

SECURED CHAOTIC MAP TECHNIQUE FOR DIGITAL IMAGES

A Thesis submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN

COMPUTER SCIENCE AND ENGINEERING

By

SUPRIYA KHAITAN

19SCSE3010022

Supervisor

Dr. SHRDDHA SAGAR

Professor



SCHOOL OF COMPUTING SCIENCE & ENGINEERING

GALGOTIAS UNIVERSITY

Uttar Pradesh

December, 2022

CERTIFICATE

I hereby certify that the work which is being presented in the thesis, entitled “**Secured Chaotic Map Technique For Digital Images**” in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Faculty of Computer Science and Engineering and submitted in Galgotias University, Uttar Pradesh is an authentic record of my own work carried out during a period from January 2018 under the supervision of **Dr. SHRDDHA SAGAR**, Professor, School of Computing Science and Engineering, Galgotias University.

The matter embodied in this thesis has not been submitted by me for the award of any other degree or from any other University/Institute.

Ms. SUPRIYA KHAITAN

19SCSE3010022

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

Dr. SHRDDHA SAGAR

Supervisor

SCSE

School of Computing Science & Engineering

Galgotias University

The Ph.D. Viva-Voice examination of Supriya Khaitan, has been held on_____

Sign. of Supervisor(s)

Sign. of External Examiner

ABSTRACT

The onset of the pandemic made companies go digital; this led to massive data transfer hence the need for highly secure and fast data encryption techniques. Most real-time applications in mobile communication, military, and private organizations often require safe and reliable data monitoring and transfer. As one of the most crucial areas of information security, chaos-based image encryption has attracted academics and scientists over the past few years. Several studies with different approaches and new algorithms to make image encryption systems safer were proposed in recent studies. Traditional encryption techniques are challenging to understand, complex to implement, slow for encryption, and unsuitable for real-time and multimedia applications. Hence many researchers used chaos-based cryptography. Chaotic-based cryptosystems take full advantage of chaotic dynamics, diffusion, and confusion performances to achieve adequate security.

In diffusion, ciphertext and plaintext form a complex relationship, while confusion emphasizes how sensitive the ciphertext is to the plaintext. A small change in the plaintext will significantly impact the ciphertext. However, the main problem with most chaos-based algorithms is the inadequacy of the chaotic maps they implement. Hence, most researchers used more than one chaotic map or a higher dimensional chaotic map in the system. We seek to develop new, secure, reliable, Symmetric, and asymmetric cryptosystems based on chaos theory. We aim to incorporate chaotic dynamics into cryptography to create new asymmetric and symmetric algorithms using the lower dimensional chaotic map. The main work can be summarized as follows:

- i. We design and test a robust, efficient symmetric key stream cipher based on chaos theory. The key was generated using based on a 3-dimensional Logistic Map. The proposed techniques use a secure logistic map with XOR operators and shift operations to perform encryption. The tests we

conducted determined that the proposed scheme is cryptographically sound and meets the needs of different analyses.

- ii. The chaotic maps used in chaos-based cryptosystems in digital devices show dynamical degradation with finite precision. Considering that chaotic maps are based on real numbers, this has the disadvantage of high computation costs and inefficient resource use. Hence, we used both the real and imaginary parts of one superior logistic map for key generation. An image is scrambled and diffused by combining a chaotic sequence with a secret key entered by the user. The image is then evaluated using various measures such as NPCR, UACI, MSE, PSNR, and entropy.
- iii. Based on the chaotic Tent map, we propose a secure and robust system for the implementation of asymmetric key cryptosystems using chaos-based techniques. For the construction of public and private keys, a salp swarm optimization algorithm was used, along with a chaotic one dimensional tent map, . In order to ensure good cryptography, the key space must be large, so that brute-force attacks cannot be performed against it, the secret key must be highly sensitive, and pseudo-randomness should be employed in order to hide the correlation between the key, the plaintext, and the ciphertext. It has been demonstrated through security analyses and experiment results that the proposed chaos-based cryptosystem is complex and provide confusion and diffusion.

ACKNOWLEDGEMENT

Working as an Assistant Professor and doing research for the degree of Ph.D in Galgotias University was quite magnificent and challenging experience for me. In all these years, many people directly or indirectly contributed in shaping up my career. It was hardly possible for me to complete my doctoral work without the precious and invaluable support of these personalities.

I would like to give my small tribute to all those people. Initially, I would express my sincere gratitude to my supervisor Dr. SHRDDHA SAGAR Professor, School of Computing Science and Engineering and and Dr. RASHI AGARWAL, Galgotias College of Engineering and Technology for their valuable guidance, enthusiasm and overfriendly nature that helped me a lot to complete my research work in a timely manner.

I express my sincere thanks to Dr. Munish Sabharwal, Dean School of Computing Science & Engineering and Dr. Sampath Kumar, Coordinator PhD for their guidance and moral support during my research work and all faculties of School of Computing Science & Engineering who helped me a lot in my course of research work and all those who stood behind me. Nothing is possible without the constant support of my husband Mr. Prakash Chandra. I would like to convey my deep regard to my family for their wise counsel and indispensable advice that always encouraged me to work hard for the completion of my research work. My highest gratitude goes to my parent's and all my family members for their relentless support, blessings and encouragement.

SUPRIYA KHAITAN

Table of Contents

ABSTRACT	iii
CHAPTER 1: INTRODUCTION	1
1.1. Research Background	1
1.2. Motivation	2
1.3. Contribution	4
CHAPTER 2: CHAOTIC MAPS	6
2.1. Introduction	6
2.2 Paradigms of Chaotic Maps	8
2.2.1. Lorenz Map	8
2.2.2. Arnold Cat Map	10
2.2.3. Henon Map	14
2.2.4. Baker Map	17
2.2.5. Logistic Map	19
2.2.6. Tent Map	21
2.3. Paradigms of Chaos-based System	22
2.3.1 One-Dimensional Chaotic Map	25
2.3.2. Two-Dimensional Chaotic	26
2.3.3. Three-Dimensional Chaotic Logistic	27
2.4 Conclusion	29
CHAPTER 3: CHAOS-BASED CRYPTOGRAPHY	30

3.1 Introduction	30
3.2. Encryption Algorithms	32
3.2.1. Symmetric Key Encryption	33
3.2.2 Asymmetric Key Encryption	34
3.2.3. Hash Functions	35
3.3. Existing Cryptographic Algorithms	36
3.4. Image Encryption	43
3.5. Chaos-Based Cryptography	48
3.6. Observation	68
3.7. Conclusion	69
CHAPTER 4: SECURITY ANALYSIS	71
4.1. Histogram Analysis	71
4.2. Correlation Coefficient Analysis	72
4.3. Entropy Analysis	74
4.4. Differential Cryptoanalysis	75
4.5. Peak Signal-To-Noise Ratio and Mean Square Error	76
4.6. Keyspace Analysis	76
4.7. Key Sensitivity Analysis	77

CHAPTER 5: 3-D CHAOS BASED IMAGE ENCRYPTION USING LOGISTIC MAP	78
5.1 Introduction	78
5.2. Proposed Methodology	79
5.2.1. Key Generation	81
5.2.2. Encrypting the image	82
5.2.3 Decrypting the image	84
5.3. Performance Evaluation	85
5.3.1 Histogram Analysis	85
5.3.2 Correlation Analysis	86
5.3.3 Key sensitivity Analysis	88
5.3.4 Differential Cryptanalysis	89
5.3.5 Mean Square Error (MSE)	90
5.4. Conclusion	90
CHAPTER 6:	92
A ONE-DIMENSIONAL SUPERIOR LOGISTIC MAP BASED IMAGE ENCRYPTION	92
6.1. Introduction	92
6.2 Methodology Used	92
6.2.1. Algorithm for Generating Chaotic Sequence	96
6.2.2. Algorithm for Encryption	97
6.2.3. Algorithm for Decryption	97
6.3. Experimental Result and Analysis	98

6.4. Comparative Analysis of Lenna Image	107
6.5 Conclusion	107
CHAPTER 7: CHAOS-BASED ASYMMETRIC KEY CRYPTOGRAPHY	109
7.1. Introduction	109
7.2. Methodology	110
7.2.1. Chaos-based Key Generation	110
7.2.2. Improved Salp Swarm Algorithm (ISSA)	113
7.2.3. Encryption Phase	117
7.2.4. Decryption Phase	118
7.3.Experimental Results and Performance Evaluation	118
7.4. Comparative analysis	125
7.5. Conclusion	126
CHAPTER 8: CONCLUSION AND FUTURE PRESPECTIVE	128
REFERENCES	131

List of Figures

Figure. 2.1. Chaotic Attractors For Logistic Chaotic Systems (Boeing G, 2016)	8
Figure 2.2. Lorenz Chaotic Attractor	9
Figure 2.3. Difference Between 3-D And 2-D Map Encryption	12
Figure 2.4. Hanon Map Image Scrambling With Different Iterations	16
Figure 2.5. Scrambled Baker Map's (A) Actual Image, (B) After The First Iteration, (C) After The Second Iteration, And (D) After The Tenth Iteration	18
Figure 2.6 (A) Representation Of Logistic Map (B) Represents Iteration Equation	20
Figure 2.7. Tent Map Bifurcation Graph	22
Figure 2.8. Classification Of Chaotic Map	23
Figure 2.9. 2-D Chaotic Encryption	27
Figure 2.10. 2-D Chaotic Decryption	27
Figure 5.1. Image Encryption Structure	78
Figure 5.2. Image Decryption Structure	79
Figure 5.4. Histogram Analysis A) Lenna Image B) House Image	86
Figure 5.6. Correlation Analysis Lenna Image	88
Figure 6.1. Frequency Distribution Of X (T) For Chaotic Parameters	93
Figure 6.2. Proposed Methodology	95
Figure 6.3. Noise Attack: A) Gaussian Noise With Mean 0 And Variance 0.001 B) Salt And Pepper Noise Of Density 0.05	106
Figure 7.1. A) Bifurcation Diagram Of Tent Map B) Lyapunov Exponent Of Tent Map	111
Figure. 7.2. Methodology	112
Figure. 7.3. Basic Chaos Function	112

Figure 7.4. Working Principal Issa	117
Figure 7.5. Reference Input Database Images	119
Figure.7.6. Correlation Analysis For Input And Encrypted Image: (A) Lenna Image, (B) Babra Image (C) Baboon Image (D) Cameraman Image (E) Puppy Image	123
Figure 7. 7: Histogram Analysis For Input And Encrypted Image: (A) Lenna Image, (B) Babra Image (C) Baboon Image (D) Cameraman Image (E) Puppy Image	124

List of Tables

Table 5.1 Encrypted and Decrypted Images using 3D Logistic Map	87
Table 5.2. Correlation of pixels of 3D Logistic Map Encrypted Image	89
Table 5.3. Key Sensitivity Analysis	90
Table 5.4. Performance Analysis of 3D Logistic Map	90
Table 6.1. Performance Analysis of Superior Logistic Map based encryption	98
Table 6.2. Histogram Analysis	99
Table 6.3. Correlation Analysis	101
Table 6.4. Correlation Analysis of Original and Encrypted Image	102
Table 6.5. Key Sensitivity Analysis	103
Table 6.6. Differential cryptanalysis	105
Table 6.7. Noise Attack	106
Table 6.8. Comparative Performance Analysis of proposed scheme	107
Table 7.1. Overall, Image Sequence Encryption and Decryption	119
Table 7.2. Encryption and Decryption Time of ISSA Algorithm	120
Table 7.3. Entropy, PSNR, and MSE ISSA Algorithm	120
Table 7.4. Differential Cryptanalysis	121
Table7.5. Cross-Correlation Analysis	121
Table7.6. Key sensitivity Analysis	125
Table 7.7. Performance analysis of the SSA and ISSA	125
Table 7.8. NPCR and UACI Analysis of SSA and ISSA	126

List of Publications

International Journals

1. Supriya Khaitan, Shrddha Sagar, Rashi Agarwal “Chaos Cryptosystem with Optimal Key Selection for Image Encryption” *Multimedia Tools and Application*, Springer, 2022 (SCI)
2. Supriya Khaitan, Shrddha Sagar, Rashi Agarwal “A One-Dimensional superior logistic map-based image encryption”, *International Journal of Internet and Protocol Technology*, Inderscience Publisher, 2022, pp 226-235 (Scopus).
3. Supriya Khaitan, Shrddha Sagar, Rashi Agarwal “Chaos based image encryption using 3-Dimension logistic map”, *Materials Today Proceedings*, 2021 (Scopus).
4. Supriya Khaitan, Shrddha Sagar, Rashi Agarwal “Public Key Cryptosystem Based on Optimized Chaos-Based Image Encryption”, *Journal of Computational and Theoretical Nanoscience’s*, Vol.17, pp. 5217–5223.

International Conference

5. Supriya Khaitan, Shrddha Sagar, Rashi Agarwal (2023) “Chaos-Based Image Encryption with Salp Swarm Key Optimization” *Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems*, vol 491. Springer, Singapore.

Indian Patent

6. Indian Patent: 202011004322, “System and Method for Cryptography Using Chaotic Tent Map” Page 25, 14 February 2020.

Abbreviations

AES	Asymmetric Encryption Standard
DES	Data Encryption Standard
RSA	Rivest, Shamir, Adleman
IDEA	International Data Encryption Algorithm
DRPE	Double Random Phase Encoding
EWB	Electronic Workbench
CTM	Chaotic Tent Map
ACM	Arnold Cat Map
LFSR	Linear Feedback Shift Register
LTM	Logistic Tent Map
NPCR	Number of Changing Pixel rate
UACI	Unified Average Changed Intensity
MSE	Mean Square Error
PSNR	Peak Signal to Noise Ratio

CHAPTER 1: INTRODUCTION

1.1. Research Background

Thanks to new technology, it has become easier to process large amounts of text, video, and audio files over the Internet. In this era of information explosion, there is a risk of transferring private information over a public channel. This has led to great attention towards information security; it is essential to encrypt data to protect the confidentiality of the data transmission (Zhu et al., 2019). Text communications are frequently encrypted using standard encryption methods like the Data Encryption Standards (DES), Advanced Encryption Standard (AES), RSA, and IDEA. However, due to high pixel correlation, these algorithms are unsuitable for other multimedia data like images, audio, and video. Digital images, unlike text messages, contain inherent characteristics such as high correlation among neighboring pixels, huge storage capacity, and high redundancy. Researchers have repeatedly suggested employing numerous image encryption methods, such as chaos cryptography, genetic coding, and quantum theory, to resolve this challenge. Chaotic systems and maps have been engaged in several fields, like business, telecommunications, and technology (Teh et al., 2020).

The chaos theory consists of studying nonlinear dynamic systems that represent unpredictable behavior. These dynamic systems are susceptible to changes, and even with tiny parameter changes, they may have very diverse chaotic paths. Crypto-analytical study into the suggested multimedia encryption methods promotes designers' understanding of crypt analytical approaches. This helps them integrate conventional text encryption techniques and multimedia features with the appropriate security levels for every application environment. There are numerous methods for developing permutation and substitution boxes using chaotic maps, as well as creating encryption keys to ensure the safety of

communication. This includes the Lorenz chaotic map, the Tent map, the Bernoulli map, the Logistic map (Munir et al., 2019), and many more. In recent research, several image encryption techniques based on chaotic schemes have been found to be vulnerable. Many chaotic map-based techniques are susceptible to attack as they only utilize one phase of confusion and diffusion, for example, the chaotic tent map (CTM) encodes images by utilizing only the diffusing phase and skipping the confusing phase, which makes the CTM-based image encryption insecure (Li et al., 2017).

Researchers used high-dimensional chaotic maps to enhance the security of chaos map-based techniques. The safety of an algorithm is directly proportionate to its key space. The High Dimensional Equation was utilized to offer a bigger key space. The original 3-dimensional Lorenz system created the four-dimensional Lorenz system to enhance system encryption and security (Bisht et al., 2020). The scheme was followed by a better 2D Arnold transformation, which increased the safety of the chaotic tent map (CTM). With the support of the logistic sinus map and the logistic tent map, the parameters for the Arnold Cat Map (ACM) are produced. The Tent-Sine map changes Scrambled pixel intensity levels (Zhu et al., 2019). Many chaos-based encryption systems are either disclosed or supported by experimental statistical validation of the cipher text. Typical encryption methods require a high encryption rate and excellent cryptographic performance. The study's main contribution is the suggested key logistic map and tent map generation methods, which offer excellent security because they take a simple image and key for every key generation iteration.

1.2. Motivation

Like the video, audio, and Image material, including the multimedia traffic, is highly voluminous in size and has a strong connection between the pixel value values, conventional algorithms like AES, DES, IDES, and

LFSR may not be used for real-time photos or movies. Researchers are seeking light, quick and secure encryption systems, particularly for online communication in real-time. Chaotic Maps can be used to create a unique Image encryption system. secure cryptosystem requires a good quality of confusion and diffusion. That means

it demands a nonlinear complex relationship between the ciphered image and the plain image. It is embodied in a uniformly distributed and random-like ciphered image and a high sensitivity of the ciphered image to its plain image and secret key, etc. There has been plenty of research on chaos-based encryption algorithms, and many of them have been shown to be vulnerable to certain kinds of attacks. There are usually several drawbacks to this type of technology, such as insecurity, inefficiency, high computational complexity, difficulties in implementation, etc. A chaotic-based cryptosystem must address the problems shown in the following to achieve high security and robustness.:

- When the confusion and diffusion strategy is insecure and not complex enough, the key stream leaks information, including the secret key.
- To achieve security use of hyperchaotic maps is becoming popular, that leads to higher complexity.
- Over finite precision platforms, chaotic systems degrade dynamically.

We recommended that simple Images with various characteristics and correlations be encrypted differently to minimize time complexity and efficiency. In addition, chaotic maps such as Logistic maps with Picard iterations have chaotic performance limits that might degrade encryption and make it simple to break encrypted Images. Furthermore, hyperchaotic maps suffer from high computational costs and complex implementation; therefore, a new chaotic system is needed to increase chaotic characteristics for various system parameters. We thus suggested using superior and Noor iterations for logistic map chaotic systems as the

motive to provide more key space and security. The suggested encryption technique offers resistance against various attacks despite only one round of encryption. In addition, the time needed to encrypt Images is significantly less than the two other typical encryption systems in the suggested algorithm.

- The secret exchange technique allows a group of individuals to exchange secret information.
- To demonstrate that chase-based image encryption is safe, reliable, effective, and sensitive to initial conditions.
- Based on chaos, evaluate the results of symmetric and asymmetric image encryption methods.
- To use lower dimension chaotic for improved symmetric and asymmetric key encryption.

Security is always in demand when it comes to cryptosystems. To design new cryptosystems that are secure, it is crucial to find efficient methods. This requires exploring practical strategies for creating cryptographic algorithms with large key spaces and randomness properties. Moreover, to ensure a high level of reliability of a cryptosystem, it is necessary to find proper methods for overcoming the dynamic degradation of chaotic maps.

1.3. Contribution

We have developed the symmetric and asymmetric key image encryption method based on a low dimension chaotic map with both diffusion and confusion phases. While key generation was achieved using an improved logistic map in symmetric key generation and tent map with optimization in an asymmetric key generation—pixel scrambling results in confusion and dispersion. Moreover, the examination of the correlation algorithm has demonstrated that the relationship among pixel values varies while changing the key value, which proves that the approach is effective and safe. The technology offered could withstand the attacks like

statistical attacks, differential cryptanalysis attacks, noise attacks, etc. The suggested system is compared with current algorithms, indicating that the approach is safe, solid, and practical. The encryption of some image files has been tested using a simple stream cipher system. A chaotic generator is used to choose the key for encryption. Performance is assessed based on several factors. The performance of the cipher system for each chaotic generator is validated using Simulation results. In comparison, our generalizations enhance the key space and give additional options that are sometimes easier to use.

