λ) for the given coupled map lattice system, we follow these steps: The system is defined by:

$$x_{n+1}(i) = (1-\varepsilon)\cdot f(x_n(i)) + \frac{\varepsilon}{2}\left[f(x_{n-1}(i)) + f(x_{n+1}(i))\right]$$

where,

$$f(x) = \text{mod}\left(ux(1-x) + e^t(10-u)\sin\left(\frac{\pi x}{10}\right), 1\right)$$

For a 1D coupled map lattice, we approximate it using the Jacobian matrix of the system.

Compute the Derivative of the Local Map The derivative of f(x) (ignoring the mod discontinuity) is:

$$f'(x) = u(1-2x) + e^t(10-u)\left(\frac{\pi}{10}\right)\cos\left(\frac{\pi x}{10}\right)$$

For a 3-node system, the Jacobian matrix J at each iteration is:

$$J = \begin{bmatrix} (1-\varepsilon)f'(x_n(1)) & \frac{\varepsilon}{2}f'(x_n(2)) & 0 \\ \frac{\varepsilon}{2}f'(x_n(1)) & (1-\varepsilon)f'(x_n(2)) & \frac{\varepsilon}{2}f'(x_n(3)) \\ 0 & \frac{\varepsilon}{2}f'(x_n(2)) & (1-\varepsilon)f'(x_n(3)) \end{bmatrix}$$

For coupled systems, we compute the Jacobian matrix and use QR decomposition.
The Lyapunov exponent λ is computed through the following iterative process:
Initialization:

- Random initial state x_0
- Identity matrix $Q = I$
- Lyapunov sum $\lambda_{\text{sum}} = 0$

Iterative calculation (for $n = 1$ to N):

1. Update the state x_n using the map function
2. Compute Jacobian J at x_n
3. Perform QR decomposition: $JQ = Q'R$
4. Update $\lambda_{\text{sum}} \leftarrow \lambda_{\text{sum}} + \log|\operatorname{diag}(R)|$

Final calculation:

$$\lambda = \frac{\lambda_{\text{sum}}}{N} \tag{4.4}$$

$$le - sum = 5.7159e+03$$

For computing a modified logistic map's 2D Lyapunov exponent map, which is shown in Figure 4.2, which incorporates an external coupling parameter (ε). One important indication of chaos $(\lambda > 0)$, stability $(\lambda < 0)$, or periodicity $(\lambda \approx 0)$ in a dynamical system is the Lyapunov exponent (λ), which calculates the average rate of divergence or convergence of neighboring trajectories.

4.4.3 KS Entropy

The KS entropy (h_{KS}) measures the rate of information production in a system. For a 1D map, it equals the sum of positive Lyapunov exponents:

$$h_{KS} = \sum_{\lambda_i > 0} \lambda_i$$

where λ_i are the Lyapunov exponents.
Compute Lyapunov Exponents For a system defined by $x_{n+1} = f(x_n)$:

- **Derivative**: Calculate $f'(x)$

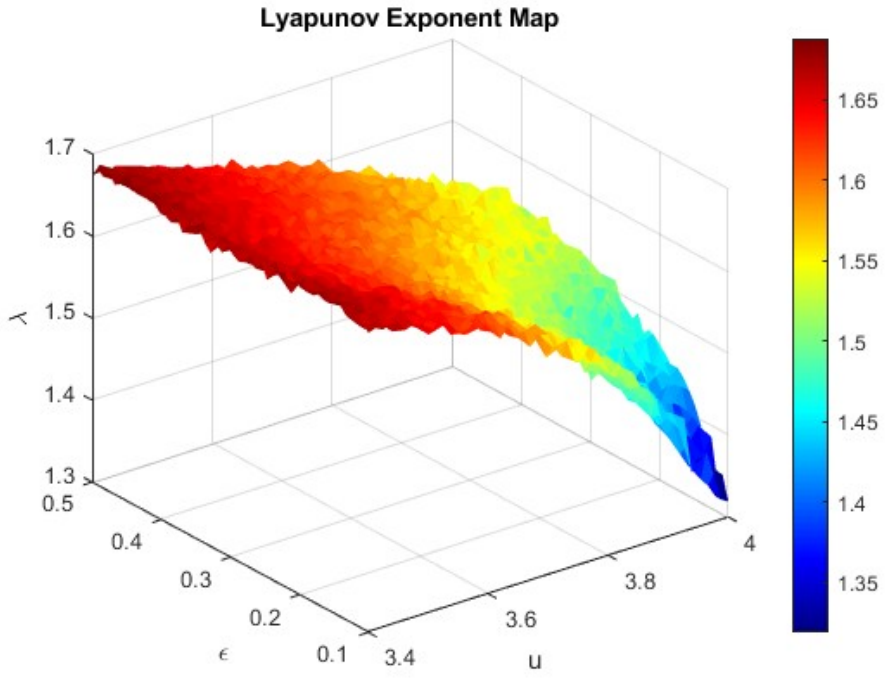


Figure 4.2: Lyapunov Exponent

- **Iterate**: Track the logarithmic derivative along a trajectory:

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \ln |f'(x_n)|$$

Sum Positive Exponents

$$h_{KS} = \begin{cases} \lambda & \text{if } \lambda > 0 \\ 0 & \text{otherwise} \end{cases}$$

For **coupled maps** (e.g., 3 nodes), sum all positive λ_i:

$$h_{KS} = \sum_{\substack{i \\ \lambda_i > 0}} \lambda_i \tag{4.5}$$

A computational method used to generate a 3D Kolmogorov-Sinai (KS) entropy map for a coupled logistic map system, as shown in Figure 4.3, that helps to visualize the formation of chaos under different logistic parameters (u) and coupling strengths (ε). The method calculates the logistic map for each pair (ε, u) iteratively, starting at $x = 0.5$, while monitoring its derivative to show local sensitivity to initial conditions, and averaging the logarithm across repetitions to estimate the LE. The LE is kept as the KS entropy if it is positive $h_{KS} > 0$ (Chaotic (higher = more unpredictable)); if not, it is set to zero $h_{KS} = 0$ (Predictable (periodic/stable) dynamics).

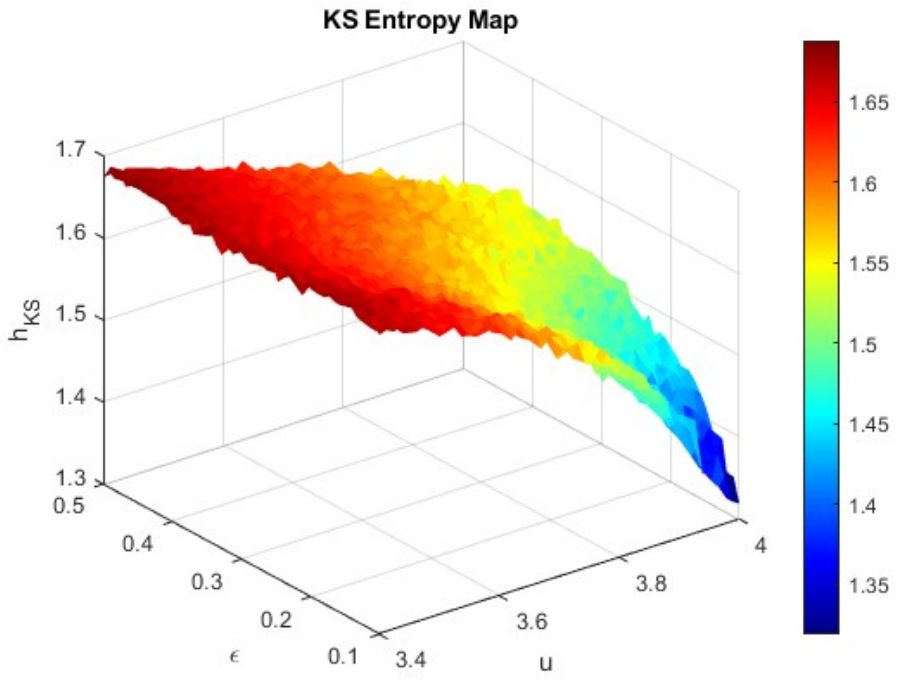


Figure 4.3: KS Entropy

4.4.4 Acceleration Coefficient

A 3D acceleration map in Figure 4.4 provides a detailed analysis of the acceleration coefficient of chaotic systems. Through various coupling strengths (ε) and values of logistic parameters (u) to analyze the dynamics of a coupled logistic map system. Acceleration is computed using the second-order difference of the system's state.

Simulate the System First, iterate the map to obtain the time series $x_n(i)$ for each node i, discarding transients to focus on steady-state behavior.

Compute Acceleration For each node i (e.g., the center node $i = 2$ in a 3-node system):

1. **Finite Difference**: Calculate the second-order difference for all valid time steps n:

$$a_n(i) = x_{n+1}(i) - 2x_n(i) + x_{n-1}(i)$$

2. **Magnitude**: Take the absolute value $|a_n(i)|$ to focus on the magnitude of acceleration:

$$|a_n(i)| = |x_{n+1}(i) - 2x_n(i) + x_{n-1}(i)|$$

3. **Average**: Compute the mean acceleration over time to summarize the system's dynamics:

$$\bar{a}(i) = \frac{1}{N-2} \sum_{n=2}^{N-1} |a_n(i)| \tag{4.6}$$

The 3D Acceleration Map demonstrates how the acceleration coefficient varies with logistic parameters and coupling strength. High acceleration indicates rapid state changes, typically near bifurcations or in chaotic regimes. Low acceleration suggests smooth, predictable dynamics (e.g., periodic or fixed-point behavior). Node-specific insights compare acceleration across nodes to study synchronization or localized chaos.

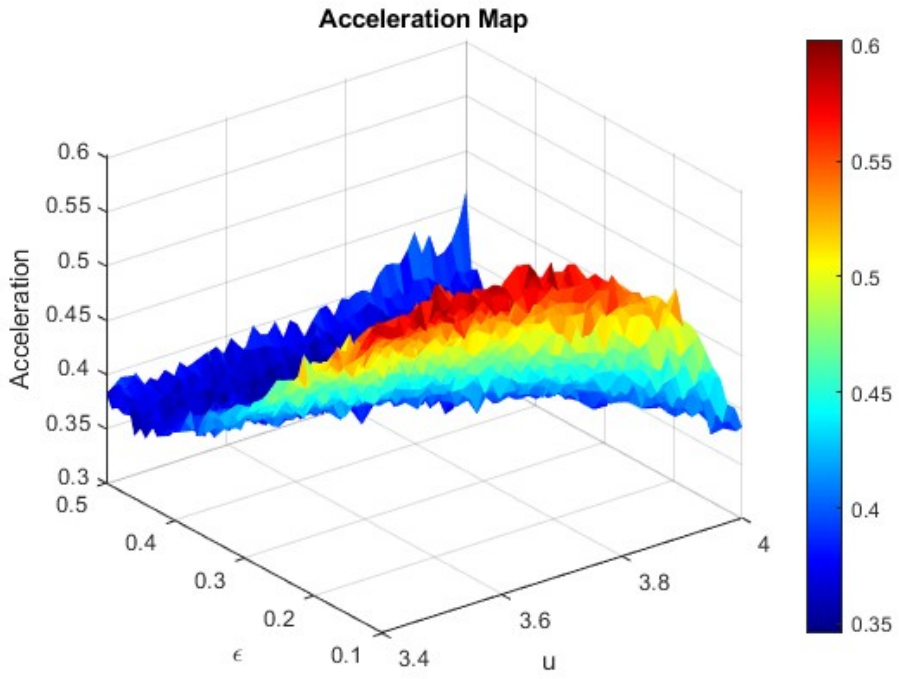


Figure 4.4: Acceleration Coefficient

4.4.5 Correlation Coefficient

To compute the correlation coefficient for the system, we need to analyze how the states x_n or $x_n(i)$ correlate over time or space. The Eq 4.3. describes a coupled logistic map with the following components:

- A **nonlinear term**:

$$ux_n(i)(1-x_n),$$

  where u controls the nonlinearity and $x_n(i)$ represents the state at time n and position i.

- A **sinusoidal perturbation**:

$$e_t(10-u)\sin\left(\frac{\pi x_n(i)}{10}\right),$$

  where e_t modulates the strength of the external forcing.

- **Coupling between nearest neighbors** $x_{n-1}(i)$ and $x_{n+1}(i)$ with strength $\varepsilon/2$, introducing spatial interactions:
$$\frac{\varepsilon}{2}\left(\mathrm{mod}(\dots)+\mathrm{mod}(\dots)\right).$$
- A **modulo operation** $\mathrm{mod}(\cdot,1)$ to ensure the state x_n remains bounded in the interval $[0,1]$.

The correlation coefficient r measures the linear relationship between consecutive states x_n and x_{n+1}:

$$r = \frac{\sum_{n=1}^{T-1}(x_n-\bar{x})(x_{n+1}-\bar{x})}{\sqrt{\sum_{n=1}^{T-1}(x_n-\bar{x})^2 \sum_{n=1}^{T-1}(x_{n+1}-\bar{x})^2}} \tag{4.7}$$

where $\bar{x}$ is the mean of the time series.

The correlation coefficient r provides insight into the dynamical behavior of the system: When $r \approx 1$, the system exhibits *strong positive correlation*, indicating predictable, periodic behavior where consecutive states are nearly identical. A value of $r \approx 0$ suggests *no correlation*, characteristic of chaotic systems where states become effectively uncorrelated over time. Finally, $r \approx -1$ reflects *strong negative correlation*, typically observed in systems with period-2 oscillations where states alternate between high and low values. These correlations help characterize the system's stability and predictability. The 3D Correlation Map in Figure 4.5 shows how the correlation coefficient changes in connection to coupling strength, logistic parameter, and correlation coefficient.