CHAPTER 2: CHAOTIC MAPS

2.1. Introduction

In order to implement chaos-based cryptography, chaotic maps are implemented to provide the properties required for confusion and diffusion, the elementary requirements of cryptography. Claude Shannon used diffusion and confusion to describe any cryptographic system's two primary structural hindrances. Shannon was concerned about cryptanalysis that relied on a statistical security assessment. The diffusion design seeks to make the quantifiable link between the plaintext and ciphertext as random as possible to thwart attempts to decipher the key. Confusion attempts to make the relationship between the ciphertext and the encryption key as perplexing as possible to obstruct efforts to locate the key. As a result of the spread and misunderstanding in capturing the essence of the ideal features of a block cipher, they have become the basis of today's contemporary block cipher. Constructing an encryption strategy makes use of both the confusion and diffusion standards.

Many chaotic maps suffer from the disadvantage of creating a cryptographic algorithm with a small key space. Hence, researchers have enhanced and merged several chaotic maps to increase chaotic characteristics, resulting in increased key space and unpredictable, chaotic sequences. (Pak & Huang, 2017) presented a framework for modifying two identical chaotic maps to achieve better results than a single map. The chaotic map range was regulated, and the MRI and X-Ray Images were presented with the specialized map with the expanding impact of the bifurcation diagram. 1-D chaotic maps have had restricted chain ranges and have been susceptible to attacks (Khaitan et al., 2020). Studies also suggest genetic encoding methods, Lorenz Map, Arnold Map, hyper-chaotic map, logistic map, scrambling bit level, tent map, and more. Several Chaos-based encryption techniques are used for Images; however,

their performance has many flaws (Chen et al., 2019). Chaotic maps contain features that fulfill the diffusion and confusion requirements for practical cryptography algorithms. Chaotic encryption exemplifies the use of the chaos hypothesis for various cryptographic problems. Many researchers have utilized the logistic map with Picard iterations in the encryption process since it is more straightforward and effective. However, they discovered that it has limited key space and poor security. Because of its flaws, researchers attempted to build new chaotic maps that are more secure and perform better (Zahmoul et al., 2017).

The intriguing characteristic of the chaotic system is its strong impact on its underlying condition, control criteria, and ease of use, which leads to high encryption rates through traits (Jithin & Sankar, 2020). A chaotic map's state function and controller parameters can be controlled, destroying the input state space. However, the performance of chaotic maps cannot be significantly enhanced using this approach alone; it works best when coupled with other approaches (Xiang & Liu, 2020). In a nonlinear function, the state variable is updated based on the parameters of the current map, and then the parameters are updated. Consequently, the state space is destroyed, and the chaotic sequence is made more random and complex. (Wang et al., 2019), investigates the characteristics of SMN produced by executing the one-dimensional logistic chaotic map in the software world. Every computationally efficient value in the chaotic map's field is regarded as a node. A directed edge between two nodes is provided, but only if the stochastic model maps the former node to the latter. The dynamical characteristics of chaotic maps in the fixed-point arithmetic domain are revealed by analyzing their equivalent using the Logistic and Tent maps as illustrations (Li C. et al., 2019). A complex dynamical strange attractor, also called a chaotic attractor, is an attractive set of states that shows sensitivity to initial conditions; due to this, the divergence among nearby states is exponentially fast, and the system becomes unpredictable. Figure 2.1 shows the chaotic attractors of chaotic logistic maps. These attractors have an outer pattern and fixed geometric

structures; however, the inner trajectories are unpredictable.

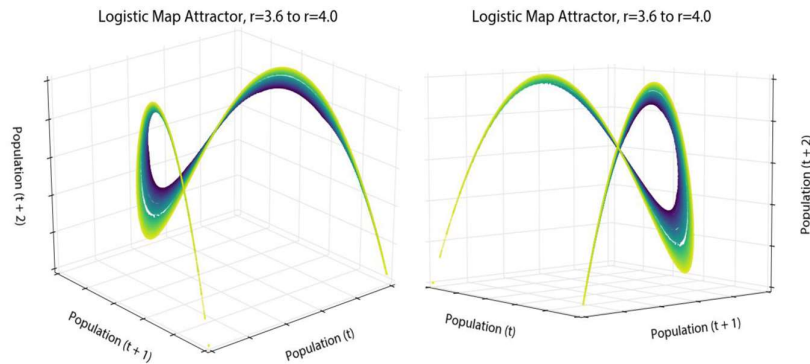


Figure. 2.1. Chaotic attractors for Logistic chaotic systems (Boeing G, 2016)

2.2 Paradigms of Chaotic Maps

2.2.1. Lorenz Map

E.N. Lorenz proposed the Lorenz ordinary differential equation in 1963; these are dynamic systems with complex structures. For some parameters and initial conditions, the Lorenz system has chaotic solutions. Three positive initial values and three parameters are used as the key to the encryption problem. As a result of the Lorenz chaos sequences, a stack of chaotic solutions is created, serving as an attractor. When the Lorenz system is plotted, it produces a Butterfly-like attractor, as shown in Figure 2.2. Initially, the chaotic system was designed to simulate atmospheric convection. The 3D Lorenz is a three-dimensional chaotic map.

Edward Lorenz, a physicist, created it using a coupled differential equation. The Lorenz chaos sequences produced attractors, the deck of chaotic solutions for the chaotic system. Equations 2.1,2.2 and 2.3 represent the 3D Lorenz chaotic formula Ali et al., (2021).

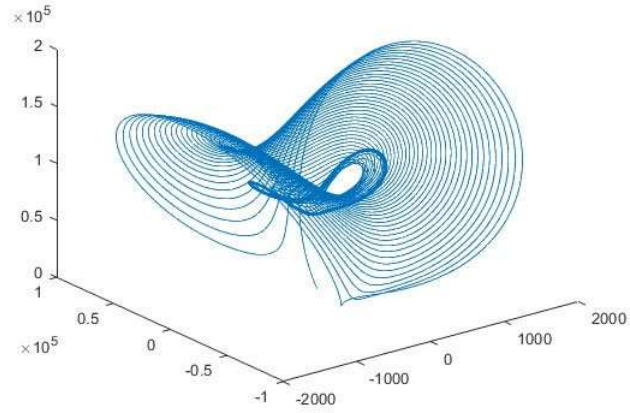


Figure 2.2. Lorenz Chaotic attractor

$$\frac{dx}{dt} = \sigma(y - x) \quad Eq (2.1)$$

$$\frac{dy}{dt} = rx - rz - y \quad Eq (2.2)$$

$$\frac{dz}{dt} = xy - bz \quad Eq (2.3)$$

There are significant effects on the system caused by the control parameters r and b . Chaos sequences are generated when the precise value of chaos is fixed. The Runge Kutta algorithm is used to determine the system's trajectory. The map shows chaotic behavior for the following values (σ) = 10, ρ (Rayleigh number) = 88500, and b (Beta) = 8/3. These chaotic values are used for encryption purposes. The technology performed even better when it came to encrypting channel-specific Images and adding an extra degree of protection to the chaos-based encrypted channels. Masood et al., (2020) Discuss the advantage of channel security. Encryption systems have also been improved using the Lorenz system. Various researchers have proposed the use of two Lorenz

Systems with permutation matrices as a chaotic-based encryption scheme. These systems had a bigger key space and were found to be secure.

As part of another research, Sharma et al. (2017) presented an image encryption technique that is based on the 3D-Lorenz system. As part of the DRPE-based image encryption, Arnold transforms and a chaotic baker's map is used. However, no research has been done on DRPE-based phase-image encryption utilizing the three Dimension Lorenz transform. This chaotic system has high dimensionality, vast key space, greater sensitivity, and unpredictability Farajallah et al., (2013). Due to the fact that Lorenz chaotic systems are not iterative and are created by solving linked differential equations, they are faster than their competitors. Neha et al. (2016) proposed a 3-dimension Lorenz chaotic map system for phase image encryption in the Fourier domain. The shuffling of pixels was done by the frequency domain of the Lorenz system. The system was attacked using a chosen plain text attack with only three images. Each plain Image processed through the encryption method recovers the three keys used for shuffling, multiplication, and bitwise XOR Munir et al., (2021).

2.2.2. Arnold Cat Map

Vladimir Arnold, a Russian mathematician, devised a chaotic change called the Arnold transformation or Arnold cat map as he worked on dynamical theory. Transforming Arnold works in an easy method; a fundamental matrix transforms the Image's coordinate location, the Image is confused by increasingly iterating, and the source is retrieved when a specific number of iterations has been achieved (Raj et al. 2019). Even for lengthy streams, a few functions (chaotic maps) and a few arguments are enough. In addition, many streams may be readily generated by altering the original circumstances. These benefits have led to chaos being used as a random generator of numbers (Avaroglu, 2017).

Arnold Cat map is a 2-D mapping, which alters the original position of pixels randomly when applied to a digital Image. Arnold Cat map is among the most common transformed image enhancement in cryptography and copyrighting (Soleymani et al., 2019). The Arnold Cat Map is chaos two-dimensional, which can be utilized to encrypt Image pixels without destroying any pixel image data; $S = \{(x, y) \mid x, y = 0, 1, 2 \dots N-1\}$ may be taken for pixel resolution. The following equation may write a 2-dimensional Image of Arnold's Cat Map (Hariyanto, E., & Rahim, R. (2016).

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} \pmod{n} \quad \text{Eq (2.4)}$$

$$\begin{bmatrix} 1 & p \\ q & pq \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \pmod{n} \quad \text{Eq (2.5)}$$

Where $N =$ Image height and width. $x, y =$ original Image pixel position,
 $x', y' =$ after mapping pixel position. $p, q =$ parameters for the system. The result of the change relies on the characteristics of the system. The system parameter standard value is $p=q=1$. After R iterations are applied to an image, a random image is generated where all pixels are the same as the original Image. The number of observations is the essential key to Arnold's transformation. The number of iterations needed to recreate the original is the transformation period in Arnold. Arnold Cat Map's diffusion and confusion characteristics make it better suited for image safety (Raj et al., 2019). The plain Image is predominantly diffused with the bitwise Exclusive-OR activity; the DNA planning rule is acquainted with encoding the diffused Image.

Chaos spatiotemporal framework is applied to confuse the lines and sections of DNA encoded image. A clever calculation for Image encryption dependent on a rough strategic guide with altering boundaries was proposed. The plain Image is rearranged by utilizing the calculated

guide's altered limit; afterward, the scrambled Image is encoded by a dynamical calculation. In a novel, the turmoil-based secure Image encryption calculation is introduced. The encryption calculation has been separated into three phases: the arbitrary number age measure, the Image change measure, and the replacement cycle. There is a 2D Chaotic map that is used to generate the random number generator. In the subsequent stage, an Image is permuted twice. This permuted Image is, at long last, applied to the encryption cycle. Groupings are introduced in a clever encryption calculation for non-equivalent measurement shading Images utilizing a tumultuous stream. This calculation changes the pixel worth and position using another chaotic collection called Chue Lorenz (CL) arrangement Batool, S. I., & Waseem, H. M. (2019).

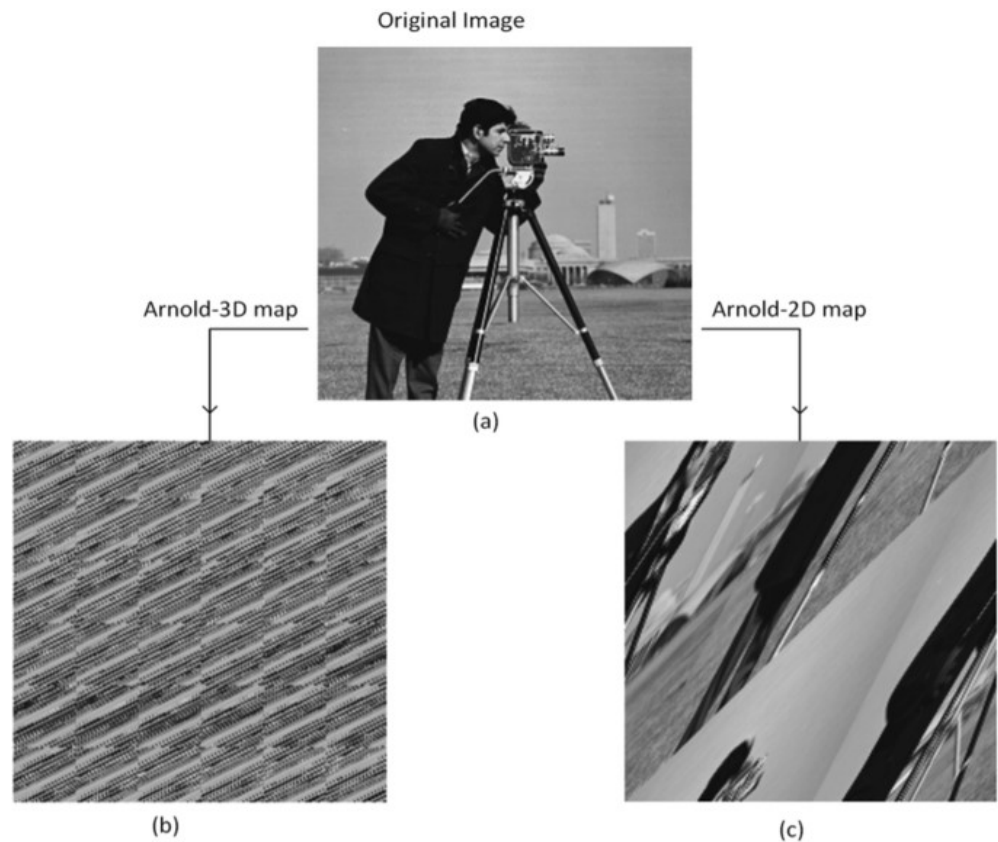


Figure 2.3. Difference between 3-D and 2-D map encryption

Figure 2.3 shows distinct variations between the three-dimensional map and the two-dimensional equivalent. However, mathematical accuracy diminishes with each iteration of the map while computing the Arnold cat map on a system. The degree of precision is limited by the period of the intended computation. ACM is a 2D inverted chaotic map used to rearrange a pixel's position. This card is a suitable scrambling device used in many cryptographic and steganographic applications to disrupt the correlation between adjacent pixels. The position of pixels in Arnold's 2D cat map is changed, compromising the encryption's security. The encryption pixels in the Image will become identical to the original after a few epochs; therefore, the periodicity will reduce security of algorithm Suneja. et. al., (2019). Because the Arnold cat map just has a linear transformation and a modulo function, scrambling the locations of pixels is highly efficient. After several rounds, the high connection between neighboring pixels is erased or considerably diminished. Attackers can, however, loop the Arnold cat map until the original Image is recovered. In addition to the pixel position scrambling, the pixel values must be hidden. This article uses the pseudo-randomly augmented logistic map to modify pixel values after Arnold shuffling to attain the necessary level of security Dagadu et al., (2017).

It has previously been stated that confusion and diffusion are the two fundamental phases in any encryption process. The new system is built, so both methods are carried out at separate stages of the algorithm. The permutation process is referred to as the confusion stage. Within the Image, the pixel locations are swapped. The diffusion technique relates to the substitution method, which implies that the values of the pixels are exchanged. The pixel permutation in the system is done in the first phase using the Arnold map. Following the confusion step, every pixel in the Image is moved. The diffusion is then carried out by XORing the pixel values with the key streams created by the Tent map Sneha et al., (2020).

2.2.3. Henon Map

The Henon map is a typical discrete, basic structured dynamic system. The effectiveness of the Henon map must be examined if memory and nonlinear characteristics of the discrete memory may be further enhanced (Peng et al., 2020). The Henon map is a basic 2-D map with chaotic strategies: quadratic nonlinear and unusual attractors. Michel Henon presented the model as a precise prediction of the Two-dimensional map that emerges from a Lorenz equation solution (Roy & Misra, 2017). This map is one of the more widely researched models of discrete nonlinear systems showing messy behavior. The 3D Henon map is characterized as the generalization of the conventional Henon map (Liu et al., 2019). 2-D forward map of nonlinearity quadratic. This map showed the unusual fractal structure attractor for the first time. The Henon map adapts numerical research due to its straightforwardness. This is how many computer exams have been performed. In any event, the entire Image of all imaginable forks under the parameter difference a and b is far from complete (Anandkumar & Kalpana, 2018).

$$\frac{dx}{dt} = a(y^2 - bz) \quad Eq (2.6)$$

$$\frac{dy}{dt} = x \quad Eq (2.7)$$

$$\frac{dz}{dt} = y \quad Eq (2.8)$$

The above equation represents the Henon mapping system. An innovative keystream generation schema is proposed using the two types of chaotic maps, the 3D Cat map and the 3D Henon map. As a first step, this approach generates random integers using a 3D Henon map and transforms them into binary sequences. Then the sequence places created

by the 3D Cat map were allowed, and XOR in the last phase. As a result, the keystream will be of high quality and will be highly secure against a wide variety of attacks Albahrani et. al., (2017). The hidden keys K1 and K2 offer several possible options, which provide maximum protection in the Image. The 64-bit binary sequence is the primary key. The 2-session keys created by the unique key are 64 bits long respectively and therefore are analyzed against the input Image, which is converted into 64-bit chunks individually (Sabah et al., 2018).

An unauthorized individual cannot exploit the frequency of two-dimensional chaotic maps because their control parameters are susceptible to secret keys. The equation for a 2D cat map with control rules Suneja et al., (2019) Confusion was achieved by pixel displacement from the current position to a new one, and diffusion was accomplished through a byte sequence created by the Henon map. An approach for creating 3D cat maps utilizing enhanced logistic maps and Henon maps has been designed. Image encryption and decryption techniques have been considered in a different context Sinha et al., (2018). There is no requirement to select the best set of values to be used as encryption sequences. Our work only requires a random set of integers to be processed. Chaotic maps are the best solution for creating such collections of numbers. The map will create a distinct set of numbers depending on the values of the parameters. Select any fine collection of sequences for our further processing. The map specification recommends appropriate values that may be set to parameters (or constants) to ensure correct randomness in its arrangements (Sneha et al. (2020).



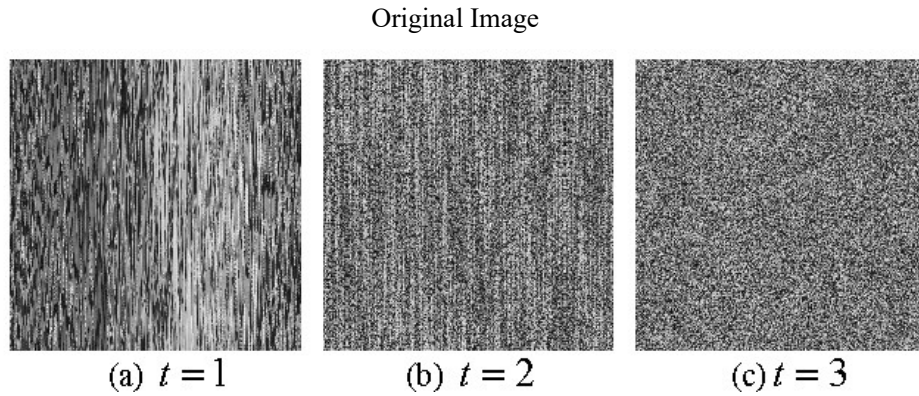


Figure 2.4. Hanon map image scrambling with different iterations

The Image created by the Henon map with three iteration rounds is shown in Figure 4. The Henon map iteration is like the random iteration, with no textural characteristics or subsequent transformation in the scrambled Image. The complexity of a chaotic sequence indicates how near it is to a random sequence, with higher complexity indicating that the chaotic sequence is more spontaneous. The spectral entropy (SE) complexity measure technique is used in this case to determine the complexity of the two systems as well as the sample size of the time series. The SE complexity of the discrete memristor-based Hénon map and the Hénon map. The presence of a dark color region suggests that the area is complicated. It demonstrates that the original Hénon map's high complexity region is relatively small. On the other hand, the discrete memristor-based Hénon map has a significantly more extensive range of high complexity, with a massive band of increased complexity in the ranges of $a [1, 2]$ and $b [0, 3.2]$. As a result, it indicates that the Hénon map based on the discrete memristor model has a greater chance of being used in technical applications such as secure communication Peng et al., (2020).

2.2.4. Baker Map

The Baker map is a rapid and invertible mapping that can securely encrypt an image with minimal computing cost. The traditional Baker map may be seen as a variable. The map exhibits a chaotic behavior while governed by these basic equations and has all of the attractive traits of cryptography (Musanna et al., 2020). The Baker map is a chaotic 2 different connections between the M*M matrix unit. They are used chiefly for adjusting the pixel location without affecting or altering the image pixels (Sekar & Arun, 2020). The map of the 2-dimensional Baker is represented as

$$p_{n+1} = \begin{cases} \gamma_a p_n, & \text{if } q_n < \alpha \\ (1 - \gamma_b + \gamma_b p_n), & \text{if } q_n > \alpha \end{cases} \quad Eq (2.9)$$

$$q_{n+1} = \begin{cases} \frac{q_n}{\alpha}, & \text{if } q_n < \alpha \\ \frac{(q_n - \alpha)}{\gamma}, & \text{if } q_n > \alpha \end{cases} \quad Eq (2.10)$$

Mod 1 is used to compute p and q. The Baker map used to scramble the intensity values offers enough algorithm of the image intensity. The chaotic attraction generates the chaotic points required by diffusion technique. The map Baker is a two-dimensional, chaos-inducing, dynamic system that conserves vertical and lateral extending, followed by chopping and layering, similar to the motion of the Baker to create the bread pudding (Chapaneri et al., 2013).

This Figure depicts the Scrambled Baker Map after ten iterations of scrambling. Taking advantage of time parameters and cascade baker mapping can be used to manage the state and parameters of chaotic systems. A logistic map based on the 2D Baker map was enhanced by regularly altering the initial parameters and states. This enhanced chaotic map can be used both for shuffling and for substitution in cryptographic

operations. A complexity analysis was carried out in order to demonstrate the unpredictability and complexity of the revised map Luo et.al. (2019)

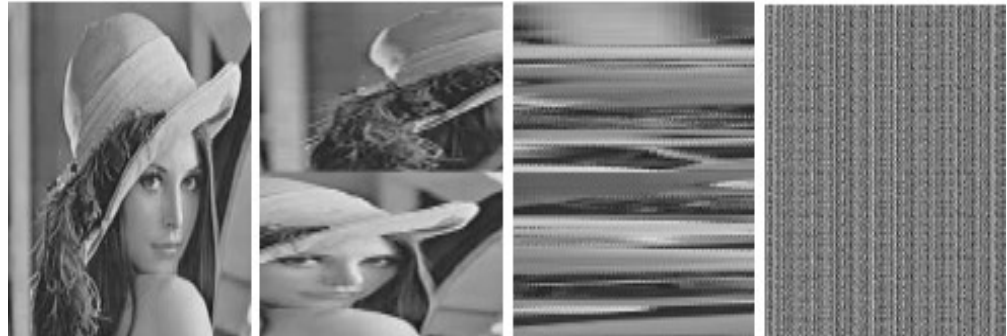


Figure 2.5. Scrambled Baker Map's (a) actual Image, (b) after the first iteration, (c) after the second iteration, and (d) after the tenth iteration (Chapaneri et al., 2013).

Some criteria, such as constraints, were not found in a search for current cryptographic algorithms based on chaos. The encryption must, for example, exist within constraints in a practical application; they are a time slice that may be highly tiny for a cryptographic application. Research teams have done a great deal of work on the overall processing time to overcome these issues (Mekki et al., 2018). To achieve higher levels of security and quicker encryption, the 2d baker map is transformed into a 3d chaotic map.

An innovative technique for permutation and substitution that is resistant to various statistical and differential attacks has been developed for image encryption. Discrete baker maps can be extended to 3D to combine gray values. Furthermore, 3D maps can be inverted to combine gray values. There are several 3D maps available, including logistic maps, Chebyshev maps, and Arnold cat maps, among others. Two additional control factors emerged from the 3D Arnold cat map Suneja et al., (2019).

2.2.5. Logistic Map

Chaotic maps are hyper-delicate and uncertain of starting value. A change in the number sequence produced by the function can occur, even if the beginning value changes slightly. Various chaotic maps are utilized, but the most prosperous one is the logistic map (Ramasamy et al., 2019). Researchers propose a hybrid control system of disruption and feedback to decrease the dynamic deterioration in the digital logistic map. To change parameters using a current status variable and to disrupt the existing status variable through the updated parameters. The original map of chaos may be enhanced, and dynamic deterioration of the initial mapping can be eliminated by disturbing the state variable and the current map parameter and utilizing a status feedback mechanism to destroy the state space (Xiang et al., 2020). This map was introduced by Robert May in 1976. Logistic maps are polynomial maps of the second degree. Logistic maps are often shown.

$$\gamma_{n+1} = r\gamma_n (1 - \gamma_n) \quad \text{Eq (2.11)}$$

The r symbols function as the original requirements in the logistic maps and are (r, ∞) in which r takes any number between $[0,1]$ at first. Those maps are being used to spread the original Image in multiple rows. Dynamical maps have various inconveniences, such as a relatively limited area of keyspace and chaotic behavior mostly within the range of alpha (3.57.4). For values over 4 (i.e., $\alpha > 4$). Negative Figures retrieve the data (Sekar & Arun, 2020). The complex variable can thus be chosen here depending on the scenario. We can select a more complicated nonlinear feature, such as complex exponential features, for security concerns, etc. Following user demands, the nonlinear function is picked, taking simply sine and cosine as references (Xiang et al., 2020).

A novel 2-D Sine Logistical Map (SLMM) is created using the logistic and sine maps. Compared to the current chaos-based, it possesses acceptable unpredictable situations, a sizeable chaotic spectrum, a hyperchaotic characteristic, and a lower implementation cost. The chaotic magic transformation (CMT) is used to assess its applicability by effectively switching an image's pixels. CMT may quickly rearrange the pixels of an Image in both row and column locations simultaneously by employing a stochastic sequence generated by 2d SLMM Suneja et al., (2019).

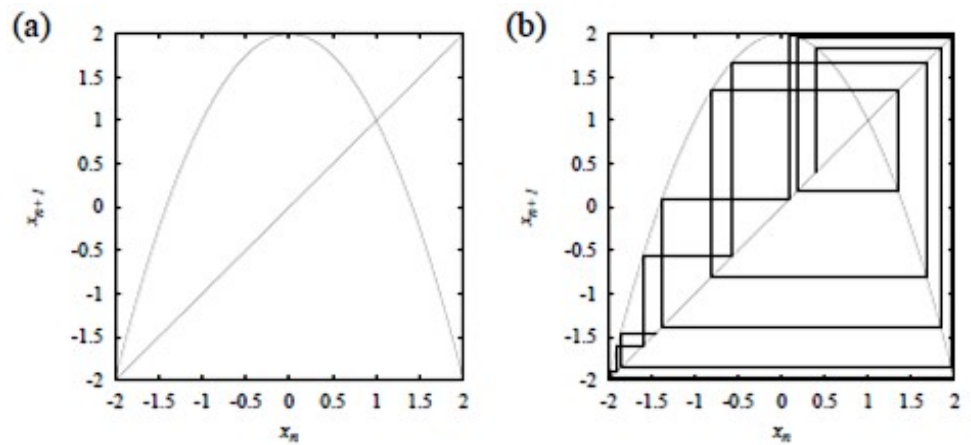


Figure 2.6 (a) Representation of logistic Map (b) Represents iteration equation (Suneja et. Al. 2019)

Therefore, dynamic deterioration occurs when the map is replicated on a workstation or other limited-accuracy devices. The output path falls into a loop, and the phase space does not pass across all areas. DH map (double-humped logistic map) is a one-dimensional (1D) map with a fixed bifurcation diagram and a predetermined chaotic range. The addition of an extra generic parameter to the equation allows greater control over the chaotic behavior of the map, simplifying the construction of any map and making it more suitable for a wide range of applications. The logistic map generalization based on fractional power was introduced by Ismail et al., (2018).

2.2.6. Tent Map

In terms of the constant density and power spectrum, the chaotic behaviors of the tent maps are analytical during its chaotic zone. With the maximum height reduced, the chaotic area is experienced with consecutive transitions of band splitting, and the point of change into the nonchaotic region is accumulated (Li et al. 2107). Tent map behaviors are nearly identical to the logistic map, and the limits, i.e., the range, are also the same. Negative values are obtained if β goes further than the maps (Sekar & Arun, 2020). The restrictions lead to a risk of empirical assaults using the encryption method with a pure tent map. The tent map can be represented as

$$\gamma_{n+1} = f_{\beta}(\gamma_n, \beta) \begin{cases} \beta\gamma_n, & \gamma_n < 0.5 \\ \beta(1 - \gamma_n), & \gamma_n > 0.5 \end{cases} \quad Eq (2.12)$$

The frequency correlation value and spectrogram of non-periodic orbits are computed accurately at and around the split band locations. Topologically, the tent map is combined, and hence the behaviors of the map are equivalent under iteration in that sense (Li et al., 2017). The mechanism is just not chaotic and generates a periodic digital output, making it unsuitable for encryption techniques. In several existing literature, the combination of logistic maps, tents, and symbols significantly increases the key size. Despite its unpredictable conditions, the map has unconstrained solutions with good chaos performance. An analytical study of a tent map (a nonlinear linear, continuous map with a single maximum) considers constant density and power spectrum throughout its chaotic area.

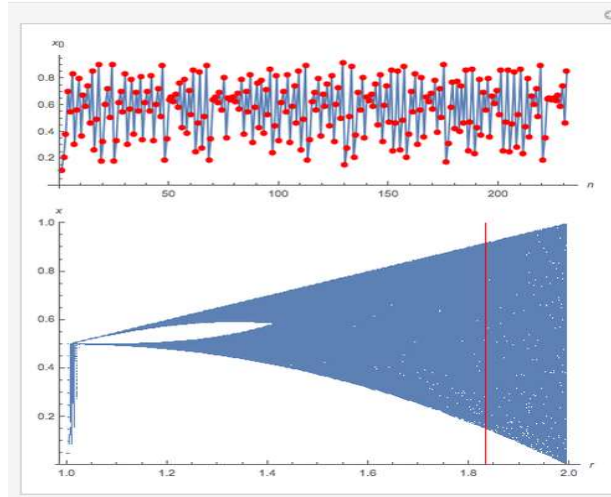


Figure 2.7. Tent Map Bifurcation Graph

(<https://demonstrations.wolfram.com>)

As the maximum height is reduced, consecutive spectrum changes in the chaotic area occur, accumulating near the nonchaotic region's transition point. At the spectrum sites and in the neighborhood of these locations, the time-correlation function and frequency spectrum of stochastic processes orbits are computed precisely. Because the tent map is highly ordered conjugate, its behaviors under repeating are, in this sense, similar (Li et al. 2017).

2.3. Paradigms of Chaos-based System

Continuous maps of discrete maps can be used to characterize a chaotic map. There are three types of maps: one-dimensional (1D), two-dimensional (2D), and three-dimensional (3D). The structure of 1D chaotic systems is essential and therefore is straightforward to construct. However, one of its flaws is low-dimensional faults, such as a tiny key space. Many researchers are looking for high-dimensional, such as 2D or 3D, to strengthen the security of encryption systems. However, the complicated structure raises the cost of development and the difficulty of processing. Because of its simple design, good chaotic properties,

acceptable autocorrelation and cross-correlation features, the traditional one-dimensional (1D) logistic map has been frequently utilized in Image encryption methods. It just contains one control parameter and one starting condition, though. Furthermore, it creates weak keys due to flaws such as blank windows, stable windows, unequal distributions of iterated sequences, and so on, as pointed out and studied

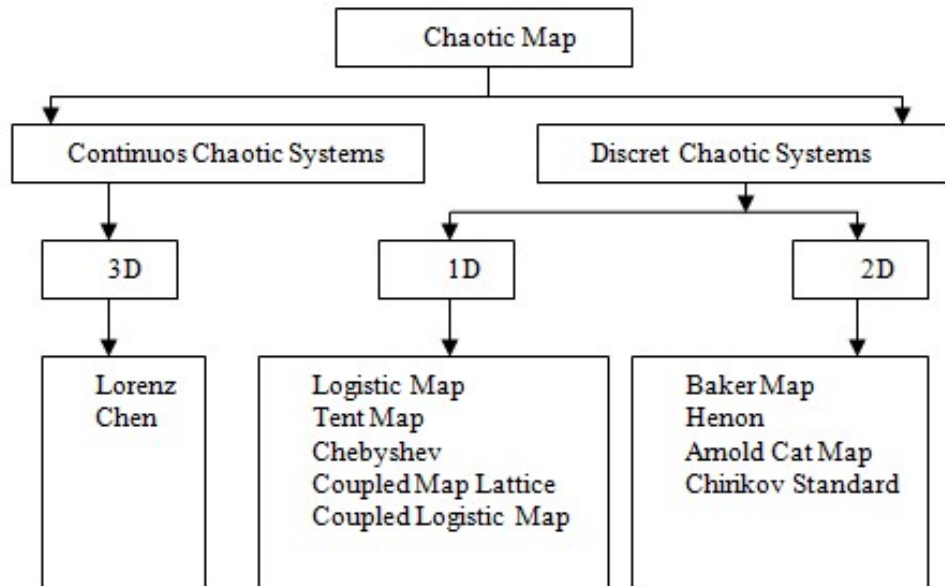


Figure 2.8. Classification of Chaotic Map (Mekki et.al. (2018))

In general, there are two primary ways to protect digital Images. Watermarking, anonymity, steganography, and cover channel are information concealing techniques. The other is encryption, which covers standard encryption and alternatives like chaotic encryption. There are many significant characteristics of chaotic systems, including their sensitivity to initial conditions, their density, and their topological transitivity, among others. In the context of cryptography, most qualities are connected to some criteria, such as mixing and diffusion. As a result, chaotic cryptosystems are more helpful and practical Zhang et al., (2015).

As a result, an interweaving logistic map with additional control

parameters and starting circumstances is developed to address such flaws Ye, G., & Huang, X. (2017). The vast majority of current one-dimensional chaotic maps feature a continuous space. On the other hand, the discrete character of digital gadgets contrasts with the constant area on which these chaotic maps work (Lambic, 2017). Because digital computers and devices can only employ mappings from finite sets to finite sets, continuous values must be approximated to discrete values. Such chaotic system approximations, specified on the endless space, induce the dynamic deterioration of digital technology (Wang et al., 2016). Henceforth we use chaos in cryptography and other fields, and a digital methodology is required. Lately, 1-dimensional discrete-space chaotic maps that entirely answer the problem of dynamical deterioration have been suggested (Lambic, 2018). Furthermore, these maps lack fixed points, which is the desired property in encryption.

However, chaotic maps have other properties that limit their use in cryptography and some other fields (Flores-Vergara et al., 2019). As with Gaussian, sine, tent, and provision maps, the chaotic map carries variable and restricted parameters. The work includes a more significant number of calculations, and every one of the upsides of assessment boundaries is worked on. The productive use of WHT empowers the framework to conceal the first pixel esteems or Image data and make them into a more minimized structure before applying encryption. Subsequently, making the proposed framework safer than some other existing strategies clarified up until this point and WHT is computationally quick. The RGB to YCbCr shading space transformation is applied in framework, unlike different techniques around here (Sneha et al., 2020).

It usually occurs in Image preparing applications. This is done to apply some type of pressure on the information Image and address it with an insignificant measure of information, so it tends to be communicated with less transfer speed. The Image in YCbCr shading space has three parts: Y (luminance), Cb (blue contrast), and Cr (red distinction). Their

chaotic orbits and style are simple. It's bound limitations like discontinuous vary and non-uniform information distribution. With the sweetening of chaotic signals, if even little data is obtained, then the orbits of chaotic maps are evaluated, and their initial values will be identified. These limitations affect their applications in varied security areas. In the image secret writing rule, various encoding algorithms seem to be insecure if 1d chaotic maps are used Suneja et al., (2019). The following section summarizes the few other discrete chaotic maps utilized for comparative analysis in this thesis.

2.3.1 One-Dimensional Chaotic Map

Elmanfaloty et al., (2020), Initially, cryptologists applied chaos theory to cryptography using one-dimensional chaotic functions because of their complicated behavior and simple mathematical and digital hardware representations. The problem with most of these functions is that the orbits collapse into a specific period, owing to limited precision and the restriction of the number of parameters that can be controlled. As a result, multiple security flaws were uncovered, and the system was vulnerable to many forms of assault. Introducing a 1D chaotic function with five control parameters solves the problem of a restricted number of control parameters. The function's chaotic qualities, as well as its capacity to generate a cryptographically safe random stream of integers, are revealed by analysis. To demonstrate its robustness, a novel picture encryption technique is developed that uses the function as its random number generator. Several tests of the proposed system show that it is secure and has good confusion-diffusion capabilities.

For instance, approximations of any sort have no effect on generating S-boxes (Lambić et al. 2017); the specific case of the chaotic map has the disadvantage of having very short orbit lengths. As a result, it must be

utilized with prudence, employing a higher number of permutation components, which reduces performance and increases memory needs. To address this issue, a novel notable instance of a one-dimensional discrete chaotic map is provided based on the composition of permutations and the sine function. Compared to the chaotic map case, the map has a more considerable length of orbits, which mitigates the potential negative consequences of shorter orbits. Figure 3.5 illustrates the diagram of a 1-Dimensional Logistic map.

2.3.2. Two-Dimensional Chaotic

A chaos map and chaotic system in cryptography have proven useful and practical. A logistic map with intricate basin structures and attractors was used to encrypt pictures Yue et.al. (2012). The method uses cryptography's traditional permutation-substitution network structure to ensure that a safe cipher has both confusion and diffusion qualities, as shown in Figure 2.9 and 2.10. The method is capable of converting an understandable image into a random-like image both from a statistical perspective and from the perspective of a human visual system. Simulations using USC-SIPI images demonstrate the method's effectiveness and resilience. The method's encryption quality meets or exceeds the existing state-of-the-art methods, according to security study results using both traditional and more contemporary testing.

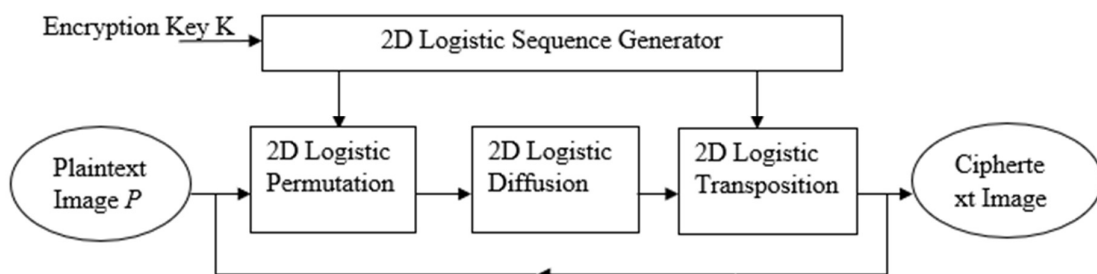


Figure 2.9. 2-D Chaotic Encryption

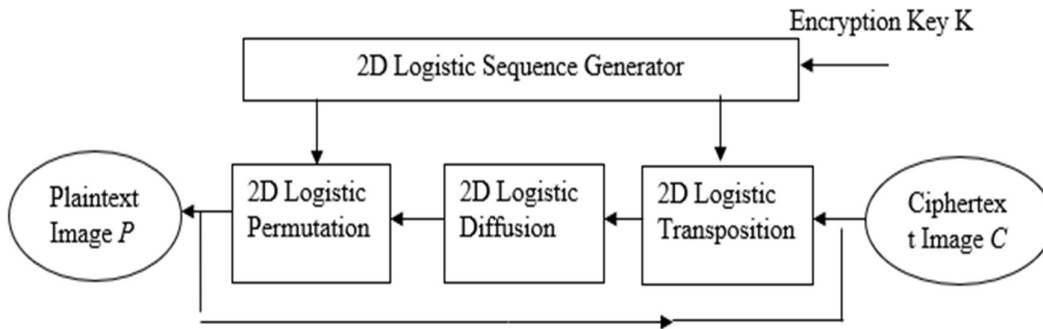


Figure 2.10. 2-D Chaotic Decryption

2.3.3. Three-Dimensional Chaotic Logistic

A chaotic system can be divided into two types based upon its dimension: a high-dimensional system and a low dimensional system. Due to their complexity and outstanding chaotic features, high dimensional chaotic orbits are more unpredictable. 1D chaos systems are easier to implement and have a less complicated chaotic structure than high-dimensional chaos systems. Despite this, they are vulnerable to assault and have restricted chaotic ranges. Thus, the chaotic system has superior chaotic properties as a result of these enhancements, which effectively compensate for the flaws of the simple one-dimensional chaotic system. In light of this, (Luo et al., 2019) proposed a method based on three overlapping chaotic systems: a cascade baker, a logistic two chaotic systems and a temporal parameter control. There was a significant improvement in chaotic features and a greater parameter space with the new system.