4.4.6 Trajectory Map

The 3D trajectory map in Figure 4.6 shows how a state variable (x) changes in iterations, considering the coupling strength parameter ε. The state variable x indicates the numerical value of the system's state variable, while the coupling strength (ε) represents the degree to which the chaotic system alters its components' interaction. The trajectory shows non-repetitive, erratic patterns with unpredictable fluctuations throughout time. Chaotic systems are susceptible to initial conditions, as indicated by the dispersion of trajectory points. The structure never settles into a periodic orbit or fixed point, making long-term prediction impossible. The system's trajectory remains chaotic during iterations due to the supposedly random distribution of paths. The 3D trajectory map effectively displays a system's chaotic dynamics, highlighting the influence of coupling strength on the evolution of state variables and the system's non-periodic, unpredictable nature.

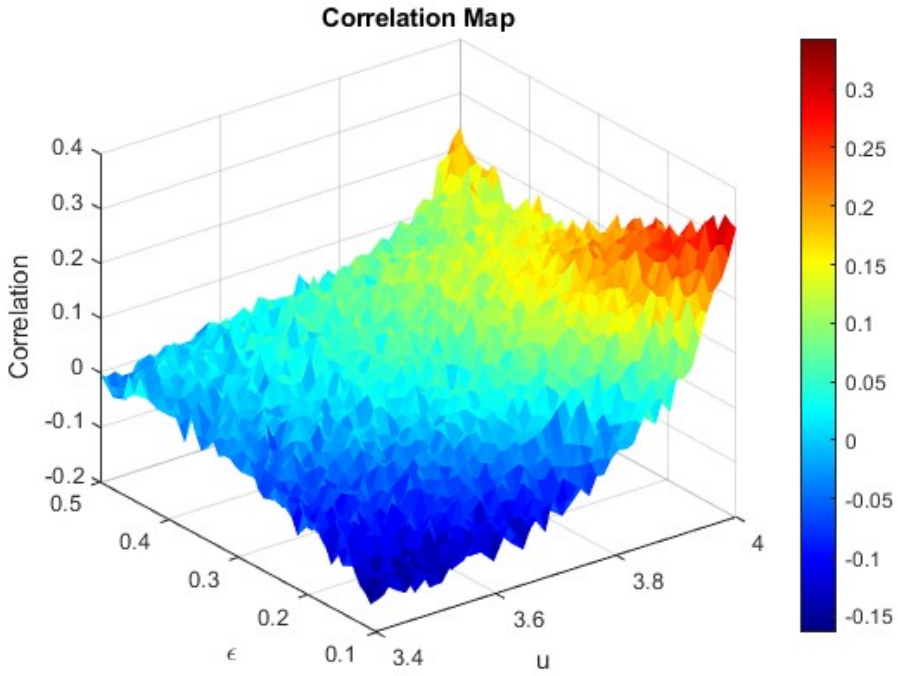


Figure 4.5: Correlation Coefficient

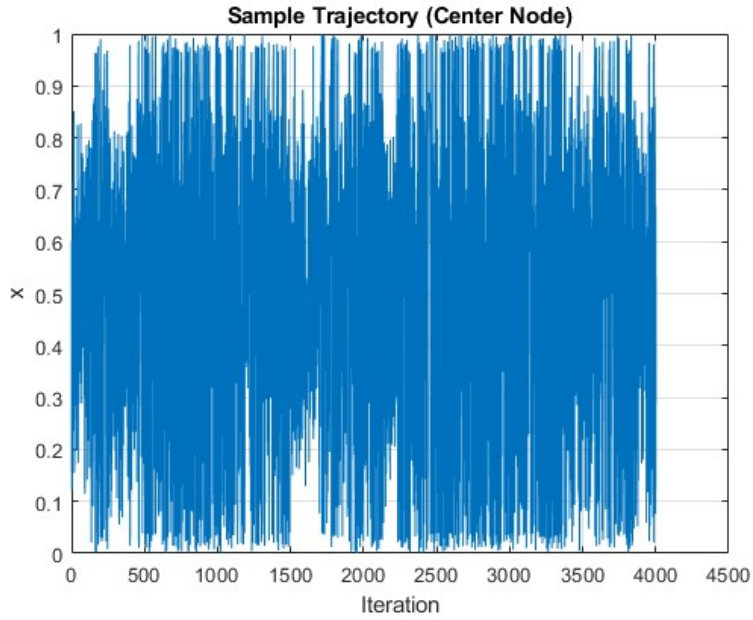


Figure 4.6: Trajectory Map

4.5 Enhanced Image Encryption Through Coupled Map Lattices Dynamics

4.5.1 Encryption Algorithm

This procedure outlines the complex image encryption process using a Coupled Map Lattices (CMLs) framework in Figure 4.7. Encryption components include random number generation,

modular arithmetic scrambling, and sorted pixel diffusion. Encryption leverages principles from chaos theory as its source of unpredictability. We have developed a new encryption scheme utilizing the updated CMLs map. Following are the key steps of the encryption scheme, as seen in Figure 4.8.

Step 1: Parameters Initialization Read the input grayscale image I. Convert the image I to a double-precision matrix if necessary. Define the parameters of the logistic map: $u = 3.5709$ (chaotic control parameter), $\varepsilon = 0.00075$ (coupling strength). Set the transient iterations $num_transient = 100$. Set the key iterations, $kp = 8192$. Initialize the chaotic sequence: Set the initial condition, $x(1) = 0.1$. Define the size of the lattice $L = 8$. Assign random initial values $x(1:L)$ using the normal seed values provided.

Step 2: Generate a chaotic key using the coupled map lattices Use the CMLs to generate a chaotic key for $n = 1$ to kp:

Regarding $m = 1$ to L:

Determine the nearest indices: $j = m+1, k = m-1$. Set recurring boundary conditions:

if $j = L+1, j = 1$,

if $k = 0, k = L$

Calculate the update for the chaotic map using the following:

$$y(m) = (1-\varepsilon)\cdot \mathrm{mod}\left(ux(m)(1-x(m)) + e^t(10-u)\sin\left(\frac{\pi x(m)}{10}\right), 1\right)$$
$$+\frac{\varepsilon}{2}\left(\mathrm{mod}\left(ux(k)(1-x(k)) + e^t(10-u)\sin\left(\frac{\pi x(k)}{10}\right), 1\right)\right.$$
$$\left.+\mathrm{mod}\left(ux(j)(1-x(j)) + e^t(10-u)\sin\left(\frac{\pi x(j)}{10}\right), 1\right)\right)$$

End the inner loop. The updated values should be kept in the chaotic key matrix K. Close the outer loop. It can be processed as in Algorithm 1.

Step 3: Create an encryption matrix from a chaotic key. Create an 8-bit integer key matrix from chaotic values:

$$AA1 = \mod\left(\mathrm{round}\left(B \times 10^{10}\right),\ 256\right)$$

Transform the key into a matrix

$$AA = reshape(AA1(1 : M \times N), M, N)$$

Step 4: Encrypt the image using modular addition Calculate the encrypted pixel values:

$$ENc(i,j) = \mod\left(I(i,j) + AA1,\ 256\right)$$

By doing this, it is guaranteed that the pixel values remain within the acceptable intensity range of 0 to 255.

Step 5: Pixel Diffusion Based on Sorting Create indices for pixel sorting:

$$\text{Idx} = 1 : (M \times N)$$

The encryption matrix K is sorted according to chaotic values:

$$\mathbf{Pr} = \text{sortrows}\left(\left[\mathbf{K}(:) \quad \text{Idx}\right], 1\right)$$

Put the encrypted image through a sorted transformation:

$$\mathbf{ENc1} = \text{sortrows}\left(\left[\mathbf{E}(:) \quad \mathbf{Pr}(:,2)\right], 2\right)$$

Convert back to an image format:

$$\mathbf{FENc} = \text{reshape}(\mathbf{E}_{\text{sorted}}, M, N)$$

Step 6: Show and Store the Outcomes Display the original and encrypted images. To analyze the pixel distribution, provide the histograms for the original and encrypted images. Additionally, include the chaotic key matrix $AA1$ and the final encrypted image **FENc**. The recommended encryption algorithm is outlined in Algorithm 2.

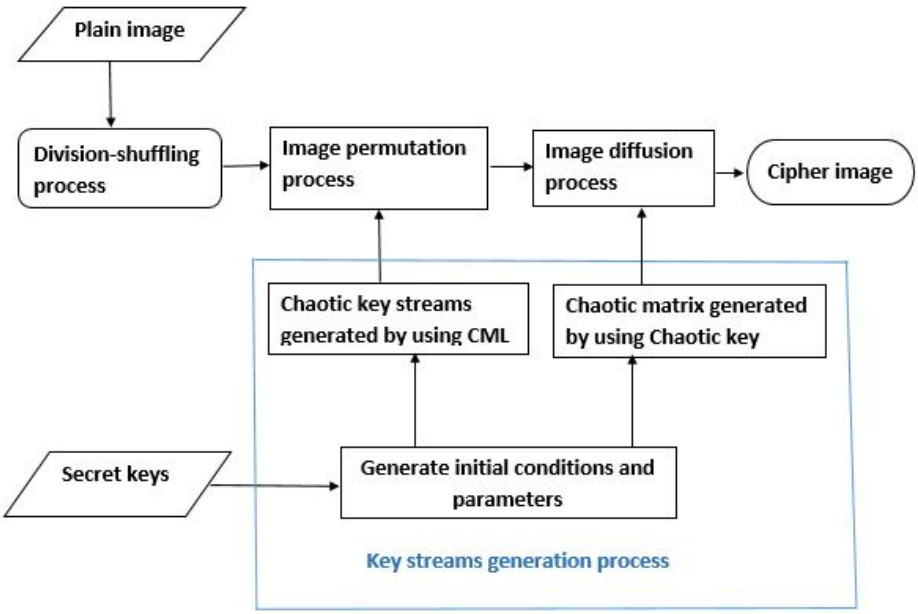


Figure 4.7: Schematic Diagram of the Proposed Encryption Scheme

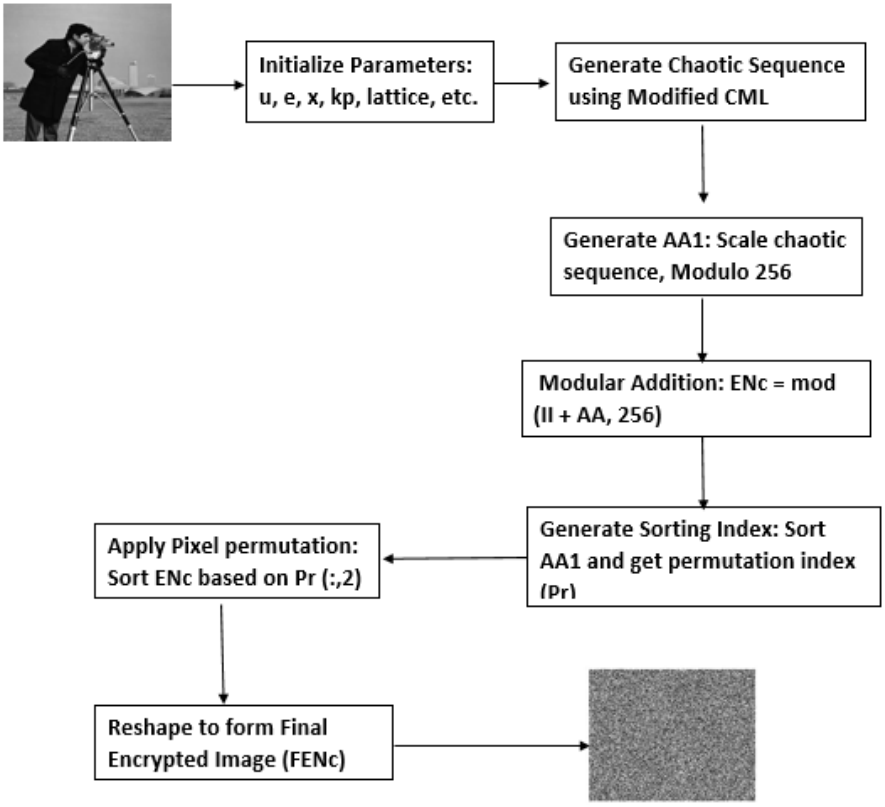


Figure 4.8: Schematic Diagram of the Encryption Process of the Proposed Scheme

4.5.2 Decryption Algorithm

The decryption algorithm reverses the encryption algorithm, as shown in Algorithm 3.

Step 1: Flatten the Encrypted Image Convert the 2D encrypted image matrix $FENc$ into a 1D vector $FENc_{flat}$. Linear indexing simplifies the reversal of pixel permutations applied during encryption.

Step 2: Reverse Pixel Permutation Use the permutation matrix Pr (stored during encryption) to restore the original pixel positions.

$Pr(:,2)$ contains the original indices of scrambled pixels.

Sort $FENc_{flat}$ $(Pr(:,2))$ to undo the permutation.

Step 3: Reshape to 2D Image Convert the 1D vector $ENc - flat$ back to the original 2D format Enc.

Restore the spatial structure of the image.

Step 4: Remove Key Matrix

Subtract the key matrix AA (used in encryption) and apply modulo 256.

Ensures pixel values wrap to the 8-bit range (0–255).

$$I_{decrypted}(x,y) = (ENc(x,y) - AA(x,y))mod256$$

Step 5: Display image After that, the final encrypted image $I_{decrypted}$ is transformed into an 8-bit unsigned integer format that can be used to display images. The decryption procedure for our suggested system is shown in Fig. 4.9.