Masood et al.(2020) propose a less computationally expensive, yet more secure, approach. In this system, fractals are used as the key and a

three-dimensional Lorenz chaotic map is used to create the shuffling. Shuffling applied the confusion attribute to the standard picture and jumbled the pixels. A three-dimensional chaotic logistic map generates the chaos-based key stream, which performs better regarding randomization qualities and security level was proposed. The projected scheme's design is effective. Figure. 3.8 illustrates a three-dimensional chaotic-logistic map to encrypt an image with confusion and diffusion. There are several well-known methods for analyzing the input picture encryption scheme's security and performance. The simulation results reveal that the recommended scheme passes all the needed presentation standards, including ample key space, high-level security, and appropriate encryption speed. The fail-safe analysis is enlightening, and the strategy may be inferred to be both efficient and secure. Because of these properties, it's a good candidate for use in cryptography applications.

The two nonlinearities are significantly considered in constructing the chaotic system with aquaretic nonlinearity and quadratic nonlinearity (Pham et al., 2017), Several studies have been conducted on the three-dimensional chaotic system, including dissipative points, rest points, and their stability, phase portraits, Lyapunov exponents of chaos, Kaplan-Yorke dimensions, etc. In order to achieve global stabilization of the chaotic system, feedback control laws were designed using adaptive control theory. To confirm the feasibility of the chaotic theoretical model, an electronic circuit design of the new chaotic system is described in detail using an electronic workbench (EWB).

Chaotic systems have indicated a possible path with desirable features; the most noticeable feature is ergodicity, strong sensitivity to initial conditions, system characteristics, and pseudo-randomness. There have been several proposals for chaos-based picture encryption methods most are based on the fundamental structure of a chaotic system that includes confusion and diffusion. For diffusion, a chaotic map is employed as the generated key stream. Experiment results suggest that this approach delivers a reasonable

degree of security. It is suitable for real-time applications where the encryption time must be kept low. In chaos-based encryption, pseudo-random sequences are constructed by using the lowest significant bits or digits of finite-precision numbers. The findings generated using this method are highly susceptible to rounding mistakes and the discretization effect, the innovative approach for calculating the maximum number of bits acceptable for producing pseudo-random sequences from the binary representation of floating-point values (Tutueva et al., 2021).

2.4 Conclusion

There are many examples of chaos in nature; it is a unique phenomenon in dynamic systems. Chaos maps can be classified as discrete-time or continuous-time chaotic maps. The chaotic maps are known to be best for cryptographic application because of their properties that constitute the core of chaotic dynamics. These properties include high sensitivity to initial conditions, ergodic nature, transitivity, and has dense periodic points. The chaotic maps can be one dimension or they may be of higher dimensions. The higher dimension maps provide better key space than Low-dimensional methods; however, are widely used in research due to their rich, chaotic nature and ease of implementation.

CHAPTER 3: CHAOS-BASED CRYPTOGRAPHY

3.1 Introduction

Information should be broken down by customers before it is outsourced to a remote distributed storage advantage. Both information security and information should be guaranteed so that distributed storage companies cannot scrap the information when customers have to look at some sections of the actual data. They must toss the information before retrieving it (Tayal S. et al., 2017). Particularly in the last century, the cryptographic process has experienced three main changes: the employment of cipher machines rather than manual encryption has considerably improved cryptographic complexity; rigorous mathematical methods in cryptography have made encryption science (LI Jian et al., 2018). Proxy encryption is a special-purpose crypto scheme that is a proxy that may transform the Alice cipher text to Bob's cipher text with specific information efficiency.

Cryptography is a technique of hiding information, utilized since Roman times for information or secrecy. Encoding a message with an unmistakably safe key, known by sender and recipient ends, is an excellent prospect to obtain high sensor security. A commonly used approach is encryption/decryption to keep information private. Proxy re-encryption (PRE) was developed to solve this key management problem. The primary aim is to have the lowest possible confidence in the proxy (Ateniese G. et al., 2009). The strength of various encryption methods is determined by the power of their keys. Encrypted communications algorithms and key managerial practices are always helpful in providing data secrecy, identification, and reliability while lowering system overheads. The longer the key, the more time it takes to crack the code,

and the attacker have a more challenging time detecting the cryptographic method Kumar, T., & Chauhan, S. (2018).

This link has been heavily utilized, giving rise to enough chaos-based encryption. And it is feasible to construct safe chaos-based cryptosystems; several papers have been published over the years demonstrating the safety and performance flaws of different cryptographic systems. In general, chaos-based cryptosystems may be split into two types: those that use chaotic synchronization and those that function in the stochastic process domain. According to the cryptographic security requirements, the broader population is susceptible due to its nature (Arroyo et al., 2017). The main issue with using such measures to judge cybersecurity is that they will be only evaluated on encoded Images and therefore do not highlight attackers who use the information of the encryption scheme throughout their attack. Indeed, passing these criteria is a necessary but not sufficient requirement for a safe system.

Furthermore, many of these tests lack a specific (statistical) judgment criterion for determining whether or not an encryption algorithm has succeeded. In most situations, it is obvious what the maximum/optimal value is; however, it needs to be more clear under what criteria an encryption technique meets the assessment (Preishuber et al., 2018). Selective area-based Image encryption, in particular, is an efficient and quicker approach to solving this problem. We don't want to secure all the data, especially when critical speed is. In the case of a bank cheque/draft, for example, only the company's seal, signatory, and quantity must be secure.

Likewise, we only had to encrypt a part of the image inside the context of health photos, army Images, aerial photographs, and remuneration Khan, J. S., & Ahmad, J. (2019). Because of the intrinsic randomness of chaotic systems, the private keys created are unpredictable and hard to estimate, making them incredibly resistant to security assaults.

Although several research studies have used chaos and cryptography to develop secure algorithms, the bulk of those papers does not appear appropriate for users that use numeric perceptual information as input. Because of this restriction, the work presented in this study focuses on encoding quantitative data stream values utilizing chaotic encryption methods Nesa et al., (2019). Chaotic encryption uses variations created by chaos networks to create complexity for decryption; this is an alternate method to utilizing numerical difficulty to encrypt data. The significant benefits of using chaotic over the traditional technique are the ease of development and the flexible key space. The drawback of chaotic cryptosystems so far is their lack of formal verification. Considerable research has been done to make the chaotic cryptosystem dependable and practical Hoang, T. M. (2019).

Encryption is a technique for concealing plaintext to disguise its specific content. The perception of encryption is that it renders a message incomprehensible to all save the intended recipient. Cryptography is the study of the calculation and arithmetic that go into encrypting and decrypting data. Cryptography makes it easier to gather sensitive information or send it through insecure networks while keeping it unreadable by everyone except the intended receiver. This chapter presents a systematic review of chaos-based cryptography techniques and different cryptography algorithms. As a result, this literature analysis provides a clear picture of the research problem and leads to new research ideas for future studies.

3.2. Encryption Algorithms

In symmetric-key encryption, only one secret key is used for both encryption and decryption, and in asymmetric-key encryption, two keys are used Teh, J. S.et. al. (2020), Harba, E. S. I. (2017). It is important to keep passwords and other credentials safe when transmitting files securely, so developers have

developed encryption and permission mechanisms. When passwords are transferred and stored in plaintext, hackers, spy agencies, and malware can access them. Advanced encryption systems minimize this vulnerability by using multiple methods to minimize the risk of revealing unencrypted credentials, as well as ensuring that any data used for verification is of low value to hackers.

3.2.1. Symmetric Key Encryption

Vyakaranal, S., & Kengond, S. (2018) Cryptography uses various methods and algorithms to protect data transmission. Authentication, confidentiality, non-repudiation, and integrity are all cryptography features that prevent unauthorized parties from accessing data. Many cryptographic algorithms are available to securely transmit data, but the method should be reliable, accurate, economical, high-performing, and easy to deploy. Selecting an algorithm that meets the consumer's needs is a critical responsibility. The proposed study considers encryption and decryption time, memory usage, entropy, avalanche effect, and energy usage for symmetric key cryptographic algorithms like DES, AES, and Blowfish using a practical implementation in Java. Instead of theoretical principles, the proposed study emphasizes the practical implementation of algorithms, focusing on the trade-off efficiency in terms of the costs associated with different factors. There has been a discussion of the avalanche impact of algorithms and battery usage. In terms of total performance, AES outperforms every other algorithm.

Symmetric key cryptography is essential for data security in many network protocols such as TLS. Academics have long focused on developing such encryption algorithms, and extensive cryptanalysis work has been conducted to assess their security margins. Cryptanalysis has led the research group to find security issues that can be solved. Recently, a neural network-based autonomous security protection method was proposed by Zhou.L. et al. (2019). A computer constructs the encryption method, which is a neural network, during the training phase in a hostile

arena. This is a radical departure from existing design philosophy, and it has the potential to alter knowledge of how encryption performs and what the scheme's security requirements are. Using numerous statistical models, we evaluate the security of the highlighted system, which is still underutilized in this study. Furthermore, we considerably increase the automatic encryption systems by introducing more powerful opponents. The findings indicated that security systems based on innovative deep-learning methods could play a significant role in upcoming developments.

3.2.2 Asymmetric Key Encryption

Chaudhury, P et al. (2017) In an unsecured network, the RSA algorithm hides and retrieves data. The RSA algorithm has the benefit of increasing accessibility. Private keys are not necessary to be exchanged or made public. In shared-key cryptography, the secret keys must be exchanged because encryption and decryption use the same key. As a result, during data transmission, a hacker could discover the private key. There are numerous drawbacks to the RSA algorithm. In the RSA algorithm, various attacks, such as forward search attacks and common modulus attacks, may occur. The factorization problem and calculation performance are two other drawbacks of RSA cryptography for encryption. We utilize a modified RSA cryptosystem technique named "Asymmetric key based Cryptographic Algorithm employing Four Prime Numbers to Secure Message Communication (ACAFP)" in this research. Four prime numbers are challenging to disintegrate, resulting in greater network effectiveness.

Xu.Q. et al. (2020) proposed a secure asymmetric picture encryption system based on RSA and a hyperchaotic map. Using row and column encryption techniques, the plain image is transformed into a cipher image. In order to improve the robustness of the embedded picture, the secret

image key is converted into ciphertext using the RSA algorithm. The Arnold map transforms and permutes the ciphertext and cipher image is obtained. Cryptographic images (ciphers and key ciphers) are embedded in carrier images (CI) to create secure snaps to achieve both image information security and image visual security at the same time. Hyperchaotic maps' starting stages are changed using plain images, in addition to the RSA keys management method. Furthermore, the encryption approach is suitable for multi-user image communication requiring high security and for transmission of images without a secure channel for key exchange.

3.2.3. Hash Functions

Scholz.D. et al. (2019) P4 establishes a standardized, universal data plane programming method. Payload data processing and specialized cryptographic hash functions are commonly used in secure and resilient communication. We've noticed that the existing P4 objectives need more support for both. As a result, programs and techniques that need authentication codes or hashing patterns resistant to denial-of-service assaults will be unable to be developed. We argue that cryptographic hash functions should be added to P4 targets to enable authentication and resilience. An efficiency evaluation and resource usage analysis was done to determine the practical applicability. Cryptographic hashing can be implemented efficiently, as demonstrated by prototype implementations. We have yet to find a single hash function that performs well on all the systems we've looked into. As a result, to maximize target-specific performance, we recommend a set of hash functions.

Liu.H. et al. (2018) The majority of contemporary symmetric cryptographic techniques are thought to be safe from quantum computer assaults. They offer an adaptive color double-image encryption technique

based on the independent SHA-512 and ODE chaotic system. The double-image is first dispersed using chaotic sequences with bitwise operations, then an algorithm is used to convert hash values into S-Boxes, which replace the pixels of the dispersed double-image. The initial values of the chaotic system in each encryption operation come from a random signal. According to simulation findings, the system is acceptable and effective for color double-image encryption.

3.3. Existing Cryptographic Algorithms

El – Haii.M.et al. (2018) examined the efficiency of various cryptographic algorithms in the Raspberry Pi 3 model B. This research indicates how much overhead a security protocol based on cryptographic primitives might add to a system. Traditional cryptographic techniques may not be suitable for IoT devices with limited resources. The choice of a cryptographic method is mainly driven by a trade-off between security and efficiency or power usage. Security architects must benchmark these cryptographic algorithms when creating protocols and schemes for IoT platforms. The results of the cryptographic algorithms on the Raspberry Pi platform are compared to the effects of an Arduino benchmark.

Regarding power usage, AES is the best symmetric algorithm for Raspberry Pi 3. AES-256 has a throughput of roughly 24.6 percent less than AES-128. Both are energy efficient and have a higher level of security than DES. MD5 and SHA-1 are among the fastest; however, they have security weaknesses and are not recommended for use. ECDH outperforms RSA in key generation and exchange methods.

Regarding digital signatures, ECDSA is superior to RSA and DSA for signing, while RSA is superior to verification. ECDSA outperforms the others on average. In a networked system, employing cryptographic techniques creates an additional overhead owing to network interface fees. The issue isn't with the numerically cryptographic costs but with the

overall protocol deadline, which includes power usage.

Zhou.B. et al. (2017) Cryptography is costlier for these devices due to the extreme power and temporal limits of the "things" in the IoT. A viable approach is custom hardware. However, given the short lifespan of these "things," cryptographic method implementations in devices must be updated frequently. As a result, adaptable, minimal power, and high-efficiency cryptography integrations are crucial. This study assesses the mapping of crypto-engines to Zed board's FPGA, as it can enable more energy-efficient crypto operations and also the ability to improve cryptographic algorithms via re-configuration. Cryptographic engines are linked with the OpenSSL library to use the cipher mode capabilities. According to proposed method, the FPGA-based cryptographic elements use less energy and run faster than the software implementation. Across various cryptographic algorithms, FPGA implementations, compared to software implementations, ranged from 1.5 to 2983 and 1.8 to 4033, respectively.

Abdul Raheem.M. et al. (2020) Various devices are interlinked and engage in various new domains to conduct various activities. The IoT and its uses have enabled numerous restricted and low-resource devices to connect, process data, and make decisions within the network. However, IoT has numerous hurdles and issues, including system energy usage, limited battery capacity, storage size, efficiency costs, and resource limits. Conventional methods are slow regarding data security and can't be utilized for encryption on an IoT platform. As a result, for an IoT-driven setting, this research presents cryptography based on the TEA to improve speed from software than hardware implementation. The proposed approach minimizes encryption time in the IoT platform while maintaining the security-efficiency trade-off. The suggested work is related to recent work on start-ups in terms of memory usage, execution time, and precision. The outcomes indicate that the algorithm is more reliable and effective in an IoT-driven system and more suitable

for data security.

Saha, R., & Geetha, G. (2017). Cryptanalysis examines various combinations of ciphertexts, plaintexts, and random keys; hackers can interpret the keys using differential or analog approaches, depending on the round functions or algorithm subset. Although the past study has focused on the design of various cryptographic operations. This work may use a random function generator for any cryptographic scheme. Due to its randomness, this generator emits a random mix of functions that cannot be traced back. The suggested method gives a random mixture of general Boolean functions utilized in MD5, block cipher, and stream ciphers rather than identifying a specific Boolean function dependent on input variables. Furthermore, cryptographic function modules benefit from randomly choosing variables for a given part. Tests reveal that the functions provided by the suggested generator have decent resilience.

A variety of neural networks and chaos-based pseudorandom sequence generators, as well as a DNA-based chaotic encryption technique, are described by Maddodli et al. (2018). The proposed approach uses a heterogeneous chaotic neural network generator to control pixel position permutation, DNA-based bit replacement, and a novel DNA-based bit permutation. Control parameters and iterations of the chaotic functions are constantly adjusted to enhance the randomness of the generated chaotic sequence. It has been demonstrated that the designed chaotic generator has a high degree of unpredictability through numerous tests, such as autocorrelation and NIST tests. Experimental findings such as pixel correlation coefficients, entropy, NPCR, and UACI provide proof of the proposed chaos-based genetic encryption's efficiency and security.

Cryptographic algorithms are susceptible to cache-timing attacks when implemented on natural systems. Knowledge and validation techniques must be used early in the development cycle to design protected implementations. A method for evaluating NIST's postquantum standardization candidates' resilience to cache-timing attacks is presented by Falcon.A. et al. (2018) . It performs static analysis and detects leakage patterns by tainting sensitive variables across the source code. We utilize it to evaluate the NIST post-quantum cryptography proposals' security. The findings demonstrate that 80% of the tested implementations had one problem, with three submissions having over 1000 reported mistakes a piece. Finally, this in-depth examination of the competitor's security enables us to pinpoint the common issues among candidates and how they may be addressed.

Rodríguez, J. (2019) This paper proposes a symmetric-key text encryption algorithm based on entropy, Genetic Algorithms philosophy, and modular arithmetic. Over a deterministic system, an experimental methodology is utilized to redistribute and modify the factors and stages of the evolutionary algorithm that affect its behavior while performing an evaluation to maximize the outcome. The auxiliary key is encrypted separately from the primary key and is responsible for improving security. The studies are on various font sizes, with the recommended parameters and criteria adjusted to the proper levels. Lastly, a contrast with the cryptographic methods DES, RSA, and AES is shown, revealing characteristics such as processing time, scalability, key size, and so on. It has been shown that the created algorithm is more efficient.

Ilayaraja.M.et al. (2017) When communicating through untrusted media, such as the Internet, cryptography is required. Unauthorized persons can access and modify data as it is transferred from one location to another. In the subject of information security, cryptography is essential. Cryptographic techniques are now employed in various fields to protect data from hackers.

Sato, M., & Matsuo, S. I. (2017) In this paper, we propose a method to apply a similar concept and data structure in a decentralized manner. Blockchain technology creates an unforgeable and decentralized ledger by combining a peer-to-peer network, cryptography, and a consensus process over a dispersed network. All of these technologies are necessary for its security. Compromising underlying cryptographic methods is one of the most fundamental problems with blockchain technology's security. This study demonstrates the impact of underlying cryptography compromise and how to prolong the credibility of blockchain using the ETSI-standard long-term signature mechanism. The technique requires a centralized PKI and a secure time-stamp mechanism. In the event of a hash function compromise, system avoids a hard fork of the original blockchain and enables a smooth separation in the event of a digital signature compromise.

Shankar.K.et al. (2018) Researchers examined various encryption methods based on chaotic systems due to the rapid progress in medical picture encryption. However, with 1-D chaotic cryptosystems, there is a problem: a tiny key space and weak security. This study proposes an alternate security model to tackle this problem. This research looked into highly secure medical images using several subkeys, first by using chaotic logistic and tent maps to generate a couple of subkeys. The security of dissemination and confusion was examined using the chaotic (C-function) process. Various random numbers were developed for each map based on the initial conditions. The grasshopper optimization algorithm with PSNR and correlation coefficient fitness function was presented to determine the best public key for the system. The adaptive technique was used to improve the current proposed model's high-security research compared to existing methodologies. Finally, the proposed strategy's findings were related to present security measures and were discovered to be highly effective.

Bader, A. S., & Sagheer, A. M. (2018) AES is one of many today's cryptographic algorithms developed to protect data confidentiality. The key and the Initial vector are utilized to encrypt the plaintext to the ciphertext in AES-GCM. The Initial vector is used with the key to generating a particular ciphertext. The randomness ratio was measured using NIST statistical functions following the adjustment, and there was a significant increase in the randomness rate in the encoded text acquired using the changed algorithm compared to ciphertext generated using the standard AES GCM.