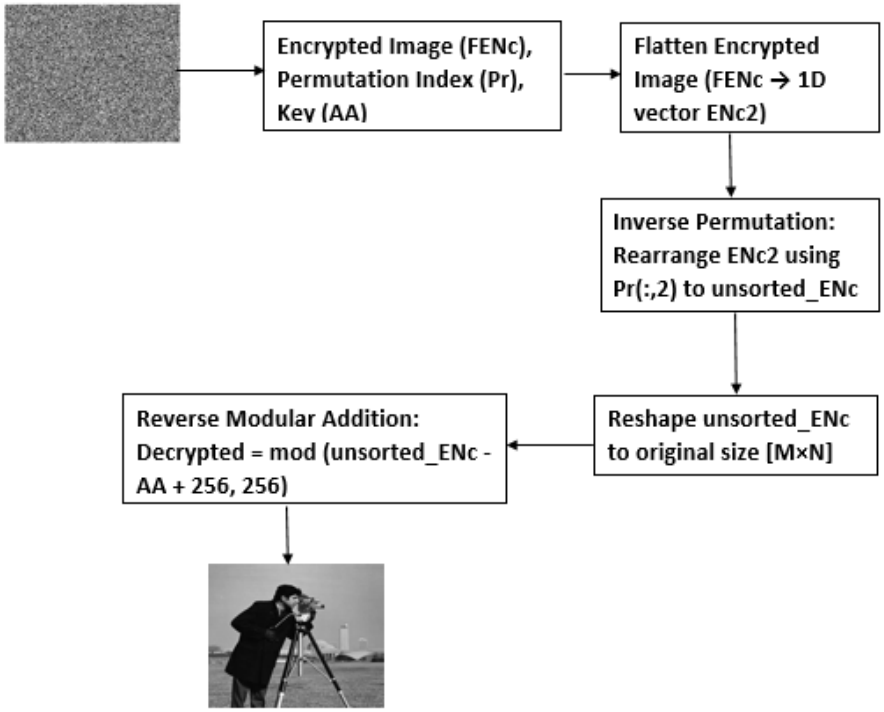


Figure 4.9: Schematic Diagram of the Decryption Process of the Proposed Scheme.

4.6 Statistical Analysis

4.6.1 Key Space

The proposed encryption technique utilizes a large key space, typically exceeding 2^{128}, to safeguard against brute-force attacks. It uses six starting values, each up to 14 digits long, exceeding the 2^{128} barrier, demonstrating strong cryptographic security.

Key components contribute to the key space in Table 4.1, which is determined by the suggested technique using a initial conditions and control parameters in a chaotic map.

Algorithm 1 Chaotic Image Encryption using Coupled Map Lattices (CMLs)

Input: Grayscale image I of size $M \times N$

Output: Chaotic key

Initialize Parameters

Read input image I and convert to grayscale if necessary.

Set logistic map parameter $u = 3.5709$

Set coupling strength $\varepsilon = 0.00075$

Set iteration limits $kp = 8192$, transient iterations $num\_transient = 100$

Set initial condition $x(1) = 0.1$

Define lattice size $L = 8$

Initialize chaotic sequence $x(1:L)$ using predefined values

Generate Chaotic Key using CMLs

for $n = 1$ to kp **do**

  for $m = 1$ to L **do**

    Set neighbouring indices $j = m+1$, $k = m-1$

    if $j = L+1$ **then**

      $j = 1$

    end if

    if $k = 0$ **then**

      $k = L$

    end if

    compute a chaotic update:

$$y(m) = (1-\varepsilon) \cdot \mathrm{mod}\left(ux(m)(1-x(m)) + e^t(10-u)\sin\left(\frac{\pi x(m)}{10}\right), 1\right)$$
$$+\frac{\varepsilon}{2}\left(\mathrm{mod}\left(ux(k)(1-x(k)) + e^t(10-u)\sin\left(\frac{\pi x(k)}{10}\right), 1\right)\right.$$
$$\left.+\mathrm{mod}\left(ux(j)(1-x(j)) + e^t(10-u)\sin\left(\frac{\pi x(j)}{10}\right), 1\right)\right)$$

  end for

  Store chaotic sequence in matrix $B(n, 1:L) = y(1:L)$

end for

Algorithm 2 Chaotic Key to Encryption Matrix

Input: Chaotic key

Output: Encrypted image $FENc$

Convert Chaotic Key to Encryption Matrix

Convert chaotic values to 8-bit key:

$$AA1 = \text{mod}(\text{round}(B \times 10^{10}), 256)$$

Reshape key into matrix

$$AA = reshape(AA1(1 : M \times N), M, N)$$

Encrypt Image Using Modular Addition

Compute encrypted pixel values:

$$ENc(i, j) = \text{mod}(I(i, j) + AA1, 256)$$

Sorting-Based Pixel Diffusion

Generate pixel sorting indices $Idx = 1 : (M \times N)$

Sort the encryption matrix K based on chaotic values:

$$P_r = \text{sortrows}([K(:), Idx], 1)$$

Apply sorted transformation:

$$ENc1 = \text{sortrows}([ENc(:), P_r(:, 2)], 2)$$

Reshape into a final encrypted image:

$$FENc = \text{reshape}(ENc1(:, 1), M, N)$$

Save the encrypted image $FENc$

Algorithm 3 Image Decryption

1: **Input:** Encrypted image $FENc$, key matrix AA, permutation table Pr
2: **Output:** Decrypted image $I\_decrypted$
3: Flatten $FENc$ into vector $FENC\_flat$
4: $indices \leftarrow Pr(:,2)$
5: $ENc\_flat \leftarrow FENC\_flat(indices)$
6: $ENc \leftarrow \text{reshape}(ENc\_flat, \text{size of original image})$
7: $I\_decrypted \leftarrow \text{mod}(ENc - AA, 256)$
8: Convert $I\_decrypted$ to `uint8` format.
9: Display decrypted images.

Table 4.1: Key Components and Their Contribution to Key Space

Parameter	**Description**	**Range / Values**	**Precision Contribution**
$x_1, x_2, \ldots, x_8$	Initial conditions for lattice points	Real numbers in $[0.01, 0.20]$	$(10^{10})^8 = 10^{80}$
e	Coupling strength	Real, e.g., 0.00075	10^{10}
u	Logistic map parameter (e.g., 3.5709)	Tunable (optional)	10^{10}

Total key space calculation:

$$\text{Key Space} = 10^{80} \times 10^{10} \times 10^{10} = 10^{100} \approx 2^{332}$$

Key space conversion to binary scale:

$$\log_2(10^{100}) = 100 \cdot \log_2(10) \approx 100 \cdot 3.32 \approx 332$$

$$\text{Key Space} \approx 2^{332}$$

Table 4.2 illustrates the key space of a proposed encryption method, which is determined by averaging eight starting values, coupling coefficients, and control parameters with a precision of 10^{-10} for each parameter. The key space increases to 10^{100} or 2^{332}.

4.6.2 NIST Analysis

The NIST SP 800-22 test suite evaluates cryptographic randomness, with most tests passing, as shown in Table 4.3. However, the random excursion variation test revealed nonrandom

Table 4.2: Value of Keyspace in All Test Results

Algorithms	**Keyspace**
Our Algorithm	10^{100}
Existing map [132]	10^{84}
Ref.[133]	10^{56}
Ref.[134]	10^{56}
Ref.[135]	10^{56}
Ref.[136]	10^{6}

behavior in states -4.0 to -2.0 ($p<0.01$), despite essential tests such as the frequency test ($p = 0.78$), the run test ($p = 0.32$) and the spectral test ($p = 0.69$), indicating small correlations in the output sequence. Most tests passed, including unpredictability (linear complexity, p=0.19) and bit independence (Serial Test, p=0.06/0.21). The findings suggest a strong generator with fixable flaws that require enhancement for high-security requirements without compromising overall quality.

4.7 Security Analysis

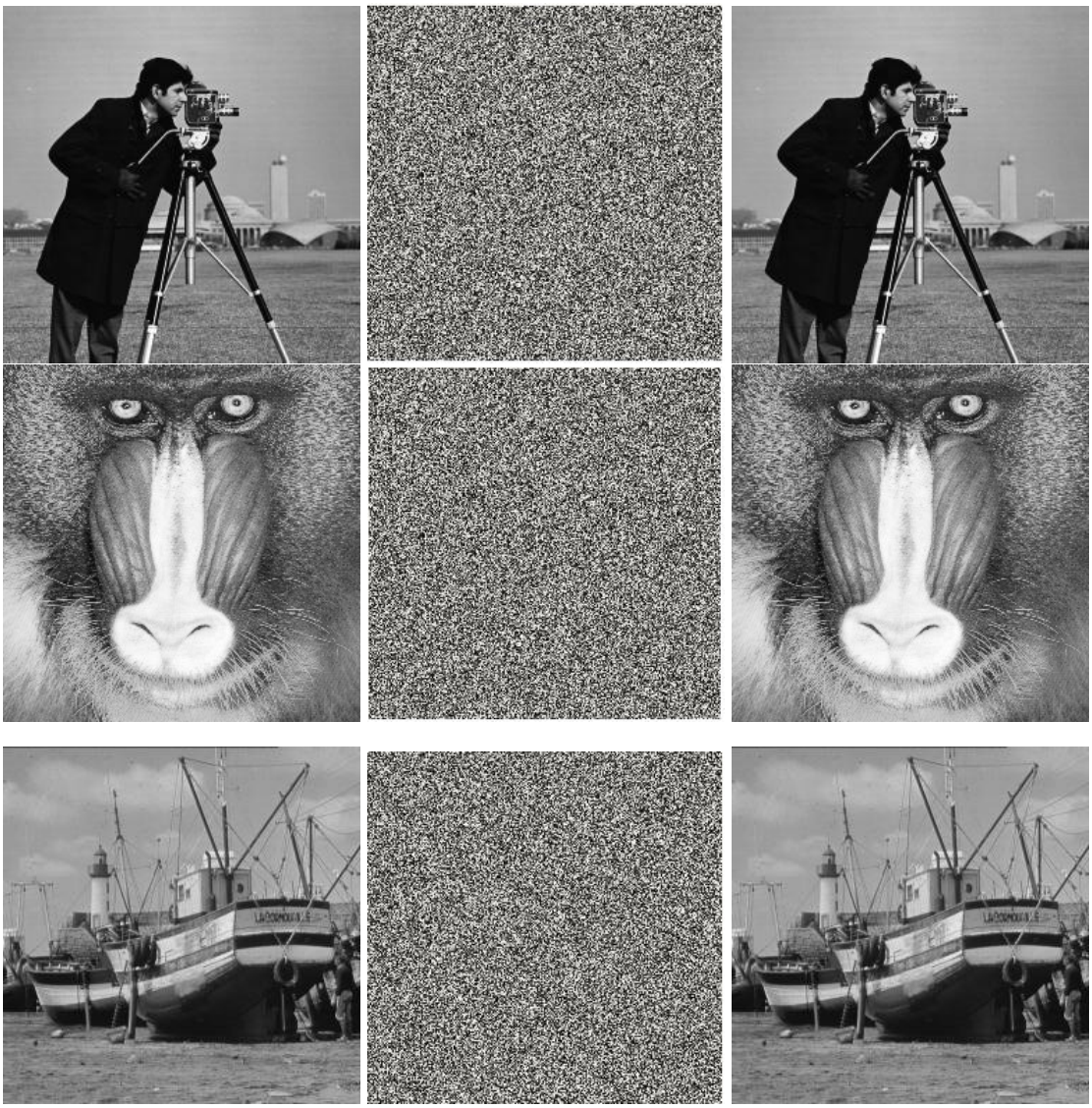
The performance and security of the encryption algorithm were evaluated by simulation tests using 10^{10} repetitions, with the first 500 numbers excluded to minimize volatile results. The development tool used is MATLAB R2023a on a Windows 10 Pro system with 8.00 GB of RAM and an Intel(R) Core(TM) i5-5200U CPU running at 2.20 GHz. The experiment's results are presented in Fig. 4.10.

4.7.1 Key Sensitivity Analysis

This experiment demonstrates that the approach is sensitive to keys, as seen in Figure 4.11. A modified key is used to encrypt the cipher image, while the original keys are used to encrypt the cameraman grayscale image. It highlights the need to examine chaotic systems for characteristics sensitive to initial conditions before using them for image encryption, as even slight changes can significantly deviate from the intended outcome.

4.7.2 Occlusion Attack

To simulate partial damage or data loss, an occlusion attack purposefully turns specific pixels in the cipher image to zero. Following this alteration, the appropriate keys are used to decode the image. The peak signal-to-noise ratio (PSNR) between the original and decrypted image is



(a) Original Image (b) Encrypted Image (c) Decrypted Image

Figure 4.10: Comparison of Original, Encrypted, and Decrypted Images

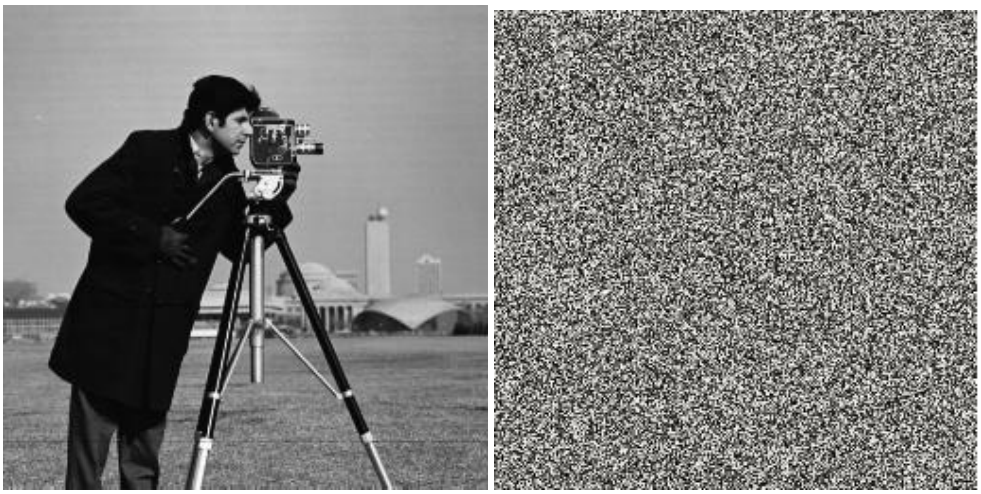
Table 4.3: NIST SP 800-22 Randomness Test Results

Test Name	**P-Value**	**Conclusion**
01. Frequency Test (Monobit)	0.78255	Random
02. Frequency Test within a Block	0.02365	Random
03. Run Test	0.32417	Random
04. Longest Run of Ones in a Block	0.33693	Random
05. Binary Matrix Rank Test	0.61028	Random
06. Discrete Fourier Transform (Spectral) Test	0.68638	Random
07. Non-Overlapping Template Matching Test	0.64597	Random
08. Overlapping Template Matching Test	0.11361	Random
09. Maurer's Universal Statistical Test	0.10256	Random
10. Linear Complexity Test	0.19275	Random
11. Serial Test	0.06406	Random
	0.21004	Random
12. Approximate Entropy Test	0.27529	Random
13. Cumulative Sums (Forward) Test	0.49674	Random
14. Cumulative Sums (Reverse) Test	0.74397	Random
15. Random Excursions Test	0.89515	Random
16. Random Excursions Variant Test	0.55997	Random

computed to assess the system's robustness. Table 4.4 illustrates the relevant MSE and PSNR values for different occlusion zones. The results indicate that the proposed encryption technique effectively resists occlusion attacks.

4.7.3 Analysis of Histogram

The histogram statistically represents the frequency of each tonal value in an image. A resilient IE method should have a uniform ciphertext image histogram, which makes it immune to statistical attacks and prevents the observation of plaintext image information. The histogram of encrypted images is notably different from those of plaintext images, as shown in Fig. 4.12 In addition, the variability of the tonal value in the encrypted image histogram is quantitatively assessed using variance and the chi-square χ^2 test. To pass the χ^2 test for encrypted images, which has 255 degrees of flexibility and a significance threshold of $\alpha = 0.05$, the value must be less than 293.25. The variance findings and χ^2 tests for the various images are presented in



(a) Correct decrypted image (b) Error decrypted image

Figure 4.11: Key Sensitivity Analysis. (a) Error-Decrypted Image. (b) Correct Decrypted Image

Table 4.4: MSE and PSNR Values

Image	**MSE**	**PSNR**
Cameraman	61.7026	12.3247
Lena	60.0132	12.5659
Boat	61.5905	12.3405

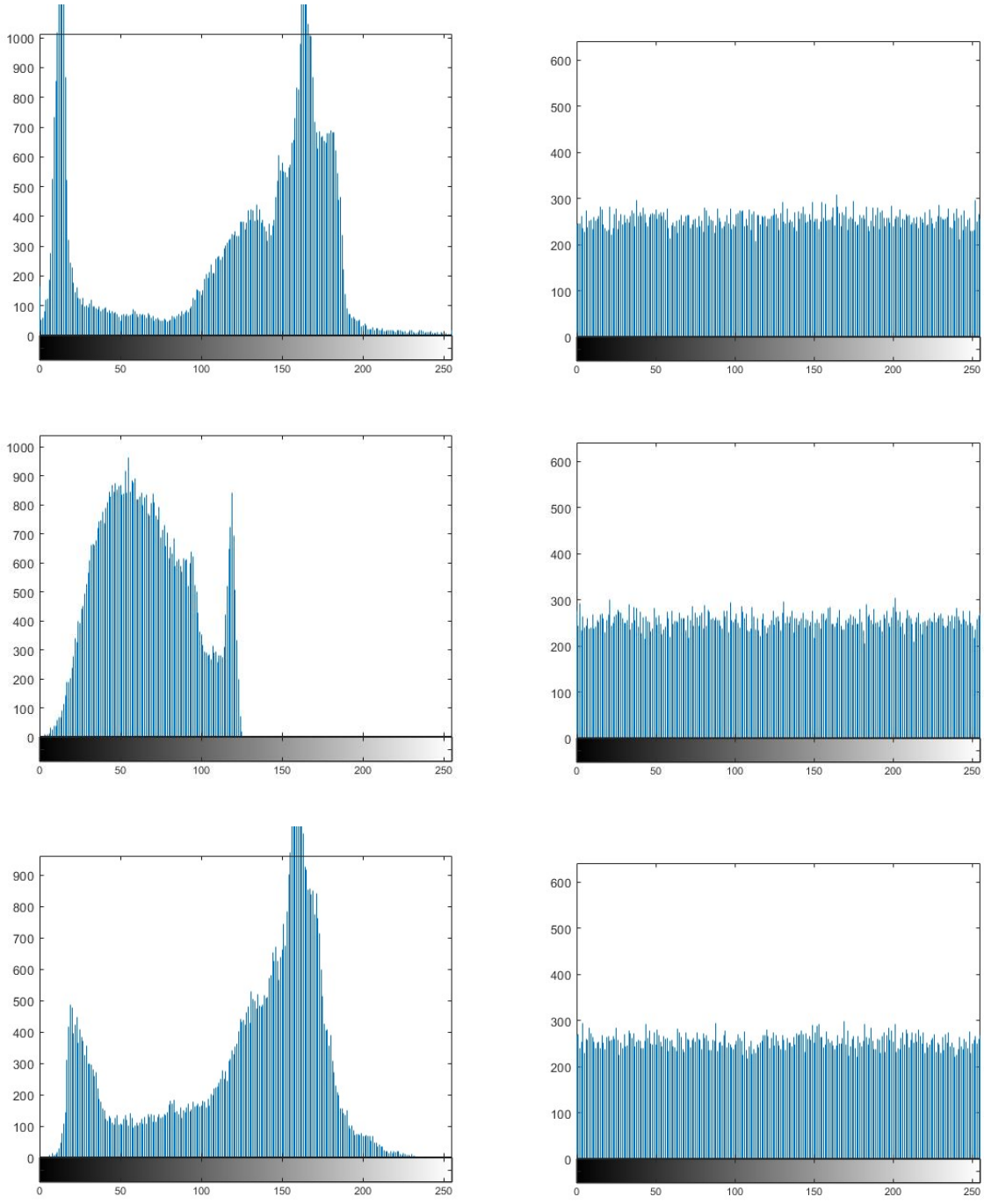
Tables 4.5 and 4.6. Furthermore, more regularity in encrypted images is indicated by a smaller variance value.

Table 4.5: The Test Results of χ^2

Images	**Cameraman**	**Lena**	**Boat**
Plain image	98781.4531	29629.5625	80889.4531
Encrypted image	278.2500	258.1719	261.9531
Result	Pass	Pass	Pass

4.7.4 Correlation Analysis

The secure connection between neighboring pixels in the plaintext image may be broken during encryption. The correlation value, which can partially represent the algorithm's effect on



(a) Plain Image (b) Encrypted Image

Figure 4.12: Histogram Analysis Diagram. (a) Plain Image of the Cameraman, Mandrill and Boat. (b) Encrypted Image of Cameraman, Mandrill and Boat.

Table 4.6: The Test Results of Variance

Images	**Cameraman**	**Lena**	**Boat**
Plain image	3886.9203	2733.9034	2564.3114
Encrypted image	5424.4849	5421.7051	5454.4359

encryption, can be determined using Equation (4.8).

$$\begin{cases} E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i, \qquad D(x) = \frac{1}{n}\sum_{i=1}^{n}(x_i - E(x))^2 \\ \text{corr}(x,y) = \frac{E\left((x-E(x))(y-E(y))\right)}{\sqrt{D(x)}\sqrt{D(y)}} \end{cases} \tag{4.8}$$

Let N represent the total number of pixels selected from the image. The variables $E(x)$ and $E(y)$ denote the mean values of the grey level values x_i and y_i for two neighboring pixels in the image, where x and y indicate the grey level values of those pixels.

The study compares 3000 pairs of neighboring pixels from original images with encrypted equivalents using a proposed method. Results in Table 4.7 shows no association between pixels, with correlation coefficients near one for original images and around zero for encrypted images. The same findings are observed for the cameraman, Mandrill, and boat images in Figures 4.13, 4.14, 4.15

4.7.5 Information Entropy

Information entropy (IE) [142] is a mathematical method for analyzing randomness in image pixel conflict. A desirable ciphertext image with 256 greyscales should have an entropy of 8, making it resistant to cyberattacks [143]. H(x) is computed as follows:

$$H(x) = \sum_{i=0}^{2^N-1} p(x_i)\log_2\left(\frac{1}{p(x_i)}\right) \tag{4.9}$$

When x is the information source, $p(x_i)$ is the probability, and N is the total number of bits required to encode the symbol x_i. The entropy of a real probabilistic source with 2^N tone values is N.

Table 4.8 presents the entropy values for the CML-based IE method, which indicates that ciphertext images are almost random, given a close-to-maximum value of 8, suggesting the cryptosystem's ability to withstand statistical attacks.

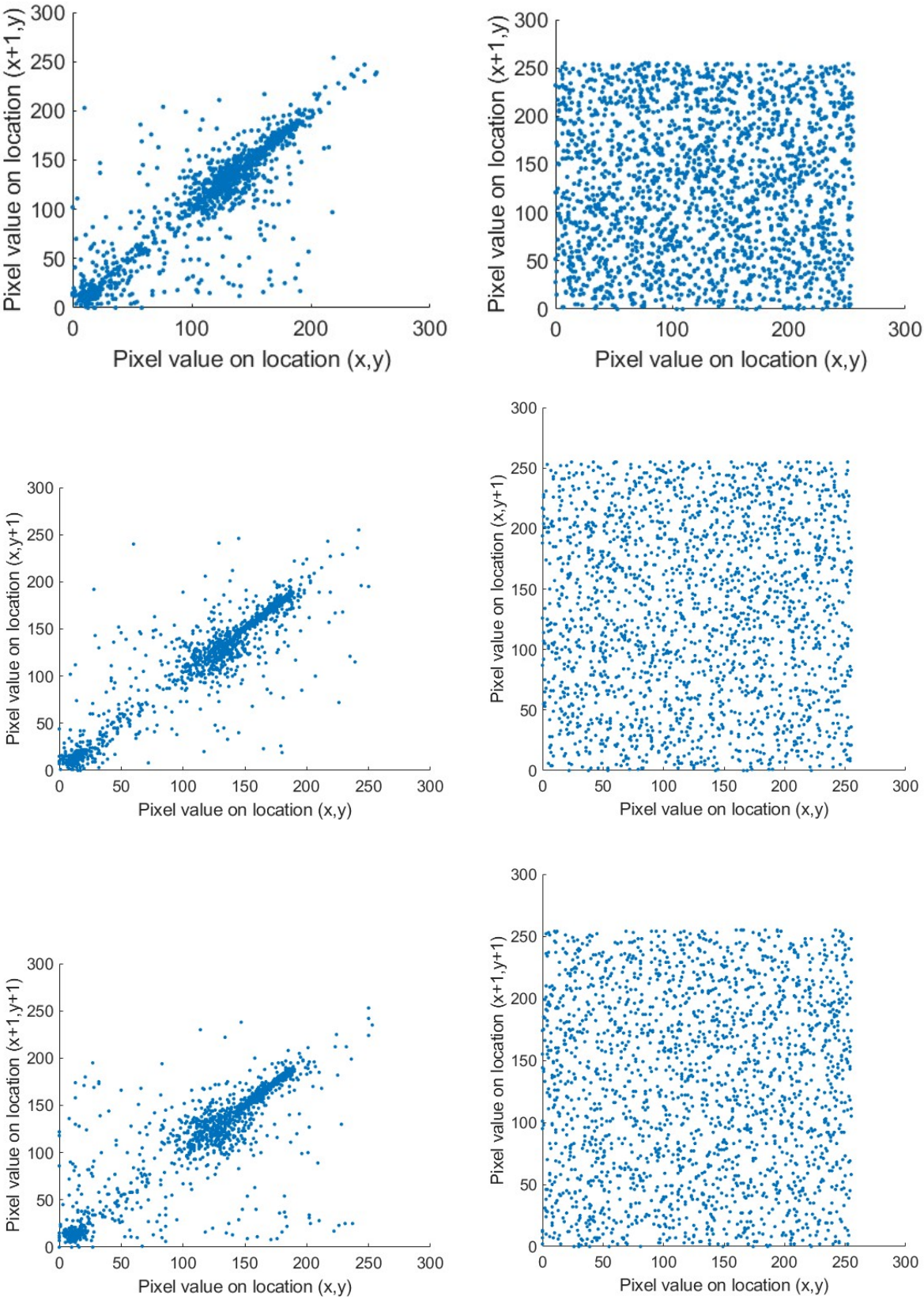


Figure 4.13: Scatter Plot of Correlations Between Neighbouring Pixels Pointing in Various Directions of Cameraman Image