Agrawal, M., Zhou, J., & Chang, D. (2019). IoT is the technology that allows these embedded devices (made of sensors, actuators, and other components) to communicate over the Internet to share data, optimize operations, and monitor equipment to benefit the industry, economy, and end users. These procedures usually involve sensitive or essential information that must be kept safe from the outside world. As a result, their safety is a top priority. However, resource constraints in computational power, storage capacity, chip size, and energy consumption are the key obstacles to ensuring security for these devices. Because of these devices' low capabilities, Lightweight Cryptography must be used (LWC). Lightweight cryptography is a branch of cryptography that deals with cryptographic algorithms specifically developed for use in limited situations, such as contactless smart cards, sensors, RFID tags, embedded systems, and healthcare devices. An existing lightweight authenticated encryption technique is presented in this paper. We polled 17 lightweight AE schemes, 9 currently competing in the CAESAR competition.

Noura.H. et al. (2018) With the exponential expansion of IoT devices, security and privacy problems have surfaced as major concerns that could jeopardize their use in various data-sensitive benefits.

Conventional cryptographic algorithms employ a static structure that necessitates multiple computation cycles, resulting in significant complexity regarding execution time and computer services. Furthermore, the problem is exacerbated when handling multimedia data because the accompanying algorithms have strict QoS requirements. A dynamic key is created in this approach, which is then utilized to develop robust substitution tables, an active permutation table, and pseudorandom matrices. While preserving high unpredictability and security, this dynamic cipher structure reduces the number of rounds. Furthermore, the suggested encryption scheme is adaptable, as the dimensions of the input matrix can be chosen to match the memory capacity of the devices. Extensive security testing demonstrated the cipher's resistance to a variety of assaults.

Kumar, T. M., & Karthigaikumar, P. (2018). AES is a cryptographic technique that encrypts and decrypts 128-bit data blocks using varying key sizes in a symmetric non-Feistel block cipher (128, 192, 256). The number of rounds of operations and subkeys created from the primary key varies depending on the block sizes. The subkey generation architecture is changed in this suggested technique to speed up the process of producing subkeys. The recommended design is simulated and integrated into an FPGA Virtex. The implementation of a novel suggested method for the encryption and decryption of ECG signals for secure communication is discussed in this study. Iqbal, A., & Iqbal, T. (2018). Modern power systems are complicated by the widespread use of renewable energy sources with their distributed generation and control. The main goal of this network is to create an economical, secure, and authentic communication system between the SCADA unit and the Remote End Devices. The challenges of security and authenticity for wireless communication are discussed in this study. To secure wireless communication for micro-grids, the AES algorithm has been implemented on the ESP32 with the LoRa module, and authenticity has been accomplished by producing new Message Authentication Codes.

Mezher A. E., (2018). Security is one of the most essential concerns for corporations, banks, organizations, and government facilities when sharing information and data. RSA is a public cryptographic technique that was created with the aim of data encryption and authentication. Eliminating key exchange in the encryption and decryption procedures is the fundamental reason; hence asymmetric key algorithms like RSA are more secure. The key length is only used in the standard RSA algorithm to safeguard computers. However, the RSA key is occasionally compromised due to the advancement of computer hardware like high-speed processors. RSA developers have enhanced the key length regularly to ensure that systems protected by the RSA maintain a high level of security and privacy. A method for strengthening the RSA algorithm by using several keys has been proposed and implemented in this work.

3.4. Image Encryption

Encryption is a hidden process of data when it is transmitted across a network. Images' security differs from the security of texts, for example, the ability to provide mass information and the interaction between the pixels. This is why the traditional technique for encrypting images is no longer feasible (Sekar et al., 2020). The only method to ensure safety is to prevent the attackers from knowing that important information is available in your transaction. Several approaches for image security have been explored. Graphic encryption and visual data are utilized to encrypt (Karthick et al., 2018). The graphic shows that data transmitted in the public domain are highly vulnerable to attack. Data should thus be converted via encryption during transmission into a safe format. Image encryption improves digital image security and is a key input in various applications such as video conferencing, pharmacy applications, and naval image communications (Kumari et al., 2017).

Image encryption is the most significant way of ensuring image security. On the other hand, the time interval in which the image is transferred from the sender to the receiver is critical since if the delay exceeds the threshold, irreversible harm may occur. As a result, to satisfy the necessary criteria, the encryption method utilized in such applications must provide high security while still being fast. As a result, none of the existing Image encryption methods are suitable for these applications Arab et al., (2019). For text encryption, several standard encryption methods have been suggested. Because of the enormous volume, the correlation between neighboring pixels, and the redundancy of visual data, these methods have inadequate security and a long encryption time. As a result, these techniques are unsuitable for Image encryption. Furthermore, because of the characteristics mentioned above of visual data, these Image encryption methods are vulnerable to statistical, differential, and other assaults and frequently fail Norouzi et al., (2014).

Sometimes encryption is utilized to increase the uncertainty of data inside the image. In addition to Images, several text algorithms are used in recognition of scripts by segmentation, and algorithms are used on voices with multi-speaking speakers to standardize vocal tract length and automated speaking recognition (Mohammad et al., 2107). Conventional cryptographic techniques like RSA, AES, and DES are not suited to encrypt images. Recently, research organizations worldwide have investigated many types of Image encryption methods based on optical, chaotic systems, transforming Spectral, cellular, waving, magic square, etc. (Jithin et al., 2020). This approach was used to develop an iterative architecture to improve cryptosystem security. The suggested cross-image pixel scrambling technique confided to produce a consistent pixel dispersion across input Images provides images for the input (Murugan & KarthigaiKumar, 2018). The encryption technique is used for Transforming Arnold (AT), beta map, NSCT, and differential development. Initially, an Image with pixels can produce a scrambled

image with AT. The idea then gets broken down into sub-bands using the NSCT (Kaur & Kumar, 2018).

A safe data transfer route over multiple communications channels necessitates encrypting confidential information delivered via the Internet or cellular networks as multimedia. Data transferred over these channels should be anchored to prevent unauthorized access, modification, or destruction. Text, Images, music, video, three-dimensional (3D), and other forms of data are transferred over the channels for various applications. On the other hand, the security of those photographs is a problem. Security is an essential aspect of image exchange since it protects the image from unwanted access and alteration Ramasamy et al., (2017). To produce encryption, chaotic maps split an Image into two phases: diffusion and permutation. Cryptosystem engineers can use permutation and diffusion in real-time to achieve considerable computational security. It illustrates the chaotic world of visual encryption technology in action. The recombination or distraction phase shuffles the image in a circular pattern based on a pseudorandom sequence. After that, the jumbled image is divided into numerous blocks during the diffusion phase. A block header is chosen to install the chaotic maps. As a result, the key sequence is dependent on the image provided.

Nowadays, digital image security has become more essential than ever because of the fast Internet development in the digital world. There were several alternative ways for encrypting images. Due to some intrinsic Image properties such as high redundancy, large data capacity, and a strong connection between neighboring pixels, the encryption of images is distinct from the standard encryption (Noshadian et al., 2018). The chaotic maps are the most incredible option for cryptography methods. We need a system that produces a genuinely random number, and pixels are encrypted based on these random numbers as the central concept underlying Image encryption (Parvaz & Zarebnia, 2018). A chaotic system is dynamic with sophisticated pseudo-randomness and

excellent confusion laws.

It is susceptible to starting circumstances and control parameters and is thus magnified exponentially by any little initial deviation. The nonlinear system model, control variables, and beginning conditions are also determinable. At the same time. Several good encryption algorithms because of the features of a chaotic system with unpredictability, unpredictability, ease, and high sensitivities of the starting values (Chai et al., 2017). The chaotic system for encryption consists of confusion and diffusion in two stages. Confusion is the period in which the pixel location is scrambled, and the value of the pixels is not changed. A diffusion stage is intended to change the estimate of each pixel throughout the Image (Suneja et al., 2019). The fundamental idea of chaotic-based encryption is to utilize dynamical technology to achieve a sort of semi-series of numbers that may be used to encrypt images (Arab et al., 2019). The following Block diagram represents the strategies of Chaotic Image Encryption

An encryption system based on chaos was proposed to lessen the limitations of existing systems. In the encryption of digital Images and high computing power for huge Images, the traditional AES, DES, IDEA, and RSA encryption systems show disadvantages and weaknesses (Kumar & Chauhan, 2018). Furthermore, in this method, we modified the notion of partial image pixel encryption instead of full encryption to allow the confusion of the intruder with the partially encrypted image in cases of arrack. There are numerous encryption methods for the encryption of text and Image data. Therefore, researchers' primary problems are ensuring that an Image is safe and secret and reducing the time required to compute the encryption method Khaitan S. et al., (2021).

In the medical field, encryption is the technique to encode images or data to be accepted. The specific disease from the manipulated digital medical image is difficult to diagnose in the medical diagnostic. In the

case of conventional methods, the calculation time for encrypting Image data is relatively high (Akkasaligar & Biradar, 2020). Based on this analysis, we present a novel technique for the dynamical key selection of chaos-based Image encryption in this work. This new algorithm can meet the security needs we anticipated and overcome the defects in most cracked algorithms through the three-part improvement. They plan to leverage the key distribution notion in encryption techniques, ensuring that the created trapdoors can only be used to search through accessible encrypted messages supplied by a specific data transmitter.

Even if the opponent (insider or outsider) has access to the zipper, they and then it can produce any ciphertext that can be examined by the acquired trapdoor, so the phrase-matching attack can be used Noroozi et al., (2018). In addition to encryption techniques, cryptographic algorithms are a study field used to decrypt keys or target block cipher. Cryptanalysis may also uncover flaws in cryptographic algorithms and aid in the advancement of cryptography. Furthermore, the decryption process can prevent dangerous encryption methods in actual transactions. Recent crypto algorithms studies reveal that several chaos-based Image encryption methods are unsafe Belazi et al., (2017).

The encryption techniques should be complicated enough to manage this while successfully implementing this algorithm, whether in application-specific computer systems. The type of chaotic system utilized, the keyspace, and the complexity of the key generation procedure all affect the encryption algorithm's security. Time and frequency dynamic systems have a beneficial effect on increasing the difficulty of chaos-based data encryption, but chaotic maps are easy to implement in hardware Valli, D., & Ganesan, K. (2017). Because the hardware realization of the Ikeda DDE utilizing the field-programmable arrangement was investigated in previous works, the lag time system described by the Ikeda delay differential equation (DDE) was chosen for the encryption procedure. The performance study of video encryption

utilizing these two distinct chaotic methods depends on the chaotic map. The effective delay system will aid us in determining which scheme is best for real-time applications in terms of safety and operational convenience Tutueva et al., (2021).

The analog technique is based on the chaos synchronization principle, which states that the sender and receiver synchronize chaotic communication impulses. Several studies in this area have been mentioned, including one that uses a nonlinear model for encryption and decryption and proposes a scheme is presented chaotic ciphertext and modulation, as well as one that incorporates a Lorenz-like system to cryptographic speech and mentioned some chaos-based technologies to enhance wireless network protection Sharif et al., (2020).

3.5. Chaos-Based Cryptography

Nardo.L. G et al. (2021) Over the last few years, picture encryption techniques based on chaos have been widely used. Many concerns have been investigated, including the deterioration of chaotic digital systems, and many viable solutions have been offered. On the other hand, the influence of finite precision in various hardware and software has received little consideration. We demonstrated in this paper that a limited accuracy defect can result in multiple cipher images on numerous devices. We propose a cryptosystem on the Galois field theory and chaotic logistic map to solve this challenge. The strategy has passed the ENT test suite as well as various cyberattacks. It also has a remarkable key space of up to 2409624096. Using multiple digital equipment's, benchmark photos have been successfully encrypted and decrypted.

The, J. S., Alawida, M., & Sii, Y. C. (2020) Since its introduction, chaos-based cryptography has become a frequently discussed topic. Despite many contributions to the field, its real-world applications are limited compared to traditional cryptography. As they exhibit desired features like pseudo randomness, complexity, and parameter variations, chaotic maps have been employed in developing cryptosystems. Even though these features are equivalent to cryptographic requirements, cryptosystems based on chaos theory are difficult to understand, inefficient, and inconsistent. We address specific issues that prevent chaos-based cryptosystems from being used in practical applications. We show that contemporary research published in renowned publications does not address these issues and remains purely academic. We also conduct experiments to illustrate some digital chaos implementation challenges that must be considered while developing chaos-based algorithms. Following that, we go over several potential strategies for resolving these issues.

Gatta, M. T., & Abd Al-Latif, S. T. (2018) Due to the apparent rapid advancement of telecommunication and networking technology, telemedicine has grown in popularity, involving the storage and transmission of medical pictures and related data, posing a security risk. Because medical photographs play an important role in people's healthcare organizations, this research proposes a strategy for ensuring their security. The fundamental idea behind this study is to use a chaotic sequence to create a practical encryption approach that allows for high-quality reconstruction of the actual image from the encrypted image with minimal content distortion and has no impact on human treatment and diagnosis. Using several statistical measures and a strong connection between the original and the decrypted image, experimental findings show that the proposed method is effective.

A number of alternatives have been developed for encrypting image and video data using chaos-based techniques in recent years. While every algorithm is subjected to a more or less rigorous experimental security study before being released. Computational effort and security benefits are two of the most common reasons for choosing chaos-based picture encryption over standard cryptographic encryption. Several statistical techniques routinely employed to analyze the security of chaos-based encryption schemes are shown to be insufficient for security analysis. It was achieved by building apparently insecure encryption schemes and showing that they pass numerous tests in an experimental setting Preishuber, M. et al. (2018). To summarize, these tests can only provide a necessary security requirement. As a result of this article, various security studies in related work are called into question, and approaches for assessing the security of chaos-based encryption systems must be completely rethought.

Nesa, N., Ghosh, T., & Banerjee, I. (2019) This work presents a new Logarithmic Chaotic Map (LCM) based on the well-known quadratic map. The proposed map LCM's chaotic dynamics are thoroughly explored, and its chaotic qualities are determined to be superior to those of other maps. In particular, a unique LCM-based encryption method is developed. The suggested LCM is based on the quadratic map but has better chaotic qualities like a bifurcation map, Lyapunov factors, and sensitivity to beginning circumstances. Furthermore, the map's pseudorandom output was tested against the NIST randomness test suite. As it uses extremely little space, the suggested PRNG has been used to encrypt sensor data in scenarios like the IoT. The performance of algorithms, and their resilience to security threats, are demonstrated by research observations and security analyses. The chaotic output created by LCM passed all 15 statistical tests conducted by the NIST, proving its randomness. The suggested encryption technique has been proven highly resilient to security threats and is especially suitable for encrypting

numeric sensor data values, ideally for IoT applications.

Santos.T, A et al., (2019). This work investigates the use of chaotic systems for encrypting and communicating images between various devices. Using two devices, the Cubic Map was replicated with identical settings to produce an encryption key. While both devices are floating-point compatible, their simulations and encryption keys differ. Therefore, existing chaos-based encryption techniques can be considered particular examples of computational arithmetic properties whose properties are similar to those of devices.

Lawn, M. (2017) The logistic map is often employed in chaos-based cryptography. Its qualities do not make it possible to build secure encryption techniques. As a result, the paper's scope suggests generalizing the logistic map using a family of chaotic maps. The distribution of the iterative variable and the Lyapunov exponent is examined in the next phase. The outcome shows that the investigated model can replace a traditional logistic map in chaotic cryptography applications. According to the results, the researched model has significantly superior qualities to a standard logistic map, like a range of permissible factors, a Lyapunov exponent, and a balanced distribution of the iterative variables. The features of the analyzed function permit its successful use from the perspective of chaos theory-based cryptography. The examined model, on the other hand, combines the simplicity of its conventional counterpart. This led to the generalized form of a logistic map being used in cryptography applications instead of the original.

Garcia-Bosque et.al. (2018) proposes a PRNG based on the logistic map. By continuously altering the chaotic system's parameters, the proposed approach prevents the system from falling into short-period orbits and enhances its randomness. A Virtex 7 FPGA with a 32-bit fixed point accuracy was used to create this PRNG with 510 lookup tables and

120 registers. NIST's randomness tests have shown that the suggested algorithm's sequences are random. Compared to a raw 32-bit logistic map, it is demonstrated that by adding only 16 percent more LUTs, the suggested PRNG achieves significantly greater unpredictability, raising the NIST passing rate. There are significant improvements in resources and randomness regarding the proposed bitwise dynamical PRNG compared to earlier chaos-based realizations.

Mail, M.S. et al. (2020) A new chaos-based affine transformation generation approach based on rotational matrices is presented. Using chaotic logistic maps, rotating matrices are constructed under specific design conditions using their nonlinear trajectories. Thus, the intrinsic logic of the affine transformation is to use chaos to complete key-value S-boxes that are as secure as AES. Chaotic sequences are tested for randomness with the NIST Statistical Assessment Suite, which validates sequences for S-box design. Researchers found that suggested key-based dynamic S-boxes have near-optimal cryptographic features, making them as effective as AES S-boxes.

The, J. S., Tan, K., & Alawida, M. In order to create hash functions, chaotic maps are used because their properties correspond to cryptographic requirements. To implement these maps with high computational complexity, a floating-point representation is typically used. Their interoperability issues and binary analysis also make them difficult to understand. Because of these flaws, chaos-based encryption is not widely accepted for practical use. By using fixed point representation and a chaos-based hash function, this study solves these issues. A Merkle-Damgård construction is used for solid security considerations, along with a generalized Feistel structure. According to a security study, the suggested hash function exhibits statistical properties such as diffusion, confusion, and distribution. In terms of performance, the proposed hash function outperforms existing chaos-based hash functions, making it a feasible hash function for practical implementation.

According to Antonik et al. (2018), reservoir computing can be used to teach dynamical systems to mimic each other. In this paper, we demonstrate that reservoir computers can sufficiently mimic the chaotic system's attractor to display chaos synchronization. As a result, the chaotic system synchronizes with the trained reservoir computer that is weakly influenced by it. To demonstrate this phenomenon, Mackey-Glass and Lorenz systems are used. A chaos cryptosystem based on Mackey-Glass is then used to crack chaos-based cryptography using trained reservoir computers.

Cavusoglu, Ü., et al. (2018) In this research, a secure and fast picture encryption technique based on chaos-based S-BOX is devised. A novel chaotic system for producing S-Box and an image encryption method has been developed. The novel chaotic system is used to create a chaos-based random number generator. The generated random numbers are then subjected to NIST tests to ensure they are genuinely random. A novel S-Box design method is devised, and performance tests are conducted to construct a chaos-based S-Box for use in encryption algorithms. The next stage is to go through the details of the newly designed S-Box-based picture encryption technique. Finally, the application of image encryption is carried out. Security analyses are carried out to demonstrate the strength of the encryption process. The suggested picture encryption technique is secure and fast for image encryption applications, according to test results.

Arroyo, D., Hernandez, F., & Orúe, A. B. (2017). Over the last twenty years, using synchronization research to explain new cryptosystems has been a significant issue. We examine an existing idea in this area. The fundamental difficulties of the software implementation of chaos-based systems that rely on synchronization theory are identified. Furthermore, we demonstrate that the cryptosystem under consideration has substantial security flaws that necessitate a significant loss in the key space. Moreover, the tools and methods used in this paper can be precious in evaluating and improving existing contributions in chaotic cryptography

and guiding the creation of new ideas. In response to this last point, it's important to remember that the computer implementation of chaos is influenced by finite precision issues, effectively annihilating the relation between chaos and cryptography. If we use continuous-time chaotic systems to build the encryption system, we'll have to cope with mathematical optimization approaches and floating-point processing challenges.

Taha. M.A. et al. (2017) utilized a chaotic generator to develop an efficient stream cipher cryptosystem. In addition to the Key-setup and Initial vector setup, the chaotic generator also consists of a nonvolatile memory and an output function. Several delays and two or three recursive filters make the internal state an area of cryptographical difficulty. Each recursive filter uses a linear feedback shift register for perturbation. Recursive filters 1 and 2 use discrete piecewise linear chaotic maps and discrete skew tent maps, respectively. In terms of security and execution speed, the proposed stream ciphers perform admirably. The proposed system's robustness against known cryptographic and statistical attacks is demonstrated by experimental results.

Kumar, T., & Chauhan, S. Textual and visual data items are becoming increasingly prevalent as the use of digital technology continues to grow. To safely communicate this data, many users use picture encryption strategies. Key generation with MASK and encryption with Chaos-based methods. MASK's primary duty is to generate the encryption and decryption keys. In order to encrypt with 16 rounds, we used a permutation-substitution chaos based on the MASK-256 key. The approach also uses partial encryption of image pixels rather than full encryption so that intruders can be confused by a half-encrypted image in the event of an attack. Different image samples of various sizes were considered in this approach.