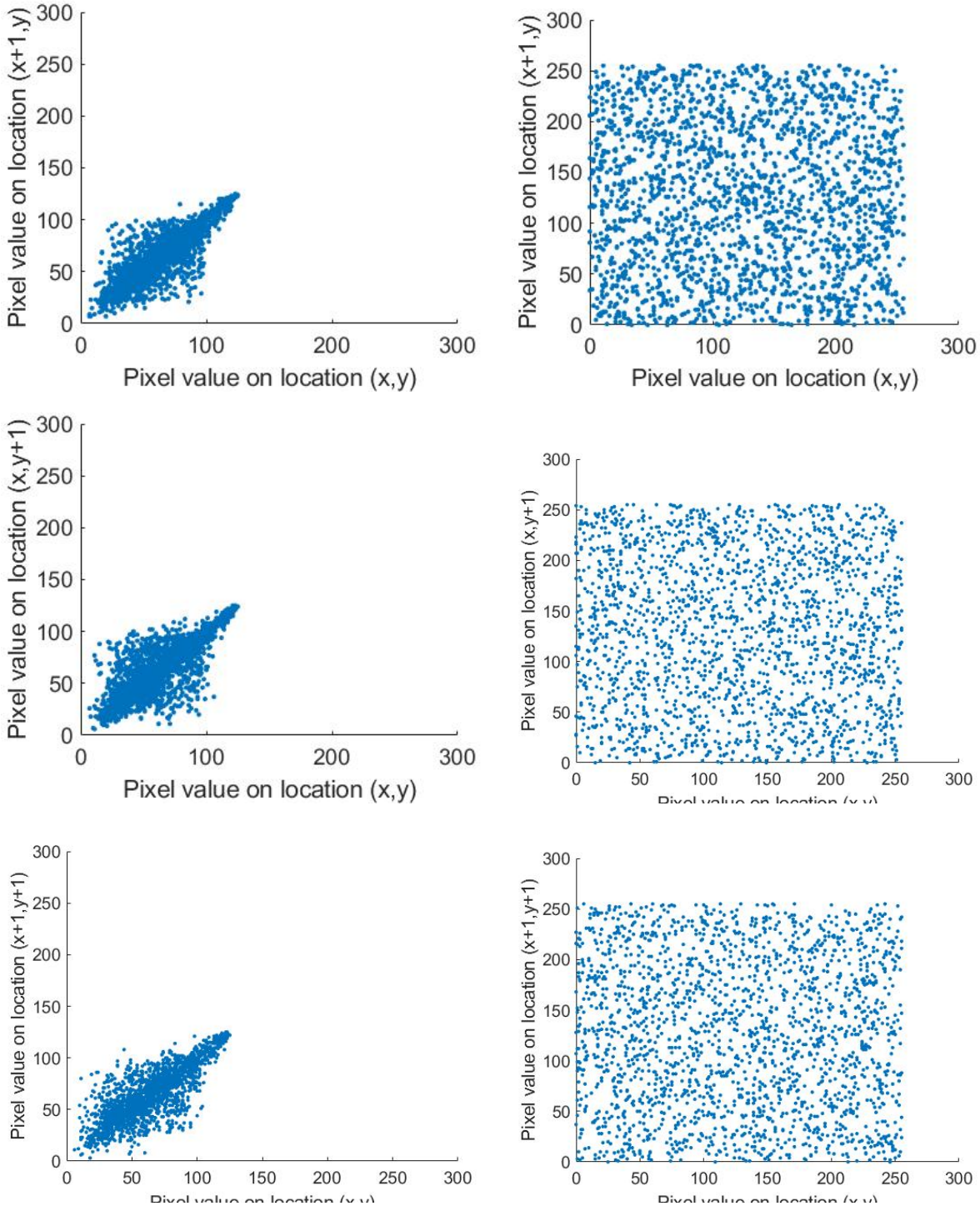


Figure 4.14: Scatter Plot of Correlations Between Neighbouring Pixels Pointing in Various Directions of Mandrill Image

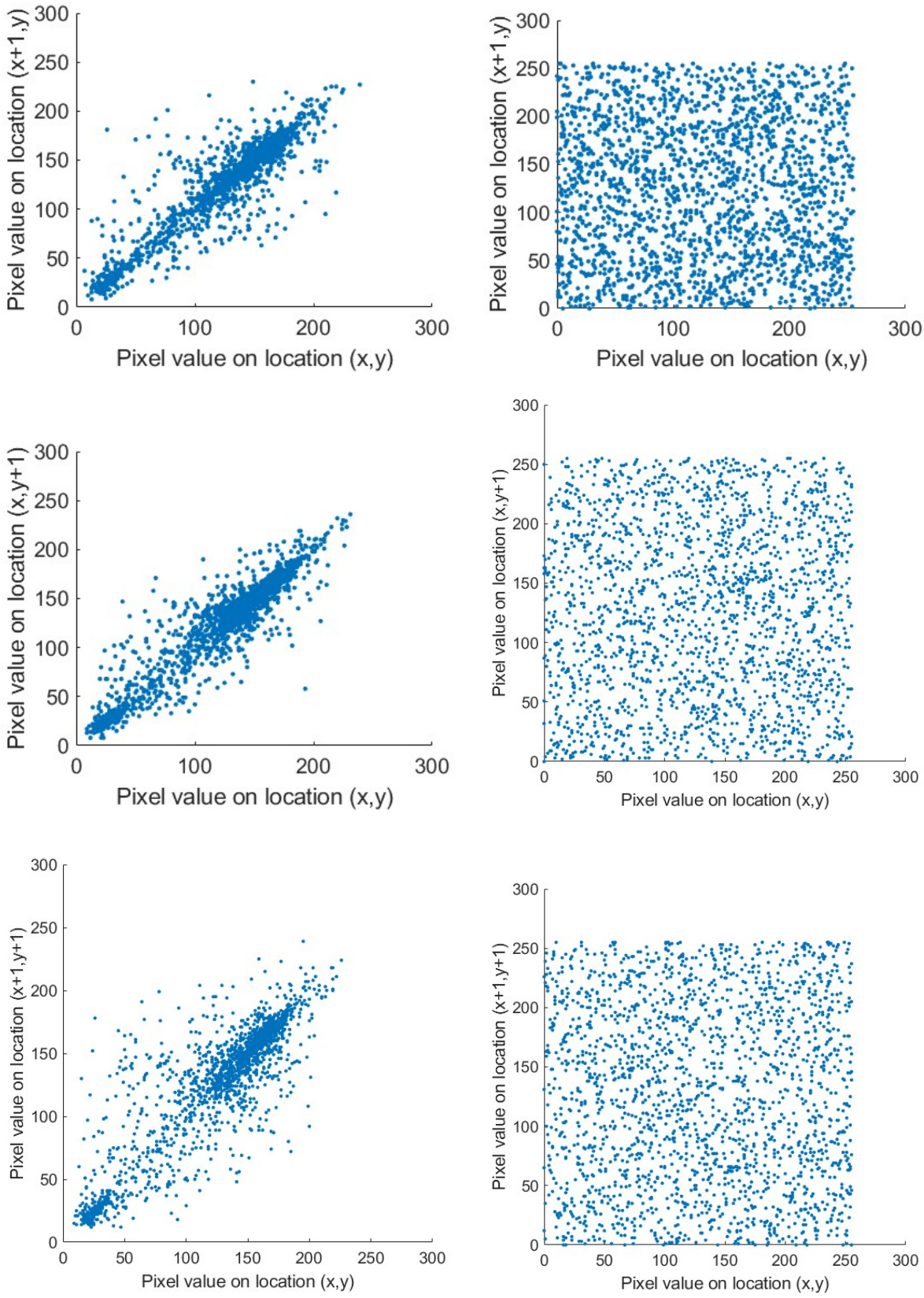


Figure 4.15: Scatter Plot of Correlations Between Neighboring Pixels Pointing in Various Directions of Boat Image

Table 4.7: Correlation Coefficients

Direction	Images	Horizontal	Vertical	Diagonal
Original Image	Cameraman	0.97309	0.96133	0.93481
	Lena	0.96896	0.93654	0.91390
	Boat	0.94761	0.93374	0.88732
Encrypted Image	Cameraman	0.0001	0.002	-0.0015
	Lena	-8.6008e-05	0.0035	0.0015
	Boat	-0.0013	0.0024	-0.0020
Existing map [132]	Cameraman	0.00116	0.00514	-0.00872
	Lena	-0.00199	-0.00189	0.00616
	Boat	0.00162	-0.00063	-0.00055
Ref.[136]	Lena	-0.0084	-0.0018	0.0002
	Boat	-0.00067	-0.03736	-0.00075
	Cameraman	0.00466	0.00868	-0.0084
Ref.[141]	Lena	0.0013	-0.0009	0.0012
	Cameraman	0.0020	0.0081	0.0073

4.7.6 Differential Attack Analysis

Selective attacks, known as differential attacks, occur when a cryptoanalyst examines modifications to an encrypted image, negating the need for the secret key to recover the original image. High NPCR and UACI scores show better resistance to specific attacks [144]. Equations (4.10) and (4.11) are used to get the NPCR and UACI scores for two encrypted images, E1 and E2, which differ from the source images by one pixel, respectively.

$$\text{NPCR} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \tag{4.10}$$

$$\text{UACI} = \frac{1}{255 \times MN}\sum_{i=1}^{M}\sum_{j=1}^{N} |E_1(i,j) - E_2(i,j)| \tag{4.11}$$

The NPCR and UACI findings, 0.996094 and 0.334635, are the optimal values, respectively. Table 4.9 shows that every test result is relatively close to the optimal values. Therefore, the suggested encryption image approach can withstand differential attacks successfully.

Table 4.8: Information Entropy Values for All Test Results

Algorithms	**Images**	**Information Entropy**
Our Algorithm	Cameraman	7.9975
	Mandrill	7.9968
	Lena	7.9975
	Boat	7.9973
Existing map [132]	Cameraman	7.9957
	Lena	7.9982
	Boat	7.9938
Ref.[141]	Lena	7.9974
	Cameraman	7.9967
Ref.[134]	Lena	7.9970

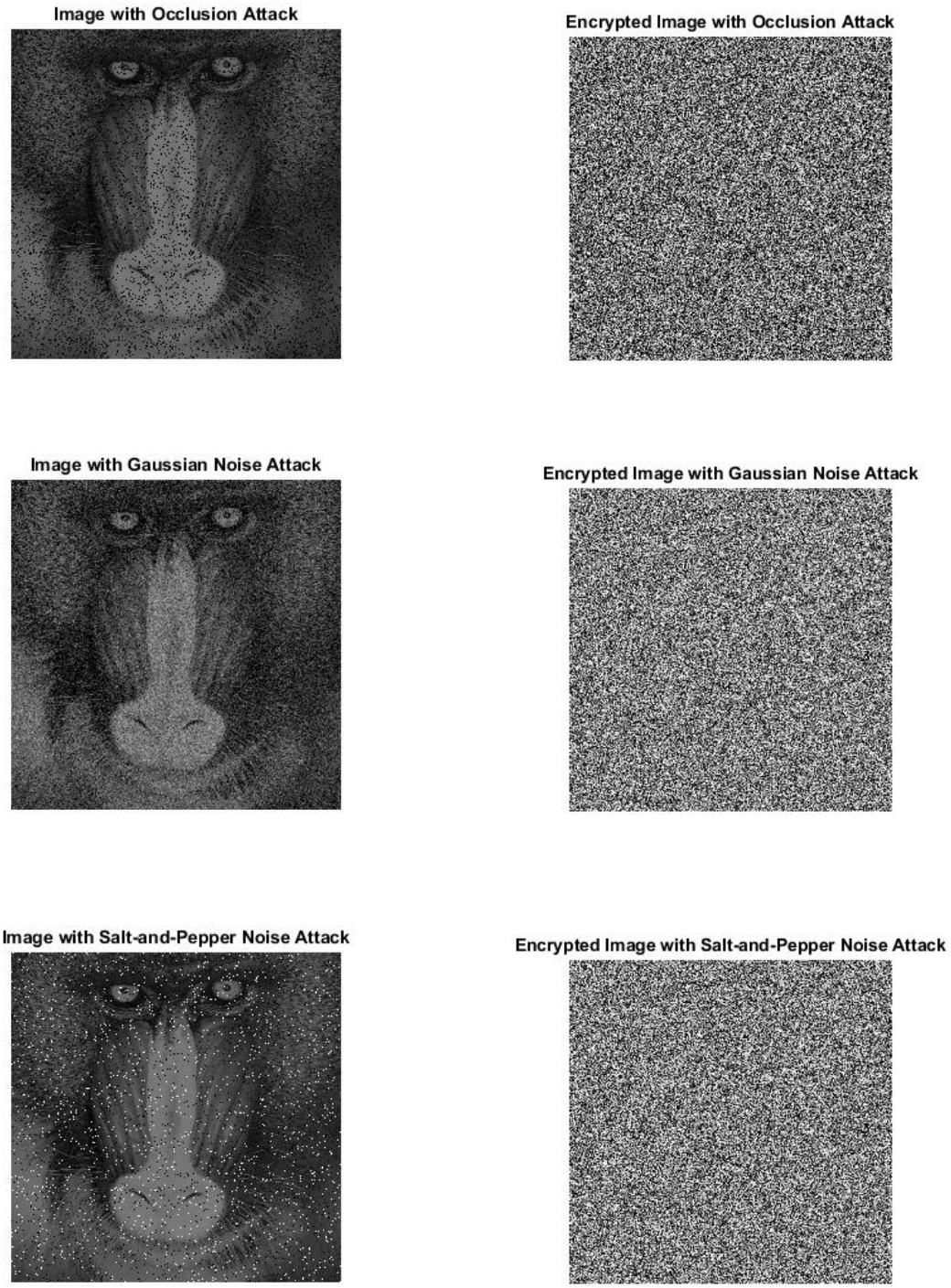
4.7.7 Analysis of Robustness

Image encryption techniques undergo robustness tests to assess their resilience against attacks, with the first test involving random blacking out 10% of image pixels to simulate partial data loss. The second test simulates real-world transmission noise distortions by subjecting encrypted images to Gaussian noise with a standard deviation of 25. The algorithm's resilience to random impulsive noise is evaluated in the third test, which adds salt-and-pepper noise with a density of 5%. The final test provides an optional cropping attack that eliminates 20% of encrypted image content, providing a framework for investigating encryption when significant data loss occurs. These tests comprehensively evaluate the encryption algorithm's resistance to data loss, occlusion, and noise. The results show that the encrypted image is still identifiable despite these disturbances, as shown in Figures 4.16,4.17, and 4.18. It suggests that the encryption technique is reliable and resilient in real-world situations.

The impacts of occlusion, salt and pepper, and Gaussian noise are quantitatively compared in terms of mean PSNR and RMSE between the original and decrypted images in Table 4.10.

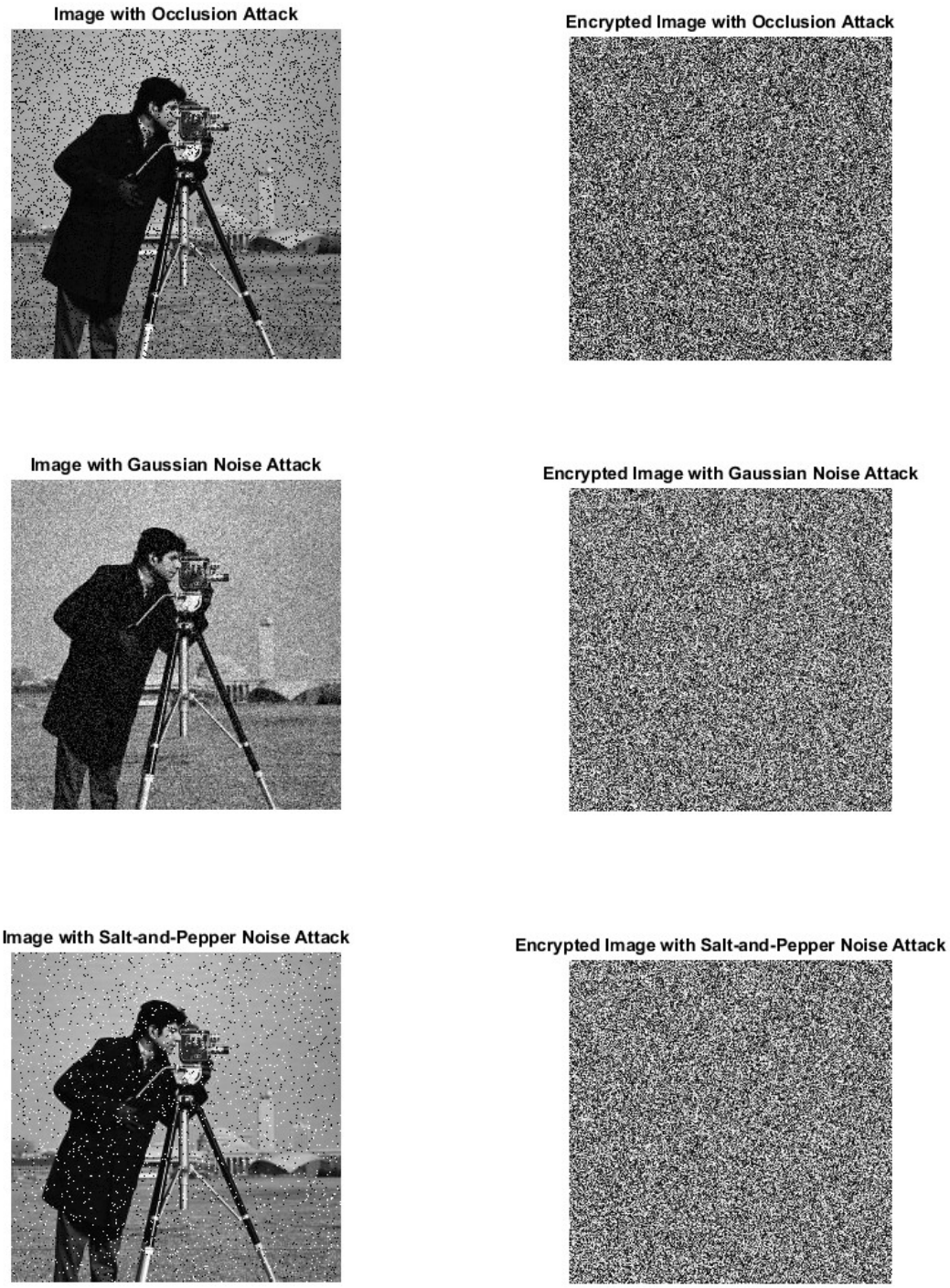
4.7.8 Time Analysis

The study focuses on optimizing encryption algorithms for computational efficiency and security. The Intel Core i5-5200u CPU was used with MATLAB R2023a and Windows 10 Pro with 8.00 GB of RAM. Experiments were conducted on 256×256 images, with an encryption



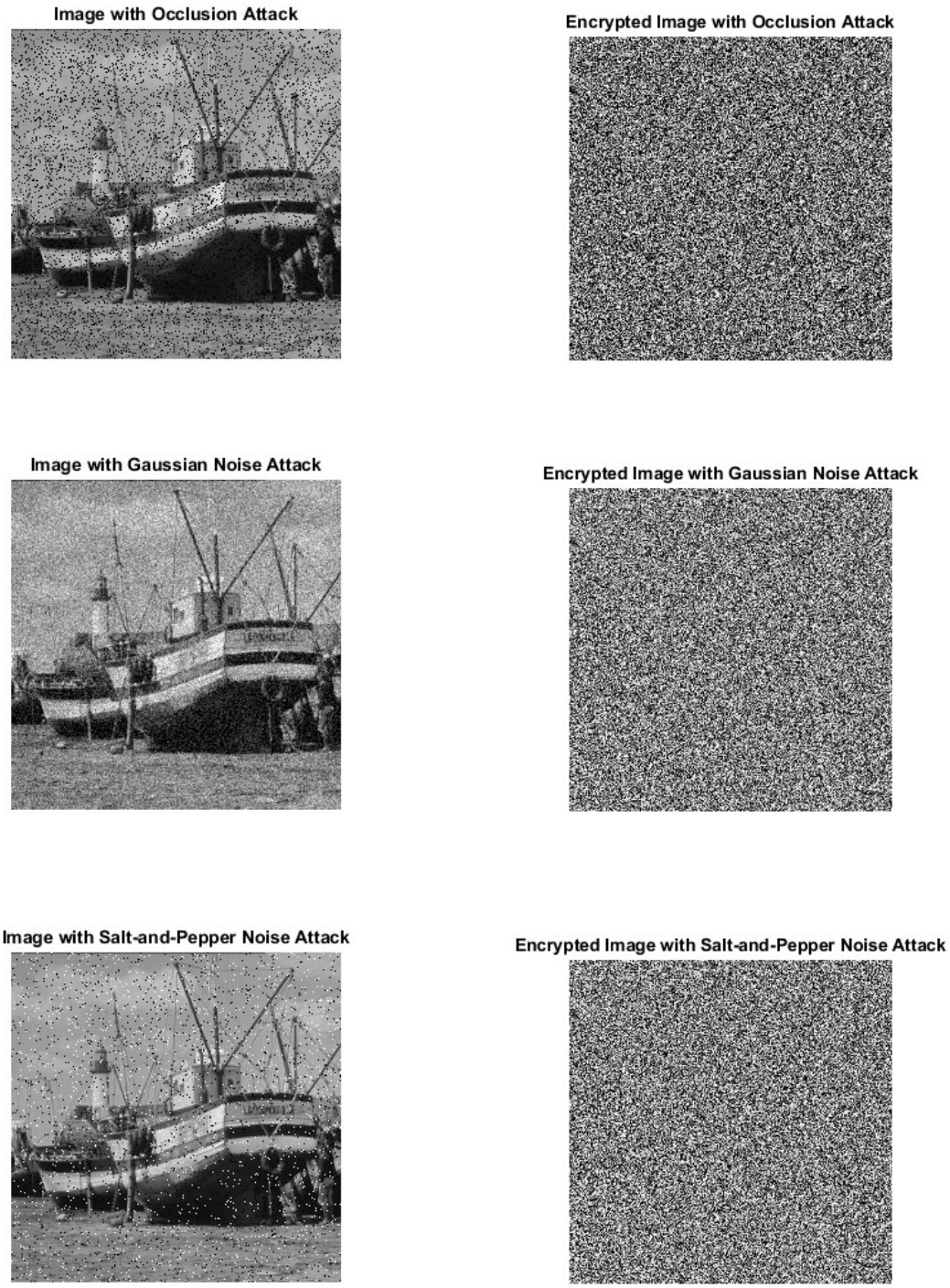
(a) Plain Image (b) Encrypted Image

Figure 4.16: Robustness Analysis of *Mandrill*: (a) Plain image with occlusion attack (10% pixels blacked out), Gaussian noise attack (standard deviation = 25), and salt-and-pepper noise attack (5% noise density); (b) Encrypted image with occlusion attack (10%), Gaussian noise attack ($\sigma = 25$), and salt-and-pepper noise attack (5%).



(a) Plain Image (b) Encrypted Image

Figure 4.17: Robustness Analysis of *Cameraman*: (a) Plain image with occlusion attack (10% pixels blacked out), Gaussian noise attack (standard deviation = 25), and salt-and-pepper noise attack (5% noise density); (b) Encrypted image with occlusion attack (10%), Gaussian noise attack ($\sigma = 25$), and salt-and-pepper noise attack (5%).



(a) Plain Image (b) Encrypted Image

Figure 4.18: Robustness Analysis of *Boat*: (a) Plain image with occlusion attack (10% pixels blacked out), Gaussian noise attack (standard deviation = 25), and salt-and-pepper noise attack (5% noise density); (b) Encrypted image with occlusion attack (10%), Gaussian noise attack ($\sigma = 25$), and salt-and-pepper noise attack (5%).

Table 4.9: NPCR and UACI Average Values for All Test Results

Algorithms	**Images**	**NPCR**	**UACI**
Our Algorithm	Lena	0.9962	0.3343
	Boat	0.9963	0.3341
	Cameraman	0.9962	0.3338
	Mandrill	0.9963	0.3360
Existing map [132]	Lena	0.9959	0.3324
	Boat	0.9961	0.3322
	Cameraman	0.9961	0.3332
Ref.[141]	Lena	0.9955	0.3336
	Cameraman	0.9964	0.3341
Ref.[138]	Lena	0.9960	0.3346
Ref.[135]	Lena	0.9960	0.3342
Ref.[136]	Lena	0.9964	0.3355
	Boat	0.9962	0.3360
	Cameraman	0.9960	0.3357

time of 0.465 seconds. Comparative techniques were compared, and the method showed minimal time spent on encryption, as shown in Table 4.11.

4.8 Results Discussion

In this section, our proposed image cryptosystems are compared with other works in recent years. The comparative analysis of encryption performance for the Cameraman image 256×256 demonstrates that our proposed image cryptosystem exhibits better security. Table 4.12 presents the test results of some recent papers, including the entropy values of [132] and [141], which are smaller than our work. Our approach is further validated by the differential attack resistance measures, which provide outstanding NPCR (99.62%) and UACI (33.38%) scores that satisfy security requirements. On the other hand, existing methods have significant drawbacks. Whereas [132] exhibits somewhat lower entropy (7.9957) and weaker correlation performance, [141] reveals alarming correlation values (up to 0.0081 vertically) that might compromise security even though its NPCR/UACI scores are comparable.

Table 4.10: RMSE and PSNR Values of Robustness Test

Image	**RMSE**	**PSNR**
Cameraman Occluded Image	71.9231	10.99 dB
Cameraman Noisy Image (Gaussian Noise)	62.3461	12.23 dB
Cameraman Noisy Image (Salt-and-Pepper Noise)	63.2218	12.11 dB
Lena Occluded Image	70.6550	11.15 dB
Lena Noisy Image (Gaussian Noise)	61.0618	12.42 dB
Lena Noisy Image (Salt-and-Pepper Noise)	61.9886	12.28 dB
Boat Occluded Image	72.4752	10.93 dB
Boat Noisy Image (Gaussian Noise)	62.3468	12.23 dB
Boat Noisy Image (Salt-and-Pepper Noise)	63.5828	12.06 dB

Table 4.11: The Encryption Time Analysis Results and Comparison with Related Algorithms

Algorithms	**Image size**	**Encryption time**
Proposed work	256×256	0.465 s
Existing map [132]	256×256	0.6933 s
Ref.[145]	256×256	0.4781 s
Ref.[146]	256×256	0.668939 s
Ref.[147]	256×256	0.44 s

Table 4.12: Comparison of Cameraman Encryption Performance

Image	**Correlation Coefficients**			**Entropy**	**Differential Attack**	
	Horizontal	Vertical	Diagonal		NPCR	UACI
Our work	0.0001	0.002	-0.0015	7.9975	0.9962	0.3338
Existing map [132]	0.00116	0.00514	-0.00872	7.9957	0.9961	0.3332
Ref.[141]	0.0020	0.0081	0.0073	7.9967	0.9964	0.3341

CHAPTER 5

CONCLUSION AND FUTURE WORK

This chapter compiles the research and offers suggestions for further study. The study evaluates the performance of a proposed encryption technique using the CMLs model and its influence on the effectiveness of image encryption. It also addresses the limitations and identifies possible directions for further research.

5.1 Conclusion

In this study, an effective image encryption method based on coupled map lattices (CMLs) has been introduced. The suggested technique improves security by using the randomness or predictability of chaotic systems. Using a secret key, encryption starts by determining the initial conditions and control parameters of the CMLs system. This method makes the encryption process extremely reliant on the input image. It makes it resilient to known-plaintext and chosen-plaintext attacks by ensuring that the encryption parameters are dynamically tied to the particular content of the plaintext image.

After the parameters have been defined, the original image is encoded and permuted (scrambled) to remove visual patterns by rearranging the spatial connections between neighboring pixels. The final cypher image is then created by diffusing the jumbled image using modular arithmetic operations and the resulting chaotic CMLs sequence, effectively modifying the pixel intensity values. A secure cryptographic system requires a high degree of confusion and diffusion, which is ensured by this two-stage process of permutation and diffusion.