Kaur, G., Agarwal, R., & Patidar, V. (2020). A robust yet simple and

efficient method for 2D picture encryption is proposed in this research. A major obstacle to encrypting data is the absence of randomness in optical transform domains, leading to blind decryption. The way of producing several transform orders is what makes this work unique. To have numerous transform orders in both dimensions, two PWLCM are employed. With the multiple-order vectors created, a fractional Fourier transform is obtained. The transform domain data is jumbled to improve security with another integrated chaotic map. The chaotic maps in the study are chosen while keeping in mind the limits of 1D chaotic maps. Because 1D chaotic maps lack periodic windows, the PWLCM, and an integrated chaotic map are resilient. It provides a fast and real-time means of storing complex transform coefficients using a reality-preserving method. The findings and results of the experiments show that the suggested technique is very random in the encrypted domain and has outstanding sensitivity.

Kaur, G., Singh, K., & Gill, H. S. (2021) Multiple chaotic maps and cryptographic algorithms are employed to encrypt speech signals. A cubic map fragments and jumbles the incoming call into four parts. In order to render scrambled signals invulnerable to attacks, different 1D chaotic maps are used, including cubic, logistic, skew-tent, and quadratic maps. All chaotic maps are used to create encryption at the transmitter end, but the reverse is done at the receiver end. To safeguard the various parameters of all chaotic approaches, the blowfish algorithm is used with a private key. Additional security is provided by the blowfish key between two ends and the hashing algorithm. An authentication and verification of chaotic maps should be based on the computed message of the secure hash algorithm. Signal-to-noise rate, specific power, peak signal-to-noise ratio, and correlation tests were conducted on an 8 kHz protected speech signal to determine the efficiency of the suggested system. The encryption design is validated and adheres to higher security standards as a result of numerous statistical analyses and tests of the adversary model, making it as insusceptible to intruder attacks as possible.

Hoang, T. M. (2019) The approach of dynamics perturbation to the Logistic map is used to develop a new chaos-based picture cryptosystem in this paper. The concern is typically performed during encryption and decryption by modifying the number of its process parameters in the bit level after each iteration. As a result, the Logistic map's dynamics become non-stationary, which aids in the resistance against statistical attacks. Furthermore, the vital area has been dramatically extended. It is proposed that bit distribution balancing be used to improve the statistical features of ciphertext. The simulation results are compared to those in other recently published papers to demonstrate the usefulness of the proposed cryptosystem.

Tuna, M. (2020). A novel, high-speed, real-time, and robust chaos-based PRNG design is presented in this paper using artificial neural network (ANN)-based 2D chaotic oscillator and ring oscillator frameworks. ANN-based 2D chaotic oscillators have been used to generate four different resilient PRNGs using different TanSig activation functions. Based on the IEEE-754-1985 number standard, the designs were programmed in VHDL. An FPGA device based on Virtex-6 was designed using Xilinx ISE Design Tools. A PRNG's maximum operational frequency varies from 184 to 241 MHz. PRNG bit streams generating 1 Mbit of random data were tested for randomness using NIST-800-22. The proposed PRNGs created utilizing the Elliott-93, and Cordic-LUT techniques have successfully passed all NIST tests and have a bit rate of 241 Mbps out of four proposed PRNGs. The hybrid chaos-based PRNG structures suggested in recent years were compared to similar studies published in recent years.

Halagali, B. P., & Desai, V. V. (2018). Cryptography is a developing technology that is critical for network security. It is a system that ensures message or data secrecy (i.e., secure data transmission). The most basic mode of communication is the cellular network. The suggested study proposes a new cryptosystem based on coupling chaos theory's Lorenz

equations with the KASUMI block cipher. Random numbers are significant in cryptography, as well as many other domains. Random numbers are generated utilizing Lorenz equations in proposed study, which is based on chaos theory. The unpredictability of generated random numbers is checked using the NIST test suite. The KASUMI block cipher is being studied for data encryption. Three characteristics, balanced output, hamming distance, and Avalanche effect, are used to evaluate the performance of encrypted data obtained using the suggested method. An experimental result provides the best randomness, resulting in better cryptosystem performance.

Cao, J., & Chugh, R. (2018). The standard logistic map has a prominent place in the dynamics of chaos theory and in different applications of science, such as a discrete traffic flow model, picture encryption in cryptography, secure communication, and weather forecasting, thanks to the crucial role of discrete chaos. This discrete chaos is traditionally managed by a single parameter utilizing Picard orbit, a one-step feedback technique. The chaotic features of the logistic map, like period-doubling, period-3 window, and Lyapunov exponent, are examined using the Mann orbit (superior orbit) in this article. Analytical and experimental results are presented by concluding remarks and a few counter instances. The map has improved chaotic qualities due to the extra degree of freedom in parameters, improving dynamical events' performance. Furthermore, this research presents an improved discrete traffic control model based on chaos. Surprisingly, the new parameter in Mann orbit acts as a process parameter, improving the traffic model's performance.

Murillo-Escobar, M. A et al. (2019) As the diffusion effect in the AES algorithm is poor, chaos-based cryptosystems are currently being developed to offer confidentiality for digital images. Recent chaos-based picture encryption methods are vulnerable to fundamental security analysis, making them unsuitable for various applications. This research

provides an integrated analytical methodology for chaos-based image cryptosystems, including thorough security analysis, cost, performance, and algorithm and implementation. Based on 20 points of research, the proposed guideline can help new cryptography inventors comprehensively examine new algorithms. The future security and efficiency comparisons of methods should be more uniform. In addition, we discuss how to increase the overall cryptosystem's security by using digital chaos, validating chaos, and defining keys. The suggested guideline does not ensure safety and has no intention of restricting the freedom to conduct new research. However, it establishes a solid foundation for critical analysis of chaos-based image cryptosystems as a viable technique to increase security for the first time in the literature.

Özkaynak, F. (2018). Chaos-based in the last two decades, cryptology has become the popular design methodology for new encryption algorithms. However, many suggestions have been found vulnerable to well-known assaults. On the other hand, the security of proposals cannot be demonstrated. For the security study of new proposals, a roadmap is required. This research seeks to solve this flaw. Many chaos-based picture encryption techniques previously published in nonlinear dynamics are not as secure as described, according to analysis and test results, despite passing various statistical and randomness tests. To tackle these issues, a checklist has been presented. The suggested checklist's applications for multiple algorithms have been demonstrated. The recommended list is a solid place to start for researchers interested in working on chaos-based cryptography.

Raza, S. F., & Satpute, V. (2019). In the last few years, much effort has been put into developing image encryption techniques. Image encryption necessitates the management of enormous amounts of data, necessitating a computationally efficient approach. Against traditional encryption techniques, chaos-based picture encryption has been proposed. A cryptosystem based on chaotic systems is computationally efficient for

photo encryption. Using a 3D puzzle and chaos for further diffusion and confusion, this work presents a new bit permutation technique in picture encryption. The proposed encryption algorithm is put to the test for security and validity using a variety of methods. The testing results show that the suggested algorithm is safe from statistical and differential attacks.

Kumar, V., & Girdhar, A. (2021). The suggested method uses DNA cryptography fundamentals, the Lorenz and Rossler chaotic system, and a 2D logistic map to encrypt RGB images. The three channels of test images are encrypted using the Lorenz and Rossler chaotic system at the pixel level during the diffusion phase. In the confusion phase, a 2D logistic map is utilized to execute a bitwise chaotic process on the bit level's diffused red, green, and blue channels. The proposed method was tested on test photos and was very efficient at encrypting color images.

Karthick, S. et al. (2018). Image encryption, also known as secure image processing, is a method of manipulating images that protects them from being stolen or damaged. It is vital to ensure security for images such as medical, military, and other sensitive information. In this way, this study aims to develop a better technique for picture data prevention and security enhancement. Qua-ternion is a type of number notation that combines scalar and vector elements. Quaternion rotation is used in picture encryption to improve performance and security. The efficiency of the suggested system is compared to that of the traditional quaternion technique, which is implemented using the MATLAB working environment. Based on a performance comparison, the proposed method outperformed the competition regarding the correlation coefficient, avalanche effect, processing speed, normalized correlation, and histogram.

Belize.A. (2017) This paper presents a novel chaos-based partial picture encryption technique using S-boxes generated by chaotic systems

and Linear Fractional Transforms. In the Lifting-Wavelet Transform frequency domain, it encrypts sensitive data using a combination of chaotic maps and an S-box. A three-phase encryption scheme is proposed to achieve confusion and diffusion features: block permutation, substitution, and diffusion. Rather than using fixed keys like in other applications, dynamic keys were used to ensure that no attack could be conducted. A chaotic map and LFT were combined to create a new S-box that ensures strong confidentiality. In addition, the hybrid S-box and chaotic systems enhanced overall encryption performance and increased the key space required to resist brute force attacks. In order to assess the security and efficiency of the suggested approach, extensive tests were conducted.

In order to ensure secure network transmission of digital images, Sasikaladevi et al. (2020) explain the high demand for digital images across all domains. Hybrid multi-layered hyper-chaotic hyper-elliptic curve-based image encryption has been proposed for use in medical and forensic applications. Chaos sequences are constructed in the first layer using hyper-chaotic DNA encoding. A substitution permutation increases confusion diffusion, which improves the security of a cryptosystem. Genus-2 Hyper Elliptic Curve Cryptography is used for the second layer, emphasizing the spatial domain for encryption. HHH is a hybrid system since it mixes symmetric and asymmetric cryptosystems. Using conventional benchmark images, the experimental results confirm optimum measures of PSNR, entropy, NPCR, UACI, and MSE, so this strategy can benefit all types of signals processing mechanisms, including color images that are vulnerable to signal processing.

Digital image security has become a significant concern with the rapid advancement of information sciences. On the other hand, many current picture encryption systems use complex algorithms and functions, resulting in substantial calculating power consumption, which is incompatible with mobile devices. In order to resolve this issue, visual cryptography, SHA-512, and a one-time password are combined into a

system for encrypting color images. Based on visual cryptography, the encryption process operates by splitting the plain image into many pieces and encrypting them for transmission. Several XOR methods are essential for picture decryption, dramatically reducing processing complexity. Furthermore, the SHA-512 algorithm and a one-time password are used to enhance the confidentiality of cipher keys and minimize the chances of incorrect cipher images being intercepted. The experiment results show that the suggested approach provides excellent security while consuming little computational effort.

Li et al. (2020) An efficient and safe chaos-based color picture encryption system employing bit-level permutation is suggested to protect the security of digital images during transmission and storage. Symmetric cryptography encompasses in suggested picture encryption algorithm. In this case, we evaluate the connection between three color components rather than processing them individually. We suggest a three-part bit-level permutation technique that includes substituting plain-image-related rows and columns, pixel-level roll shift, and bit-level cyclic shift. We use plain-image information to build a control sequence using a skew tent system. This procedure assures that the correlation between three color elements can be destroyed entirely, and cryptosystem has sufficient plain-image sensitivity to withstand a differential attack. Using a Rucklidge system, we have a fully bit-level permutation controlled by two sequences. Test findings suggest that the proposed approach has strong security and speed benefits compared to other efforts.

Ahmad.M.et al. (2021) To secure color images during transmission, an image cryptosystem is investigated. The cryptosystem uses synchronized 4D hyperchaotic systems based on the permutation-only cipher. The cryptosystem has proven reliable in terms of ciphertext statistical encryption quality. This study examines the security of this image cryptosystem in terms of flaws and attack resistance. The security research reveals that the cryptosystem has several major security flaws

and cannot protect encrypted data. The inherent flaws are highlighted to substantiate the allegation, and an attack process is presented to illustrate that the cryptosystem can be broken using the proposed cryptanalysis. Without knowing the secret key, the attacker can retrieve the entire plaintext picture from the ciphertext image. To prove the success of cryptanalysis, computer simulations are used. The image cryptosystem is unsafe for use in real picture-based secure wireless communication applications. As a solution, this work proposes security modifications and an updated cryptosystem to make it totally resistant to the cryptanalytic assaults described previously and other forms of cryptanalytic attacks, as well as to improve plain image sensitivity and statistical encryption strength.

Bansal.R. et al. (2017) Many experts are concerned about the confidentiality of images during data transmission, and as a result, numerous approaches for image encryption have been proposed. Image encryption is considered adequate if it has an ample key space sensitive to the initial conditions. Furthermore, the technique should have a suitable balance of computational speed, security, and time complexity. A new image encryption system based on chaotic maps and the Vigenère Scheme is proposed in this study. There is only one round in this method, and it consists of stages: diffusion and confusion. Forward diffusion, Vigenère scheme matching, and backward diffusion are the three steps of the first step. To exchange pixel locations in the later phase, position permutation utilizing a chaotic map is used. The proposed strategies are implemented in Matlab-2015, and their efficacy is evaluated using a variety of performance indicators.

Riffi, S et al. (2021) In this paper, we extract the region of interest from a facial image to reduce its size by disregarding the undesirable section to secure its exchange. A sampled quantum encryption circuit

based on a quantum-gate sequence in the MATHEMATICA quantum package is then used to store it following the GNEQR representation. Quantum image processing proposes a scrambling strategy based on perturbing pixel locations per block rather than their values using GNEQR representations as a suggested scrambling method. Compared to recent work, a statistical investigation is performed to demonstrate encryption model's mean robustness.

Zhang.X. et al. (2017) Recently, a hyper-chaotic system and dynamic S-box image encryption technique were suggested. The encryption algorithm's core idea is to permute and replace plain-image pixels using key streams produced by a hyper-chaotic system. This research examines the encryption technique's potential security issues and suggests a chosen-plaintext attack to crack the encryption system. The chosen-plaintext attack shows that the encryption technique is unsafe and unsuitable for picture-secure communications. Based on the cryptanalysis results, an enhanced approach addresses Liu's algorithm's potential security flaw. Modifications to the original scheme not only inherit their virtues, but also outperform them in experiments on statistics, plaintext sensitivity, and key sensitivity.

Lu.Q.et al. (2020) This work provides a chaotic S-Box-based picture encryption technique that is both efficient and secure. Using a chosen-plaintext attack, we broke the cryptosystem by cryptanalysis, a multiple chaotic S-Boxes-based picture encryption technique (CPA). Second, we suggest a picture encryption approach based on a single S-Box and a novel compound chaotic map. A new discrete compound chaotic system, the LSS, is indicated in the new scheme, which has a more extensive chaotic range and improved chaotic features. In addition, LSS is used to create a new S-Box with acceptable cryptographic performance. The new picture encryption technique is based on the S-Box and the chaotic key stream, consisting of permutation substitution. The plaintext image content is linked to the permutation and substitution key sequences, allowing the

cryptosystem to withstand CPA. The suggested picture encryption scheme's efficiency was confirmed by simulation results and security research. The novel approach, in particular, exhibits clear efficiency benefits, indicating that it has more significant potential in real-time image encryption.

Luo.Y. et al. (2019) An image encryption process centered on double chaotic systems is suggested in this study. Due to the restricted chaotic range and vulnerability of a single chaotic map, we use a 2D Baker chaotic map to manage the chaotic logistic map's system parameters and state variables. After control, the logistic map's parameter varies, and the resulting logistic sequence is non-stationary. A complexity study has shown that the upgraded map is random and unpredictable. Based on the improved chaotic maps, a unique picture encryption technique is given, which includes shuffling and replacement operations. Many statistical tests and security analyses show that this technique performs admirably in terms of security and can compete with other relatively new picture encryption algorithms.

Xiang, H., & Liu, L. (2020). Due to their inherent merits, like excessive sensitivity to beginning values, ergodicity, and pseudo-randomness, chaos maps are commonly utilized in picture encryption systems. Because of its structure and ease of implementation, the 1D logistic map has attracted the attention of researchers. However, finite precision easily affects the map, resulting in dynamic degradation. In order to achieve maximum precision, this map should produce a sequence with a shorter period. The simulation shows that the suggested method enhances the unpredictability and complexity of the improved logistic mapping with original logistic mapping. We develop a novel picture encryption algorithm suited for color and grayscale images to show the practicality and application of the enhanced chaotic map. The results show that the proposed algorithm is highly efficient in encryption, has significant resistance to other assaults, and is compatible with other

encryption algorithms.

Ye, G. et al. (2018) The SHA-3 and an ECG signal are described in this research, together with an optimum structure for chaotic encryption based on a 3D logistic map. Following a study of the shortcomings of several present algorithms, particularly fixed key and low sensitivity, this work attempts to address these two issues and comprises two contributions: To eliminate the problem of summation invariance in a plain image, SHA-3 is employed to predict the hash value, with the results used to impact the initial keys for the chaotic map. Using an ECG signal solves the problem of a fixed key, which can be for various subjects or different for the same subject at different periods. In the proposed encryption approach, the Wolf algorithm is used to generate all of the control parameters and initial keys. Summation invariance in the plain image and the lack of a fixed key are expected to be avoided by integrating with the conventional architecture of permutation-diffusion. In addition, the research findings and security analysis reveal that the suggested encryption algorithm can achieve confidentiality.

Shah. A.A. et al. (2020) The transfer of critical real-time image information through unsecured networks is intercepted or even attacked by an adversary in this information age with digitalization. Cryptography turns the information in real-time photographs into incomprehensible data to avoid unwanted access. An efficient picture encryption technique for real-time photos has been designed and evaluated in this study. The suggested system combines encryption with a permutation algorithm based on a modular logistic map to reduce the chaotic value size vector necessary to permute real-time images. We show that an efficient permutation may be produced for a square image with $3N$ pixels using only N chaotic numbers. A 192-bit key is used in the technique, which is broken into smaller pieces and randomly picked to dilute the pixel using numerous XOR operations. The suggested algorithm is resistant to entropy, histogram analysis, spectral characteristic analysis, and other

statistical and differential attacks, according to the results of the experiments.

Safi, H. W., & Maghari, A. Y. (2017) This research investigates the efficacy of a double-chaotic logistic map equation-based picture encryption technique. In two steps, the method generates two sequence keys. To begin, an encrypted key is created by XORing K1 with K2. The novel key is XORed with the original image in the second phase. By evaluating the Histogram, Correlation, and MSE, we could relate the performance of the suggested technique between the original and encrypted images using the MATLAB tool (Mean Square Error). Compared to images produced by a single logistic map, the findings show a flatter and more uniform histogram plot with high MSE values. Furthermore, the correlation between neighboring pixels is almost 0; there is no correlation between the two image versions. As a result, the proposed approach improves encoding efficiency compared to a single logistic map.

Yang, B., & Liao, X. (2018). In recent years, various picture encryption methods based on chaotic systems have been developed, where chaotic maps always work over the actual domain. However, when implementing the map, the complex calculation of the floating-point number can be twice, which is a drawback of the standard chaotic map. As a result, there is a significant disadvantage in terms of practical use. To effectively address this obstacle, a generalized Logistic Map based on chaos theory was used. The automorphic mapping between two logistic maps was used to study the different parameters over finite field. In addition, encryption was done on colored images using the sequence obtained by automorphic mapping. According to security and performance analyses, the suggested system has better qualities that provide a solid guarantee for algorithm efficiency. As a result, the proposed approach can be used to encrypt both images and data.

Manisekaran, P. et al. (2020) The proposed Arnold coupled generalized logistic map lattices picture encryption method is based on nonlinear lattice coupling employing multiple iterated 2D Arnold cat maps, with the number of permutations added as a key space. The suggested ACGLML nth order permutation approach minimizes mutual information between lattice values from 0 percent to 0.1 percent. In particular, a generalized logistic map is employed to widen the diffusion key space compared to previous studies. With the help of metrics like the space-time and space amplitude diagram, bifurcation diagram, Kolmogorov-Sinai entropy, and the strength of diffusion utilizing mutual information, several analyses have been presented to prove the chaotic behavior of the suggested technique. Though the proposal's primary duty is encryption and decryption, they also incorporated compression and decompression using traditional wavelet-based decompositions to confirm that it may be used in a common communication channel.