Even when the same key is used, each encryption is distinct due to the encryption process's reliance on the plaintext image, significantly enhancing resistance to cryptanalytic attacks. The suggested approach works very well, according to a security study that includes statistical tests

like histogram uniformity, correlation analysis, entropy measurement, and differential attack resistance (NPCR and UACI). The encryption technique is appropriate for real-world uses in secure image transmission and storage as it maintains computational economy and provides high security. Considering all factors, the suggested CMLs-based image encryption technique provides a very reliable, secure, and computationally effective approach to contemporary image security requirements.

5.2 Future Work

Future research will focus on several avenues to improve the usefulness and resilience of the encryption scheme. Real-time applications can be made possible if the technique is optimized for speed and computation efficiency using hardware implementations like GPUs or FPGAs. When the technique is extended to handle color images or higher-dimensional data formats, the method might become more versatile in various domains, including surveillance and telemedicine. Hybrid cryptographic techniques, such as post-quantum encryption or DNA computing, improve the system's security and enable safe key sharing. Another possible approach is to use error-tolerant decryption or error correction coding to increase resilience against extreme noise and data corruption. Additionally, the algorithm's resistance to known attacks would be theoretically supported by establishing formal security proofs or using model-based verification tools. Lastly, adding capabilities like digital watermarking and user identification might expand the encryption scheme's scope for secure image transmission and copyright defence.

BIBLIOGRAPHY

[1] S. Singh, *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor Books, 2000.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*. Prentice Hall, 3rd ed., 2003.

[3] D. Gollmann, "E-commerce security," *Computing and Control Engineering*, vol. 11, no. 3, pp. 115–118, 2000.

[4] C.-H. Yuen and K.-W. Wong, "A chaos-based joint image compression and encryption scheme using dct and sha-1," *Applied Soft Computing*, vol. 11, no. 8, pp. 5092–5098, 2011.

[5] J.-S. Coron, "What is cryptography?," *IEEE security & privacy*, vol. 4, no. 1, pp. 70–73, 2006.

[6] M. N. Aslam, A. Belazi, S. Kharbech, M. Talha, and W. Xiang, "Fourth order mca and chaos-based image encryption scheme," *IEEE Access*, vol. 7, pp. 66395–66409, 2019.

[7] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.

[8] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," *Journal of Electrical and Computer Engineering*, vol. 2012, p. 15, 2012.

[9] M. Kalra, S. Katyal, and R. Singh, "A tent map and logistic map based approach for chaos-based image encryption and decryption," in *Innovations in Computer Science and Engineering: Proceedings of the Sixth ICICSE 2018*, pp. 159–165, Springer Singapore, 2019.

[10] D. Stiawan, M. Y. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating brute force attack patterns in IoT network," *Journal of Electrical and Computer Engineering*, vol. 2019, no. 1, p. 4568368, 2019. Article ID 4568368.

[11] G. Tang, X. Liao, and Y. Chen, "A novel method for designing s-boxes based on chaotic maps," *Chaos, Solitons & Fractals*, vol. 23, no. 2, pp. 413–419, 2005.

[12] N. A. Azam, G. Murtaza, and U. Hayat, "A novel image encryption scheme based on elliptic curves and coupled map lattices," *Optik*, vol. 274, p. 170517, 2023.

[13] K. Kaneko, "Spatiotemporal chaos in one-and two-dimensional coupled map lattices," *Physica D: Nonlinear Phenomena*, vol. 37, no. 1-3, pp. 60–82, 1989.

[14] E. Candès, J. Romberg, and T. Tao, "Robust uncertainty principles: Exact signal reconstruction from highly incomplete frequency information," *IEEE Transactions on Information Theory*, vol. 52, pp. 489–509, 2006.

[15] M. Wang, X. Wang, C. Wang, Z. Xia, and S. Zhou, "Novel image compression-then-encryption scheme based on 2d cross coupled map lattice and compressive sensing," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 1891–1917, 2024.

[16] Q. Zhang, Y. Yan, Y. Lin, and Y. Li, "Image security retrieval based on chaotic algorithm and deep learning," *IEEE Access*, vol. 10, pp. 67210–67218, 2022.

[17] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata," *Neural Computing and Applications*, vol. 32, pp. 4961–4988, 2020.

[18] M. S. Fadhil, S. R. Taha, and A. H. Abbas, "Designing substitution box based on the 1d logistic map chaotic," in *International Scientific Conference of Engineering Sciences (ISCES 2020)*, (Baghdad, Iraq), 2020.

[19] H. Demirci and N. Yurtay, "Effect of the chaotic crossover operator on breeding swarms algorithm," *Sakarya University Journal of Computer and Information Sciences*, vol. 4, pp. 120–130, April 2021.

[20] T. Alshekl and E. Albhrany, "A new key stream generator based on 3d hénon map and 3d cat map," *IJSER*, vol. 8, pp. 2114–2120, January 2017.

[21] M. S. Azzaz, C. Tanougast, S. Sadoudi, and A. Bouridane, "Synchronized hybrid chaotic generators: Application to real-time wireless speech encryption," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 2035–2047, August 2013.

[22] A. Hasheminejad and M. J. Rostami, "A novel bit level multiphase algorithm for image encryption based on pwlcm chaotic map," *Optik*, vol. 184, pp. 205–213, May 2019.

[23] A. Alfalou, C. Brosseau, and N. Abdallah, "Simultaneous compression and encryption of color video images," *Optics Communications*, vol. 338, pp. 371–379, March 2015.

[24] H. Elkamchouchi, W. M. Salama, and Y. Abouelseoud, "New video encryption schemes based on chaotic maps," *IET Image Processing*, vol. 14, pp. 397–406, February 2020.

[25] F. Sbiaa, S. Kotel, M. Zeghid, R. Tourki, M. Machhout, and A. Baganne, "A selective encryption scheme with multiple security levels for the h.264/avc video coding standard," in *2016 IEEE International Conference on Computer and Information Technology (CIT)*, pp. 391–398, 2016.

[26] P. McLaren, W. J. Buchanan, G. Russell, and Z. Tan, "Deriving chacha20 key streams from targeted memory analysis," *Journal of Information Security and Applications*, vol. 48, October 2019.

[27] A. M. Raheema, S. B. Sadkhan, and S. M. A. Sattar, "Performance comparison of hybrid chaotic maps based on speech scrambling for ofdm techniques," in *2018 Third Scientific Conference of Electrical Engineering (SCEE)*, 2018.

[28] H. A. Ismael and S. B. Sadkhan, "Security enhancement of speech scrambling using triple chaotic maps," in *2017 Annual Conference on New Trends in Information & Communications Technology Applications (NTICT)*, 2017.

[29] F. Özkaynak, "Cryptographically secure random number generator with chaotic additional input," *Nonlinear Dynamics*, 2014.

[30] V. D. Tô, "A note on devaney's definition of chaos," *Journal of Dynamical Systems and Geometric Theories*, vol. 2, no. 1, pp. 23–26, 2004.

[31] J. Scharinger, "Fast encryption of image data using chaotic kolmogorov flows," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 318–325, 1998.

[32] V. Patidar, N. K. Pareek, and K. K. Sud, "A new substitution–diffusion based image cipher using chaotic standard and logistic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 7, pp. 3056–3075, 2009.

[33] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Optics and Lasers in Engineering*, vol. 66, pp. 10–18, 2015.

[34] S. Liu, J. Sun, and Z. Xu, "An improved image encryption algorithm based on chaotic system," *Journal of Computers*, vol. 4, no. 12, pp. 1091–1100, 2009.

[35] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *Chaos, Solitons & Fractals*, vol. 42, no. 3, pp. 1745–1754, 2009.

[36] J. Y.-H. Ng, F. Yang, and L. Davis, "Exploiting local features from deep networks for image retrieval," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, (Boston, MA, USA), pp. 53–61, 2015.

[37] Z. Li, S. Yang, W. Tan, Z. Huang, and J. Wang, "A novel dynamic compressed sensing method for image encryption based on a new coupled map lattices model," *Nonlinear Dynamics*, pp. 1–25, 2024.

[38] Y. Dong, G. Zhao, Y. Ma, Z. Pan, and R. Wu, "A novel image encryption scheme based on pseudo-random coupled map lattices with hybrid elementary cellular automata," *Information Sciences*, vol. 593, pp. 121–154, 2022.

[39] S. Fan, K. Chen, and J. Tian, "A novel image encryption algorithm based on coupled map lattices model," *Multimedia Tools and Applications*, vol. 83, no. 4, pp. 11557–11572, 2024.

[40] I. Waller and R. Kapral, "Spatial and temporal structure in systems of coupled nonlinear oscillators," *Physical Review A*, vol. 30, no. 4, p. 2047, 1984.

[41] S. Kuznetsov and A. Pikovskii, "Universality of period-doubling bifurcations in one-dimensional dissipative media," *Radiofizika*, vol. 28, no. 3, pp. 308–319, 1985.

[42] G. Gong and A. M. Youssef, "Cryptographic properties of the welch-gong transformation sequence generators," *IEEE Transactions on Information Theory*, vol. 48, no. 11, pp. 2837–2846, 2002.

[43] A. Belazi, M. Khan, A. A. A. El-Latif, and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dynamics*, vol. 87, pp. 337–361, 2017.

[44] J. Xu and X. F. Wang, "Cascading failures in scale-free coupled map lattices," in *Proceedings of the 2005 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2005.

[45] Y.-Q. Zhang, Y. He, and X.-Y. Wang, "Spatiotemporal chaos in mixed linear–nonlinear two-dimensional coupled logistic map lattice," *Physica A: Statistical Mechanics and its Applications*, vol. 490, pp. 148–160, 2018.

[46] A. Gordo, J. Almazán, J. Revaud, and D. Larlus, "Deep image retrieval: Learning global representations for image search," in *Computer Vision – ECCV 2016: 14th European Conference*, (Amsterdam, The Netherlands), pp. 241–257, 2016.

[47] G. Chen, *Controlling Chaos and Bifurcations in Engineering Systems*. Boca Raton, FL, USA: CRC Press, 1999.

[48] S. Naveenkumar and H. Panduranga, "Chaos and hill cipher based image encryption for mammography images," in *Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, (Coimbatore, India), pp. 1–5, March 2015.

[49] S. Mostafa, M. Fahim, and A. Hossain, "A new chaos based medical image encryption scheme," in *2017 6th International Conference on Informatics, Electronics and Vision & 2017 7th International Symposium in Computational Medical and Health Technology (ICIEV-ISCMHT)*, (Himeji, Japan), pp. 1–6, September 2017.

[50] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and dna encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.

[51] S. Ibrahim, H. Alhumyani, M. Masud, S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. Hossain, and A. Abbas, "Framework for efficient medical image encryption using dynamic s-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433–160449, 2020.

[52] B. Vaseghi, S. Mobayen, S. Hashemi, and A. Fekih, "Fast reaching finite time synchronization approach for chaotic systems with application in medical image encryption," *IEEE Access*, vol. 9, pp. 25911–25925, 2021.

[53] A. Boutros, S. Hesham, and B. Georgey, "Hardware acceleration of novel chaos-based image encryption for iot applications," in *Proceedings of the 2017 29th International Conference on Microelectronics (ICM)*, (Beirut, Lebanon), pp. 1–4, December 2017.

[54] S. Nath, S. Som, and M. Negi, "Lca approach for image encryption based on chaos to secure multimedia data in iot," in *Proceedings of the 2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, (Mathura, India), pp. 410–416, November 2019.

[55] E. García-Guerrero, E. Inzunza-González, O. López-Bonilla, J. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using pic-microcontroller via zigbee channels," *Chaos, Solitons & Fractals*, vol. 133, p. 109646, 2020.

[56] M. Usama, M. Khan, K. Alghathbar, and C. Lee, "Chaos-based secure satellite imagery cryptosystem," *Computers & Mathematics with Applications*, vol. 60, pp. 326–337, 2010.

[57] Y. Bentoutou, E.-H. Bensikaddour, N. Taleb, and N. Bounoua, "An improved image encryption algorithm for satellite applications," *Advances in Space Research*, vol. 66, pp. 176–192, 2020.

[58] B. Vaseghi, S. Hashemi, S. Mobayen, and A. Fekih, "Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in ofdm communication systems," *IEEE Access*, vol. 9, pp. 21332–21344, 2021.

[59] W. Song, C. Fu, Y. Zheng, L. Cao, M. Tie, and C.-W. Sham, "Protection of image roi using chaos-based encryption and dcnn-based object detection," *Neural Computing and Applications*, vol. 34, pp. 5743–5756, 2022.

[60] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, pp. 394–400, 2008.

[61] M. Sobhy and A.-E. Shehata, "Methods of attacking chaotic encryption and countermeasures," in *Proceedings of the 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing*, (Salt Lake City, UT, USA), pp. 1001–1004, 2001.

[62] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, pp. 2129–2151, 2006.

[63] G. Alvarez, J. Amigó, D. Arroyo, and S. Li, "Lessons learnt from the cryptanalysis of chaos-based ciphers," in *Chaos-Based Cryptography: Theory, Algorithms and Applications*, vol. 42, pp. 257–295, 2011.

[64] R. Rhouma and S. Belghith, "Cryptanalysis of a new image encryption algorithm based on hyper-chaos," *Physics Letters A*, vol. 372, pp. 5973–5978, 2008.

[65] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 8, pp. 1259–1284, 1998.

[66] E. Solak, C. Cokal, O. Yildiz, and T. Biyikoğlu, "Cryptanalysis of fridrich's chaotic image encryption," *International Journal of Bifurcation and Chaos*, vol. 20, pp. 1405–1413, 2010.

[67] E. Xie, C. Li, S. Yu, and J. Lü, "On the cryptanalysis of fridrich's chaotic image encryption scheme," *Signal Processing*, vol. 132, pp. 150–154, 2017.

[68] X. Zhang *et al.*, "Analysis of s-box vulnerabilities in aes," *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 135–145, 2013.