Sharma, M., & Bharti, V. (2020) To improve the original 1D logistic map, a novel 2D chaotic map is developed that uses a currently suggested bit reversal function. The map is put through a series of conventional tests to ensure that it can generate pseudorandom numbers. The bit-reversed 2D logistic map generates a sequence of two random integers with the improved logistic map's parameter continuously changing. The picture encryption schema is then implemented using the 2D map. A series of simulation runs are conducted to verify the method's overall performance in parameters such as sensitivity to the initial key and the input plain picture. Essaid, M. et al. (2019) Based on the double permutation process, this research proposes an effective image encryption solution. Using an updated 2D logistic map, the goal is to protect color and grayscale photos.

First, we strengthened the chaotic behavior of the 2D logistic map to build an excellent pseudorandom number generator that is more suitable for image scrambling because chaotic features are closely related to cryptographic properties in permutation and diffusion. The plain image is

then subjected to the usual permutation and diffusion encryption techniques. As a result of the augmented 2D logistic map, we construct a first pseudorandom sequence that will be utilized to exchange the rows of the plain image and apply a strong diffusion. A second sequence will be produced to swap the columns and use a double diffusion to reinforce the security. The simulation results for the histogram, key space, correlation coefficient among neighboring pixels, NPCR, entropy, and UACI show that the suggested technique is efficient and reliable.

Li, C., Luo, G., & Li, C. (2019). The three-dimensional chaotic logistic map provides a new image encryption strategy. To generate a keystream, the three-dimensional chaotic logistic map is first adjusted. Second, a three-dimensional chaotic logistic map generates the chaos-based key stream, which performs better regarding randomization qualities and security level. The proposed scheme's design is effective. It includes the confusion and diffusion qualities required for a safe picture encryption technique. The suggested picture encryption scheme's security and performance are assessed using well-known methods. According to simulation findings, the proposed system passes the needed performance requirements, such as ample key space, high-level security, and acceptable encryption speed. The fail-safe analysis is encouraging, and the suggested approach may be inferred to be both efficient and secure. Because of these qualities, it is suitable for use in cryptography applications.

3.6. Observation

After reviewing several image encryptions approaches, the chaotic image encryption method is the best, providing a fair balance of speed, computing power, and security. A new method for image encryption is developed based on this analysis, which uses the chaotic map to encrypt images via permutation and substitution procedures. As chaotic signals are typically noise-like, chaos maps have pseudorandom features and non-

periodicity, and as condition-specific parameter values are calculated, the suggested technique leads to high encryption rates and outstanding security. A paradigm for picture encryption based on the feedback stream cipher and the construction of a chaotic logistic map. It starts with an overview of picture encryption schemes based on chaos. It introduces chaos cryptography and analyses the design principles of proposed algorithm by examining step-by-step procedures of encryption modules for proposed algorithm employing various chaotic maps. The proposed approach is tested, verified, and shown to be efficient. Proposed algorithm's detailed security analysis, which includes key space analysis and statistical and sensitivity analysis regarding key and plaintext, is investigated, as well as a comparison between proposed algorithm and other algorithms.

The logistic map is a straightforward nonlinear model with complex dynamic behavior. The logistic map generates a chaotic sequence sensitive to changes in its beginning value. The auto-correlation and cross-correlation features of logistic mapping sequences are also quite good. The logistic map's iterative sequences can replace the typical pseudorandom sequences generated by the LFSR in encryption.

3.7. Conclusion

An encryption algorithm's primary goal is to transform plaintext to ciphertext using an encryption key. This method must be invertible, meaning that the ciphertext may be converted back to the original message or plaintext using the same key, a process known as decryption. Most encryption techniques are built on the confusion and diffusion notions to ensure that such conversion of plaintext to ciphertext is effective. According to the term confusion, statistical study of the ciphertext should only reveal information about the encryption key. The term diffusion means the plaintext's data should be widely dispersed across the ciphertext, so no statistical examination can disclose any information about the plaintext. Using substitution-permutation networks (SPN) in encryption algorithms like the Advanced Encryption Standard (AES), which will be

discussed later in this chapter, is the most straightforward approach to attain such features. Encryption algorithms are usually measured and evaluated for security and speed.

Because of the rapid advancement of computer technology and the widespread use of the Internet, the security of digital images has become increasingly important, while communication via the transmission of digital applications over an exposed network has become increasingly common. The current works on chaos have been studied in this study and are centered on picture encryption algorithms. These encryption techniques are carefully researched and analyzed to improve the encryption methods' efficiency and ensure the security of digital images transmitted via networks. All of the strategies are beneficial for real-time digital image encryption in this case. Each approach is unique, making it suitable for a variety of applications. New encryption techniques are being developed daily; therefore, traditional encryption approaches will continue to work with a high level of security. Many picture encryption algorithms have been developed in the literature, and the key is created using various maps and procedures. The majority of schemes are linear in nature and have a weak key.

CHAPTER 4: SECURITY ANALYSIS

4.1. Histogram Analysis

An image's histogram displays the pixel value distribution. Histograms of relevant plain images usually have a non-uniform distribution. A high-security Image encryption technique requires a histogram with a uniform distribution. Figure 4.1 shows plain and encrypted histograms for Image Lena. Plain image histograms are non-uniform, but cipher image histograms are flat and uniform, similar to random data distributions.

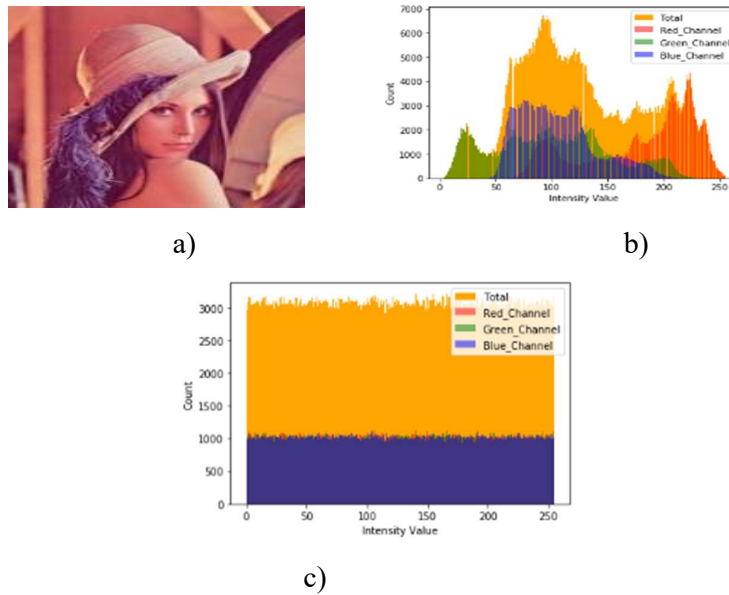


Figure 4.1 a) Lena Image b) Histogram of Lena image c) Histogram of Encrypted Lena Image.

Therefore, the enhanced encryption technique covers the original Image's pixel distribution information (Zhu et al., 2018). An encrypted Image's distribution is determined by its histogram. A cipher's primary goal is to prevent statistical attacks on the image; therefore, the histogram

should be uniform. Histograms are used to analyze irregular distributions of pixel values in encrypted images. According to the results, the pixels of the encrypted Image are equally dispersed, making it difficult for unauthorized individuals to undertake statistical assaults to obtain the plain Image Suneja et al., (2019).

Histogram values of an encrypted image should be uniform, making it impossible for the attacker to understand anything about it. Therefore, the uniform distribution of pixel values in a coded image supports the suggested encryption approach Ye, G., & Huang, X. (2017). To some extent, the statistical features of the images mirror the distribution of gray values in the original images. A significant assessment criterion in image encryption is the ability to modify the statistical distribution of the original images. This method protects against gray statistics attacks. Based on the pixel diffusion and replacement processes, the statistical histograms of the encrypted images were highly uniform, indicating that the technique can withstand statistical assaults and that the attacker cannot determine the gray value distribution range of the original images Zhang et al., (2019).

4.2. Correlation Coefficient Analysis

A correlation coefficient analysis determines the degree of similarity between adjacent pixels (Ramasamy et al., 2019). Statistical attacks are possible in plain images due to the high correlation between adjacent pixels. An encrypted image's adjacent pixels should have weak correlations, indicating that they have no relationship. It is demonstrated that ciphered images have improved confusion and diffusion capabilities by calculating and evaluating Pearson correlation coefficients. This is done by calculating and evaluating the vertical, horizontal, and diagonal directions of unencrypted and encrypted images. The symmetric nature of the encryption method allows the receiver to fully decode the cipher image. Li et al., (2017) display the restoration results for several plain-image cipher images. They are unable to tell the difference between plain-

image cipher images and encrypted images. The correlation coefficient of adjacent pixels of any two images is calculated using following Equations (4.1 to 4.4)

$$r_c = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \quad , \quad \text{Eq (4.1)}$$

$$\text{Where, } cov(x,y) = \frac{1}{N} \sum_{i=1}^N (x_i - F(x))(y_i - F(y)) \quad \text{Eq (4.2)}$$

$$D(x) = \sum_{i=1}^N (x_i - F(x))^2 \quad \text{Eq (4.3)}$$

$$F(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad \text{Eq (4.4)}$$

N is the total number of pixels, and x and y are two adjacent pixels. Figure 4.2 shows the correlation analysis of Lenna's original and Encrypted Image.

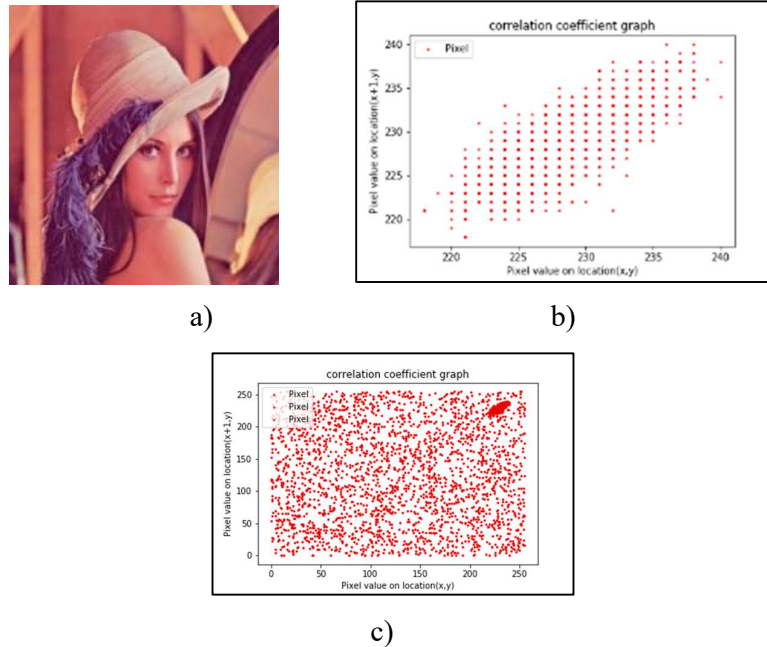


Figure 4.2. a) Lenna Image b) Correlation analysis of Lenna Image c) Correlation analysis of Encrypted Image

Image security analysis relies heavily on the correlation of neighboring pixels since it indicates how much scrambling there is in an image's distribution of pixels. In an encrypted image, the better the scrambling effect, the lower the correlation of neighboring pixels, and vice versa. An attacker can easily extract plaintext information from a plain image because the connection between neighboring pixels is quite strong. The goal of employing an image encryption approach is to decrease pixel correlation and get the relevant cipher Image Zhang et al. (2019).

4.3. Entropy Analysis

Shannon's information theory is a mathematical theory that he developed in 1949. Error correction, data compression, cryptography, communications systems, and other related subjects are all covered in modern information theory. The entropy is calculated using a well-known formula Equation 4.5

$$H(d) = \sum_{i=1}^N P(d_i) \log_2 P(d_i) \quad \text{Eq (4.5)}$$

Where P is the probability of occurrence of a symbol, N represents the total number of symbols in data $d_i \in d$, and \log_2 represents entropy in bits. Ideally, the cipher image should be random and the information entropy should approach 8. Ye, G., & Huang, X. (2017), The higher the entropy value, the more secure the image encryption. It is generally considered secure from brute-force attacks when the entropy number is extremely close to 8 (Ramasamy et al., 2019). A 256-grayscale image has 28 levels of pixel values, so 8 is the optimal information entropy value. A new calculating method called local Shannon entropy was presented by Wu et al. that addresses the shortcomings of global entropy, such as its inaccuracy and inconsistency. The local entropy approach is better than the global entropy approach. Zhang et al. (2019) compute the average Shannon entropy value by selecting non-overlapping blocks in the image at random. Compared with most other current techniques, the entropy of the decrypted image is remarkably close to the optimum entropy value.

4.4. Differential Cryptoanalysis

One of the most effective and widely used security attacks is the differential cryptoanalysis attack. Two metrics are used to determine if image calculation encoding can withstand differential attack: unified average change intensity and number of pixel change rate. It may be possible to retrieve specific secret keys involved in executing a crypto algorithm by collecting this information, at least in a sloppy implementation. The process is known as a Linear Analysis when a single input elicits information. The process is known as a Differential Analysis when many inputs are utilized in conjunction with statistical techniques. In this work, we focus on the second type of attack, specifically in the context of elliptic curve encryption Joye, M., & Tymen, C. (2001). NPCR and UACI are calculated using Equations 4.6 and 4.7.

$$NPCR = \frac{1}{L \times M} \sum_{i=1}^L \sum_{j=1}^M x(i, j) \times 100 \quad \text{Eq (4.6)}$$

$$UACI = \frac{1}{L \times M} \left[\sum_{i,j} \frac{|e_1(i,j) - e_2(i,j)|}{N-1} \right] \times 100\% \quad \text{Eq (4.7)}$$

Where L and M are the width and height of an image, e1 and e2 represent encrypted images after a 1-pixel value change.

The higher the NPCR, the more sensitive the image encryption method is to the plain Image and the better its ability to withstand differential attack. The method's capacity to resist differential assaults improves as the values get closer to their optimum levels. The NPCs and UACIs of the three Images, as well as similarities to previous research. As the findings show, this technique is resistant to differential assaults (Zhang et al., 2019).

4.5. Peak Signal-To-Noise Ratio and Mean Square Error

PSNR is given by a signal's max power ratio and the de-noised signal. It is a measure of the quality of an image; the higher value of PSNR represents a better image quality. Equation 4.8 and 4.9 are used to calculate PSNR and MSE.

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \quad \text{Eq (4.8)}$$

$$MSE = \frac{1}{W*Z} \sum_{x=1}^W \sum_{y=1}^Z [P(i,j) - P'(i,j)]^2 \quad \text{Eq (4.9)}$$

Where W and Z are the dimensions of an image, P(i,j) is the input image, and P'(i,j) is the encrypted Image; table 1. exhibits the analysis of different images picked from the SIPI database. R stands for maximum fluctuation of an Input Image, for an image with 8 bits pixels per sample, R=255, and MSE stands for mean square error. Mean Square Error measures the system's robustness, the average of squared distances between the observed and actual value.

4.6. Keyspace Analysis

For an excellent encryption scheme, the encryption keys should be the center of attention in both the encoding and decoding processes. The size of the key decides how robust the algorithm is; it gives all the distinct and valid keys that can be used to encrypt data. The key size helps in resisting brute force attacks. The key space analysis gives the total number of unique keys used in encryption. As a result, the security key should be reasonably sized and resistant to brute force attacks Suneja et al., (2019). An encryption system's key space can range from several combinations to millions. The larger the size of all possible permutations, the stronger the

encryption system. For an image encryption algorithm to have high security, the keyspace should to at least as large as $2^{100} \approx 10^{30}$.

The term "key sensitivity" refers to the fact that if an attacker modifies even a single pixel in the original key, the original Image is rendered unrecoverable. Security keys are essential to every encryption method since they determine the algorithm's strength. The secret keys must be powerful enough to withstand any sort of attack. Ample key space and great sensitivity are desired features of powerful secret keys Kaur, M., & Kumar, V. (2020).

4.7. Key Sensitivity Analysis

A suitable encryption method should be susceptible to tiny changes in plain Images and key components. When the key remains constant, the encryption technique is considered very sensitive to plaintext if the plaintext to be encrypted varies significantly, creating a significant change in the ciphertext. If the encrypted plaintext remains constant, but the encryption key varies little, the ciphertext changes substantially. The encryption technique needs to be extremely sensitive to the key. Even a minor modification in the plain Image, such as a single-bit alteration, can significantly impact the cipher image. An encryption method, as is widely known, should be susceptible to any secret key. Any minor alteration must result in a new cipher image or an incorrect decrypted Image from the same cipher-image Ye, G., & Huang, X. (2017).

CHAPTER 5: 3-D CHAOS BASED IMAGE ENCRYPTION USING LOGISTIC MAP

5.1 Introduction

Multimedia communications have surpassed the use of text messages as a result of current technical breakthroughs. The majority of these messages are sent through the internet, the number of security dangers on the internet is rapidly expanding. Traditional techniques facilitate interaction latency and processing expense while simultaneously providing little protection against new threats. These difficulties in contemporary algorithms push academics to delve deeper into this field Khan et al., (2019) suggested such algorithms that have reduced overhead, are more efficient than existing techniques, and are equipped to meet the needs of next-generation multimedia networks. To solve all of these concerns, and with the future of next-generation multimedia networks in mind, and developed a safe and lightweight encryption technique for digital pictures. By combining cryptography approaches with image processing, security precautions may be applied, Figure 3.1 and 3.2 illustrates image encryption and decryption. Using a logistic map, the original image is first permuted.

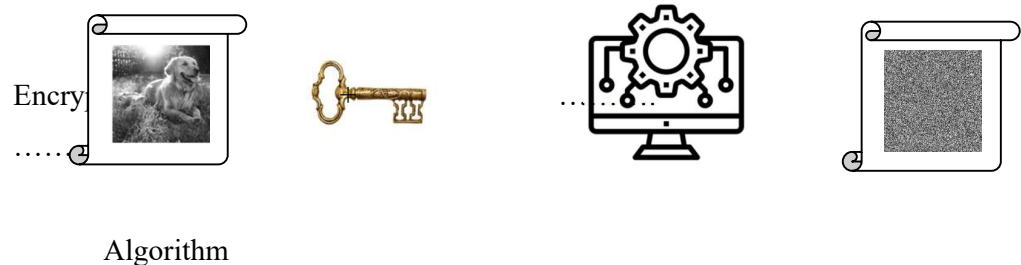


Figure 5.1. Image encryption structure

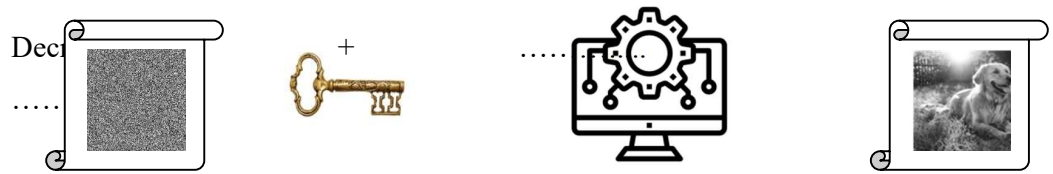


Figure 5.2. Image decryption structure

Due to its outstanding cryptographic distinctiveness, domain chaos is ideally suited for use in information security. However, computer limited precise expression, and unitary chaos with basic structure was merely threatened by chaotic reconstruction, limiting its practical application. A novel type of chaos encryption method has been proposed and achieved to resolve the problem of which overcomes the drawback of the key size being determined solely by the user password and improves the algorithm's security performance. It uses the Noor iterations of Logistic map as the chaos model. The algorithm's resilience is great, and its encryption effect is better than current techniques, according to theoretical analysis and experimentation results.

5.2. Proposed Methodology

The fundamental premise of encryption with chaos is based on the ability of some dynamic systems to generate random numbers in a series. Encryption is done with this sequence. The series of random integers used for decryption is extremely dependent on the initial condition used to generate this sequence. It passes the statistical tests of a current test suite, even when quantized, indicating that the suggested key stream generator is not only efficient but also has a high throughput. By iterating a one-dimensional chaotic map, chaos is brought to cryptology and a secret key cryptosystem. It is based on chaotic properties such as parameter

unpredictability, sensitivity of beginning points of sequences created by iterating a chaotic map. Researchers have been interested in studying chaos-based systems for the past decade. Matthews invented the chaotic encryption technique in 1989. Chaos-based systems are nonlinear dynamic systems that are sensitive to initial condition dependencies. They are popular among academics for encryption algorithms because of qualities such as unexpected behavior, periodicity, and pseudo randomness.