[69] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.

[70] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, p. 1850010, 2018.

[71] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dynamics*, vol. 94, pp. 1319–1333, 2018.

[72] L. Liu, Z. Zhang, and R. Chen, "Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos," *IEEE Access*, vol. 7, pp. 126450–126463, 2019.

[73] Y. Zhou, Z. Hua, C.-M. Pun, and C. P. Chen, "Cascade chaotic system with applications," *IEEE Transactions on Cybernetics*, vol. 45, no. 9, pp. 2001–2012, 2014.

[74] Y. Zhang, R. Zhao, Y. Zhang, R. Lan, and X. Chai, "High-efficiency and visual-usability image encryption based on thumbnail preserving and chaotic system," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, pp. 2993–3010, 2022.

[75] S. Ansari, N. Gupta, and S. Agrawal, "A review on chaotic map based cryptography," *International Journal of Scientific Engineering and Technology*, 2012.

[76] N. S. Raghava and A. Kumar, "Image encryption using henon chaotic map with byte sequence," *International Journal of Computer Science Engineering and Information Technology Research (IJCSEITR)*, vol. 3, pp. 11–18, December 2013.

[77] A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using xor based on hénon map," 2016.

[78] E. A. Albahrani and T. K. Alshekly, "A new key stream generator based on 3d henon map and 3d cat map," *International Journal of Scientific and Engineering Research*, vol. 8, no. 1, p. 2114, 2017.

[79] P. Sankhe, S. Pimple, S. Singh, and A. Lahane, "An image cryptography using henon map and arnold cat map," *International Research Journal of Engineering and Technology (IRJET)*, vol. 5, April 2018.

[80] A. T. Khudhair and A. T. Maolood, "Towards generating a new strong key for aes encryption method depending on 2d hénon map," *Diyala Journal for Pure Science*, 2018.

[81] E. A. Albahrani, "A combination of two-dimensional hénon map and two-dimensional rational map as key number generator," in *2019 First International Conference of Computer and Applied Sciences (CAS)*, 2019.

[82] A. Sabah, S. Hameed, and M. A. A. K., "Key generation based on hénon map and lorenz system," *Al-Mustansiriyah Journal of Science*, vol. 31, no. 1, 2020.

[83] D. Murillo-Escobar, M. Ángel Murillo-Escobar, C. Cruz-Hernández, A. Arellano-Delgado, and R. M. López-Gutiérrez, "Pseudorandom number generator based on novel 2d hénon-sine hyperchaotic map with microcontroller implementation," *Springer Nature B.V.*, 2022.

[84] M. G. Abdelfattah, S. F. Hegazy, N. Fayez, and S. Obayya, "Optical cryptosystem for visually meaningful encrypted images based on gyrator transform and hénon map," *Optical and Quantum Electronics*, January 2022.

[85] A. T. Khudhair, E. K. Gbashi, and A. T. Maolood, "A novel dynamic s-box based on password key and circle map," *Iraqi Journal of Science (IJS)*, 2023.

[86] M. Bishop, "What is computer security?," *IEEE Security & Privacy*, vol. 99, no. 1, pp. 67–96, 2003.

[87] W. Stallings, *Cryptography and Network Security, 4/E*, vol. 4. Pearson Education India, 2006.

[88] M. S. Iqbal, S. Singh, and A. Jaiswal, "Symmetric key cryptography: Technological developments in the field," *International Journal of Computer Applications*, vol. 117, no. 15, pp. 1–4, 2015.

[89] J. Daemen and V. Rijmen, *The design of Rijndael: AES-the advanced encryption standard*, vol. 1. Springer Science & Business Media, 2013.

[90] J. Wang, L. Liu, M. Xu, and X. Li, "A novel content-selected image encryption algorithm based on the ls chaotic model," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, pp. 8245–8259, 2022.

[91] B. Schneier, "Description of a new variable-length key, 64-bit block cipher (blowfish)," in *International Workshop on Fast Software Encryption*, vol. 809, pp. 191–204, Springer, 1993.

[92] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[93] N. R. Wagner and M. R. Magyarik, "A public-key cryptosystem based on the word problem," in *Workshop on the Theory and Application of Cryptographic Techniques*, vol. 196, pp. 19–36, Springer, 1984.

[94] M. M. Rahman, T. K. Saha, and M. A.-A. Bhuiyan, "Implementation of rsa algorithm for speech data encryption and decryption," *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 12, no. 3, pp. 1–74, 2012.

[95] R. Singh and S. Kumar, "Elgamal's algorithm in cryptography," *International Journal of Scientific & Engineering Research*, vol. 3, no. 12, pp. 1–4, 2012.

[96] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*, vol. 1. Springer Science & Business Media, 2006.

[97] L. M. Kohnfelder, *Towards a practical public-key cryptosystem.* PhD thesis, Massachusetts Institute of Technology, 1978.

[98] C.-J. Cheng and C.-B. Cheng, "An asymmetric image cryptosystem based on the adaptive synchronization of an uncertain unified chaotic system and a cellular neural network," *Communications in Nonlinear Science and Numerical Simulation*, vol. 18, pp. 2825–2837, 2013.

[99] Y. Shan, M. He, Z. Yu, and H. Wu, "Pixel level image encryption based on semantic segmentation," in *Proceedings of the 2018 International Conference on Control, Artificial Intelligence, Robotics & Optimization (ICCAIRO)*, (Prague, Czech Republic), pp. 147–152, 2018.

[100] C.-H. Yang, C.-Y. Weng, and Y.-Z. Yang, "Tpeip: Thumbnail preserving encryption based on sum preserving for image privacy," *Journal of Information Security and Applications*, vol. 70, p. 103352, 2022.

[101] C. Wolf, *Hidden Field Equations"(HFE)-Variations and Attacks*. PhD thesis, Verlag nicht ermittelbar, 2002.

[102] T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Transactions on Computers*, vol. C-34, no. 1, pp. 81–85, 1985.

[103] R. Canetti, S. Halevi, and J. Katz, "A forward-secure public-key encryption scheme," *Journal of Cryptology*, vol. 20, no. 3, pp. 265–294, 2007.

[104] M. Matsui, "Linear cryptanalysis method for des cipher," in *Workshop on the Theory and Application of Cryptographic Techniques*, pp. 386–397, Springer, 1993.

[105] C. Rackoff and D. R. Simon, "Non-interactive zero-knowledge proof of knowledge and chosen ciphertext attack," in *Annual International Cryptology Conference*, pp. 433–444, Springer, 1991.

[106] T. Habutsu, Y. Nishio, I. Sasase, and S. Mori, "A secret key cryptosystem by iterating a chaotic map," in *Advances in Cryptology—EUROCRYPT'91*, (Brighton, UK), pp. 127–140, Springer Berlin Heidelberg, April 8–11 1991.

[107] J. M. T. Thompson and H. B. Stewart, *Nonlinear Dynamics and Chaos*. Chichester, UK: John Wiley and Sons, 1986.

[108] Y. Zhang, R. Zhao, X. Xiao, R. Lan, Z. Liu, and X. Zhang, "Hf-tpe: High-fidelity thumbnail-preserving encryption," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, pp. 947–961, 2021.

[109] P. Collet and J. P. Eckmann, *Iterated Maps on the Interval as Dynamical Systems*. Boston, USA: Birkhäuser, 1980.

[110] C. Wang and Q. Ding, "A class of quadratic polynomial chaotic maps and their fixed points analysis," *Entropy*, vol. 21, no. 7, p. 658, 2019.

[111] F. Radenović, G. Tolias, and O. Chum, "Fine-tuning cnn image retrieval with no human annotation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 41, pp. 1655–1668, 2018.

[112] V. Avrutin, L. Gardini, I. Sushko, and F. Tramontana, *Continuous and Discontinuous Piecewise-Smooth One-Dimensional Maps: Invariant Sets and Bifurcation Structures*. Singapore: World Scientific, 2019.

[113] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, 1976.

[114] T. Guo and Y. Lin, "Chaos-based image encryption using coupled logistic map lattice," *Optics Communications*, 2009.

[115] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, pp. 46–56, Oct./Dec. 2018.

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

[117] K. Kaneko, "Lyapunov analysis and information flow in coupled map lattices," *Physica D*, vol. 23, no. 1-3, pp. 436–447, 1986. Derives master stability function for synchronization.

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

[119] P. Collet and J.-P. Eckmann, *Iterated Maps on the Interval as Dynamical Systems*. Springer, 2009.

[120] J.-R. Chazottes, "Dynamics of coupled map lattices: From hyperbolicity to quasi-stationary states," *Journal of Statistical Physics*, vol. 149, no. 1, pp. 1–23, 2012. Spectral analysis of transfer operators.

[121] Y. Kuramoto, *Chemical Oscillations, Waves, and Turbulence*. Springer, 1984.

[122] S.-N. Chow and J. Hale, *Methods of Bifurcation Theory*, vol. 251. Berlin/Heidelberg, Germany: Springer Science & Business Media, 2012.

[123] A. Wolf, J. Swift, H. Swinney, and J. Vastano, "Determining lyapunov exponents from a time series," *Physica D: Nonlinear Phenomena*, vol. 16, pp. 285–317, 1985.

[124] J. Theiler, "Efficient algorithm for estimating the correlation dimension from a set of discrete points," *Physical Review A*, vol. 36, no. 9, pp. 4456–4462, 1987.

[125] A. N. Kolmogorov, "A new metric invariant of transient dynamical systems and automorphisms in lebesgue spaces," *Doklady Akademii Nauk*, vol. 119, no. 5, pp. 861–864, 1958.

[126] P. Grassberger and I. Procaccia, "Estimation of the kolmogorov entropy from a chaotic signal," *Physical Review A*, vol. 28, no. 4, p. 2591, 1983.

[127] S. Pincus, "Approximate entropy as a measure of system complexity," *Proceedings of the National Academy of Sciences of the United States of America*, vol. 88, pp. 2297–2301, 1991.

[128] A. Toktas, U. Erkan, and D. Ustun, "An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using abc algorithm," *Nonlinear Dynamics*, vol. 105, no. 2, pp. 1885–1909, 2021.

[129] X. Wang, S. Gu, and Y. Zhang, "Novel image encryption algorithm based on cycle shift and chaotic system," *Optics and Lasers in Engineering*, vol. 68, pp. 126–134, 2015.

[130] L. Liu, H. Xiang, and X. Li, "A novel perturbation method to reduce the dynamical degradation of digital chaotic maps," *Nonlinear Dynamics*, vol. 103, pp. 1099–1115, 2021.

[131] L. Lacasa and J. Gomez-Gardenes, "Correlation dimension of complex network," *Physical Review Letters*, vol. 110, no. 16, p. 168703, 2013.

[132] L. Liu, Z. Wei, and H. Xiang, "A novel image encryption algorithm based on compound-coupled logistic chaotic map," *Multimedia Tools and Applications*, vol. 81, pp. 19999–20019, 2022.

[133] H. Gao, Y. Zhang, S. Liang, *et al.*, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[134] M. Khan and T. Shah, "An efficient chaotic image encryption scheme," *Neural Computing and Applications*, vol. 26, no. 5, pp. 1137–1148, 2015.

[135] Y.-J. Xian, X.-Y. Wang, Y.-Q. Zhang, X.-Y. Wang, and D. Xiao-Hui, "Fractal sorting vector-based least significant bit chaotic permutation for image encryption," *Chinese Physics B*, vol. 30, no. 06, pp. 238–247, 2021.

[136] C. Madan Kumar, R. Vidhya, and M. Brindha, "An efficient chaos-based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function," *Applied Intelligence*, 2021. Prepublish.

[137] Z. Guan, F. Huang, and W. Guan, "Chaos-based image encryption algorithm," *Physics Letters A*, vol. 346, no. 1-3, pp. 153–157, 2005.

[138] Z. Xiaoqiang and Y. Xuangang, "Adaptive chaotic image encryption algorithm based on rna and pixel depth," *Electronics*, vol. 10, no. 15, 2021.

[139] X.-Y. Wang, H.-H. Sun, and H. Gao, "An image encryption algorithm based on improved baker transformation and chaotic s-box," *Chinese Physics B*, vol. 30, no. 06, pp. 221–230, 2021.

[140] X. Huang and X. Huang, "Image encryption algorithm using chaotic chebyshev generator," *Nonlinear Dynamics*, vol. 67, no. 4, pp. 2411–2417, 2012.

[141] X. Wang, Y. Hou, S. Wang, and R. Li, "A new image encryption algorithm based on cml and dna sequence," *IEEE Access*, vol. 6, pp. 62272–62285, 2018.

[142] 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.

[143] U. Erkan, A. Toktas, and Q. Lai, "2d hyperchaotic system based on schaffer function for image encryption," *Expert Systems with Applications*, vol. 213, p. 119076, 2023.

[144] N. Tsafack, J. Kengne, B. Abd-El-Atty, A. M. Iliyasu, K. Hirota, and A. A. Abd El-Latif, "Design and implementation of a simple dynamical 4-d chaotic circuit with applications in image encryption," *Information Sciences*, vol. 515, pp. 191–217, 2020.

[145] X. Y. Gao, J. Mou, S. Banerjee, Y. H. Cao, L. Xiong, and X. Y. Chen, "An effective multiple-image encryption algorithm based on 3d cube and hyperchaotic map," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1535–1551, 2022.

[146] X. Wang, N. Guan, H. Zhao, S. Wang, and Y. Zhang, "A new image encryption scheme based on coupling map lattices with mixed multi-chaos," *Scientific Reports*, vol. 10, p. 9784, Dec 2020.

[147] X. Chai, X. Zheng, Z. Gan, and Y. Chen, "Exploiting plaintext-related mechanism for secure color image encryption," *Neural Computing and Applications*, vol. 32, pp. 8065–8088, Jun 2020.