Chaotic systems possess traits that satisfy the diffusion and confusion requirements of a successful cryptography algorithm. The fascinating aspect of chaos-based systems is their great affectability to their fundamental situation, control criteria, and ease of use, which leads in high encryption rates when properties like as avalanche effect, confusion, and diffusion are present.

The underlying premise of chaos encryption is based on the ability of some dynamic systems to generate random sequences of integers. Encryption is done with this sequence. The series of random integers used for decryption is extremely dependent on the initial condition used to generate this sequence. A minor change in the starting condition will result in a completely different series. Chaotic systems are useful for encryption because of their sensitivity to beginning condition. An arrangement of three chaotic functions with great sensitivity to beginning circumstances is employed proposed technique to appropriately apply uncertainty and diffusion concepts to pictures with some entropy. The routines are used to shuffle pixel locations, while the other is used to alter pixel values. Adjacent pixels containing related values would take on significantly distinct values in the subsequent fresh pixel generation, making splitting the encrypted picture difficult. Exclusive-or and circular rotation operations are employed to spread the impact of a small change in the single-pixel intensity of the plain picture across numerous pixels in the cipher image. A lot of investigations and tests have been conducted to

demonstrate the algorithm's security and validity.

5.2.1. Key Generation

In this paper we have used 3 such chaotic-logistic map to encrypt an image. The 3D Logistic Map is given by the Equation 5.1 to 5.3.

$$x_{n+1} = \gamma x_n(1 - x_n) + \beta y_n^2 x_n + \alpha z_n^3 \quad \text{Eq (5.1)}$$

$$y_{n+1} = \gamma y_n(1 - y_n) + \beta z_n^2 y_n + \alpha x_n^3 \quad \text{Eq (5.2)}$$

$$z_{n+1} = \gamma z_n(1 - z_n) + \beta x_n^2 z_n + \alpha y_n^3 \quad \text{Eq (5.3)}$$

The chaotic behavior of 3D logistic map is exhibited for $3.53 < \gamma < 3.81$, $0 < \beta < 0.022$, $0 < \alpha < 0.015$ and the values of x , y , z lie $[0,1]$. The initial value of $x_0 = 0.235$, $y_0 = 0.37$, $z_0 = 0.3735$, which serve as our keys in the encryption. A 3D position matrix using chaotic equations with unique values is generated that is used in encryption to shuffle an image. The proposed methodology is given in Figure 5.3.

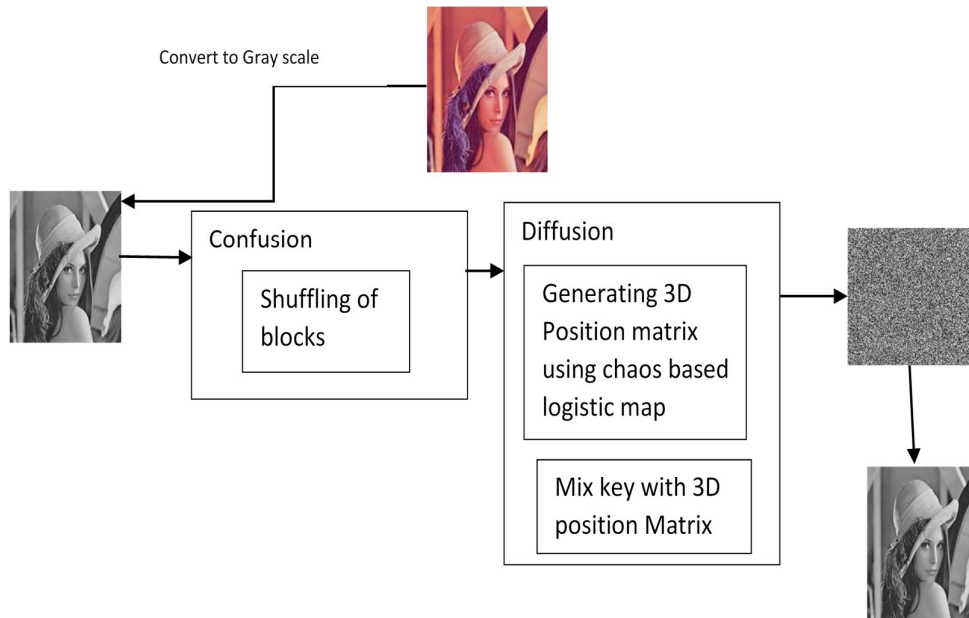


Figure 5.3. Proposed Methodology

5.2.2. Encrypting the image

It's an encoding method that uses an encryption algorithm to encrypt the secret image so that unauthorized users can't see it. Encryption is the process of changing the data or bits of a certain source in a specific pattern that is only known by the sender and receiver. This is commonly done using plaintext passwords or Secure SSL encryption technologies. However, applying the same encryption algorithm to an image is a game-changer in the realm of secret message transmission via visuals.

5.2.2.1 Permutation

It is a method in which the plaintext stays unchanged but the letters are shuffled in a different sequence. Any plaintext data unit lack uniformity must be dispersed over the cipher text to be effective, making that no consistency tough to detect.

5.2.2.2 Substitution

Each character in the plaintext is exchanged for another character in the cipher text in this approach. To retrieve the plaintext, the receiver reverses the replacement on the encrypted text.

5.2.2.3 Confusion

The goal is to make the link between the cipher text and the symmetric key as complicated as feasible. This means that each character of the encrypted text should be dependent on many key elements.

5.2.2.4. Diffusion

The plaintext statistical structure is dissipated throughout the bulk of cipher text. It implies that if we alter a character in the plaintext, the characters in the cipher text should change dramatically. This level of intricacy is usually achieved by a sequence of replacements and permutations. The picture encryption system suggested by Mekki et al., (2018) is made up of several rounds of permutation and diffusion. To permute all of the pixels, the permutation method is utilized. Following that, the diffusion process altered the pixel value. The logistic map generates the pseudo number. The only change in the decryption algorithm is the opposite of iteration. Diverse criteria have been employed in order to conduct a complete examination of the approaches. The current section goes through all of the parameters in depth mentioned by Mohammad et al., (2017).

Algorithm 1: Encryption using 3D Chaotic Logistic map

Result: Encrypted Image

- Input the Number of iterations, Key, Plain Image.
- Generate a new 3-D position matrix using chaotic equations with unique values which correspond to change in positions of blocks.
- Gray Scale image is converted into a 3D matrix of 0's and 1's where each binary stream in the position (i,j) is the binary representation of intensity of pixel at that position.

- Generate a new 3D position matrix by iterating chaotic equations with unique values which correspond to new positions of blocks after shuffling.
 - Apply circular shift operation on rows, in case of even row apply right shift operation or else apply left shift operation on row.
 - Similarly apply circular shift operation on Columns, in case of even column apply rightshift operation or else apply left shift operation on column.
 - XOR the shuffled key matrix with plain image matrix.
-


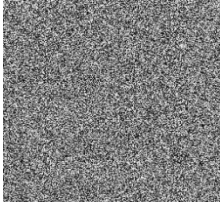
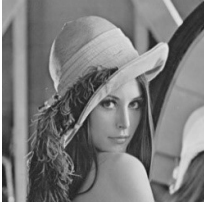

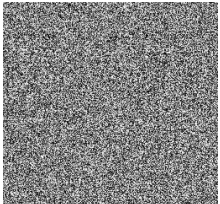


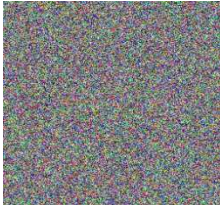


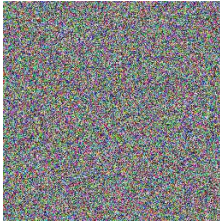

5.2.3 Decrypting the image

Algorithm 2: Decryption using 3D Chaotic Logistic map

Result: Decrypted Image

- Input the Number of iterations, Key, Encrypted Image.
 - Generate a new 3-D position matrix using chaotic equations with unique values which correspond to change in positions of blocks.
 - Convert encrypted image to a 3-D matrix of 0s and 1s where each binary stream in the position (i,j) is the binary representation of intensity of pixel at that position.
 - Apply circular shift operation on Columns, in case of even column apply left shift operation or else apply right shift operation on column.
 - Apply circular shift operation on rows, in case of even row apply left shift operation or else apply right shift operation on row.
 - XOR the shuffled key matrix with encrypted image matrix
-

Table 5.1 Encrypted and Decrypted Images using 3D Logistic Map

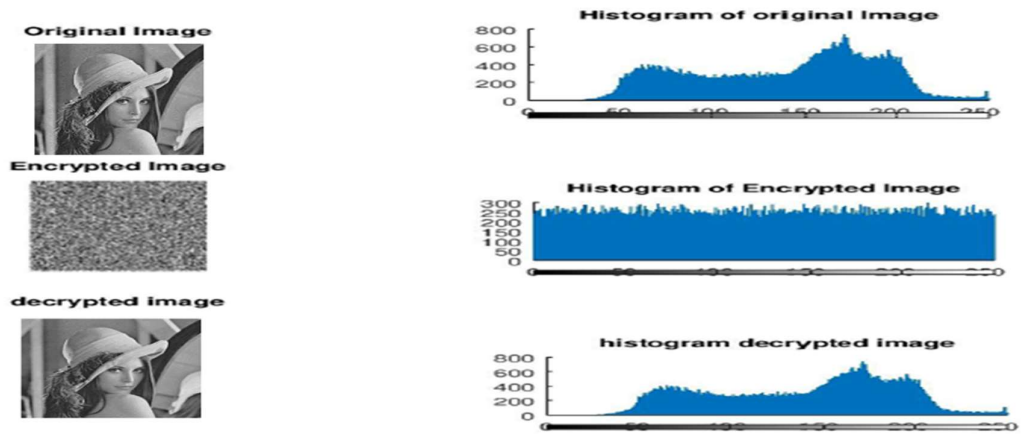
Plain Image	Encrypted Image	Decrypted Image
		
		
		
		

5.3. Performance Evaluation

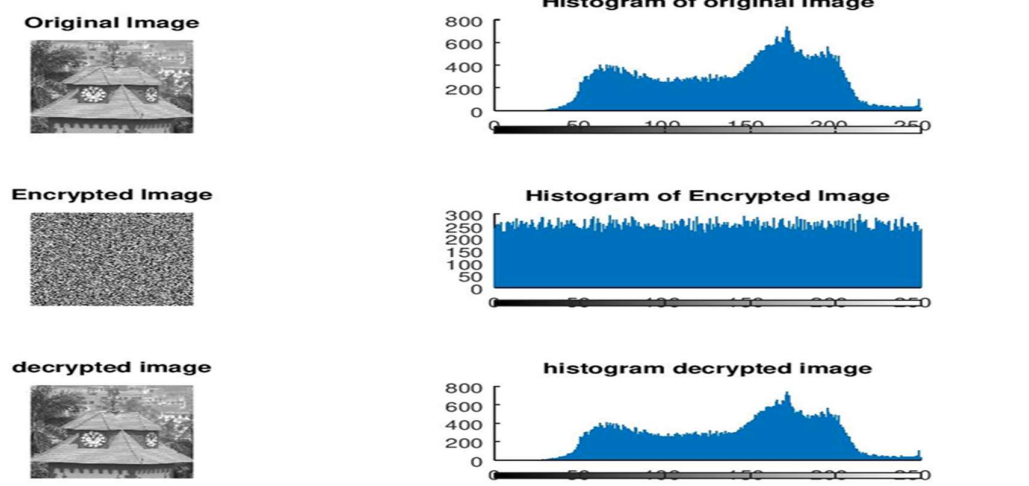
5.3.1 Histogram Analysis

An image's basic attribute is its pixel value distribution. This distribution can be seen in a histogram analysis. It is imperative that the distribution of pixels within an encrypted image differs entirely from that of a plain image in

order to maintain the confidentiality of the image. The probability distribution of the proposed scheme can be seen in Figure 5.4.



a)



b)





Figure 5.4. Histogram Analysis a) Lenna Image b) House Image

5.3.2 Correlation Analysis

Across adjacent pixels in an image, there is strong pixel correlation and there is a significant amount of redundancy. It is possible to remove the dependency between these adjacent pixels using a good encryption algorithm. Based on Table 5.2, it can be seen that there is a correlation analysis of original

and encrypted image horizontal pixels, vertical pixels, and diagonal pixels. Figure 5.3. c) and d) illustrate that adjacent vertical and horizontal pixels in the encrypted Lena image do not have any correlation.

Table 5.2. Correlation of pixels of 3D Logistic Map Encrypted Image

Image	Original Image	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
	0.9467	0.0053783	0.006321	0.002341
	0.9822	-0.0022596	0.0012312	0.0021223
	0.9243	0.0086	0.00512	0.00521
	0.9876	0.00231	-0.00232	0.1298

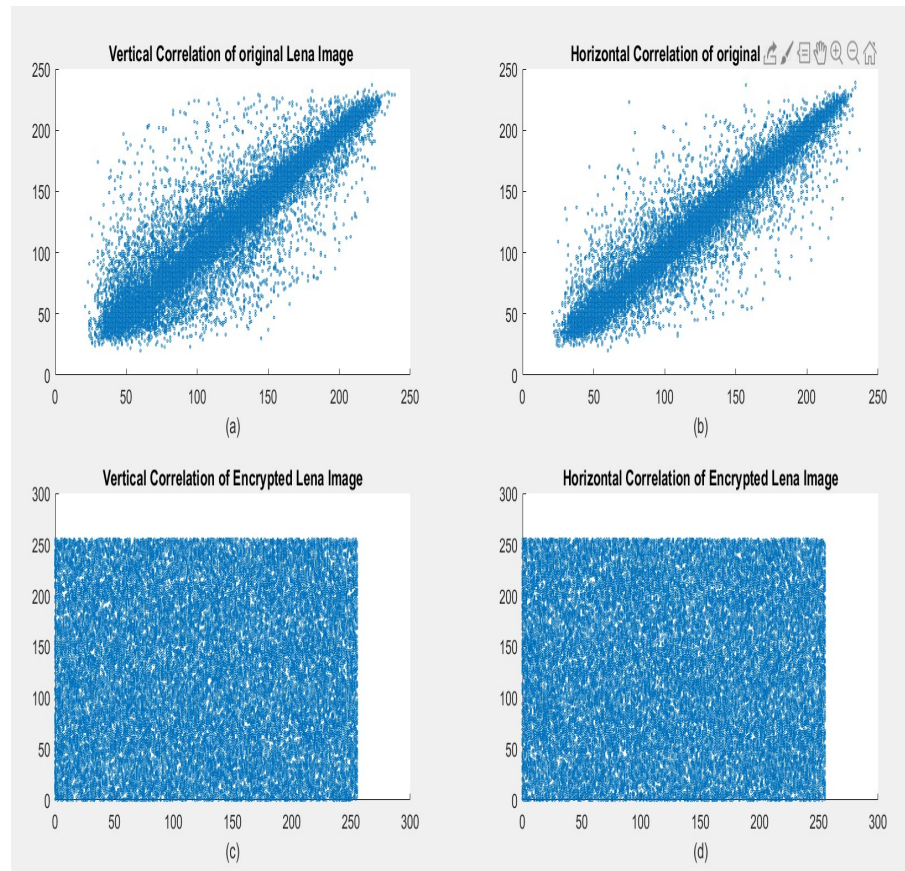



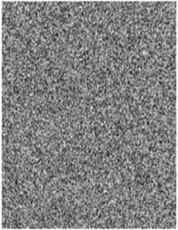
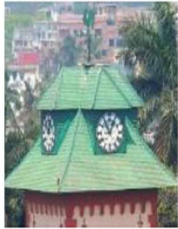





Figure 5.6. Correlation Analysis Lena Image

5.3.3 Key sensitivity Analysis

The most effective encryption algorithm has the characteristics of an avalanche effect, which is an effect in which a minor change results in a different image. Using the wrong key with even a 1-bit change can result in an entirely different image when compared to using the right key, as shown in Table 5.2.





Table 5.3. Key Sensitivity Analysis

Plain Image	Encrypted Image	Decrypted Image with correct key	Decrypted Image with Incorrect Key
			
			

5.3.4 Differential Cryptanalysis

Any effective cryptographic algorithm must be able to resist differential attacks. NPCR and UACI are two parameters used for measuring the sensitivity of an image. The UACI measures the difference in the moderate intensity of pixels between the two images. NPCR gives the change rate of number of pixels of cipher image if one pixel is changed in plain image. In Table 5.3, it can be seen that the proposed techniques have NPCR (ideal value 99) and UACI (ideal value 33) values that are higher than the expected value, thus making them resistant to differential cryptography attacks.

Table 5.4. Performance Analysis of 3D Logistic Map

Image	UACI	NPCR	MSE	Entropy
	33.434	99.609	0.11871	7.9974
	33.464	99.609	0.12634	7.9972
	32.0852	99.6159	0.18682	7.9989
	33.123	99.561	0.0042	7.9988

5.3.5 Mean Square Error (MSE)

Entropy, which measures the randomness of any cryptosystem, is measured by Mean Square Error (MSE). As shown in table 5.3. According to the proposed algorithm, the entropy value is 7.9998, which is very close to the ideal value of 8.

5.4. Conclusion

A symmetric key image encryption algorithm was introduced in this paper. As part of the proposed scheme, a key generation system is implemented using a 3-dimensional chaos-based logistic map, which utilizes block shuffling as a key generation method. In order to achieve confusion and diffusion, pixel shuffling is

used. Based on the experimental results of the presented method, it can be shown that the histogram of the cipher image has a uniform distribution of pixels. In addition, the entropy value of the cipher image is more than 7.99, which is very close to the ideal value of 8. It is also shown by the NPCR and UACI values, that the proposed scheme can also be protected from differential cryptanalytic attacks due to its security features. Compared to other schemes, the proposed scheme is simple and fast.

CHAPTER 6:

A ONE-DIMENSIONAL SUPERIOR LOGISTIC MAP BASED IMAGE ENCRYPTION

6.1. Introduction

Digital media security is a significant issue in this pandemic; this has enabled the development of fast and secure cryptographic technologies. Image encryption based on chaos has become popular due to its ergodic properties. In this chapter we used a one-dimensional chaos logistic map based on Superior iterations. In order to generate the chaotic sequence, both imaginary and real parts of the 1-dimensional map are considered. An image is scrambled and diffused by combining a chaotic sequence with a secret key entered by the user. The image is then evaluated using various measures such as NPCR, UACI, MSE, PSNR, and entropy. The simulation result shows that the cipher image's correlation coefficient is below 0.01. The entropy of the cipher picture is similar to its optimal value of eight; making it resistant to statistical attacks. The proposed scheme is robust and reliable to differential crypto-analysis attacks based on the results of NPCR and UACI. The results show that the proposed scheme is resistant to occlusion attacks when Gaussian and salt and pepper noise are included in the picture.

6.2 Methodology Used

The simple logistic map with picard iterations is given by Equation 6.1

$$x_{n+1} = r \times x_n(1 - x_n), \quad \text{Eq (6.1)}$$

Where the value of x_n lies between (0,1), it represents the population of year n where the initial year is 0 and r produces a positive reproduction rate and starvation. Most of the cryptographic algorithms proposed use Picard iterations, the most common method of solving nonlinear equations. They are simple; however, the convergence rate is decelerated for low values of r and became unstable at $r > 4.2$. Mann iterations increased this convergence range. Rani et al. (2011) used Mann's successive approximation technique, also known as superior iterations with a stable logistic map behaviour for a larger value of r . The proposed method uses these superior iterations to encrypt an image. The following Equation gives superior iterations:

- $x_{n+1} = g(f(x_n), x_n) = \beta(f)(1 - \beta)x_n$, where β lies between 0 and 1
- The map exhibits stable behavior for $r > 3.2$ for $\forall x \in [0, 1]$.
- For $\beta < 0.15$, the logistic map is only convergent.
- The logistic map leaves its chaotic behavior for $\beta < 0.64$.
- An unstable range of β is undefined.

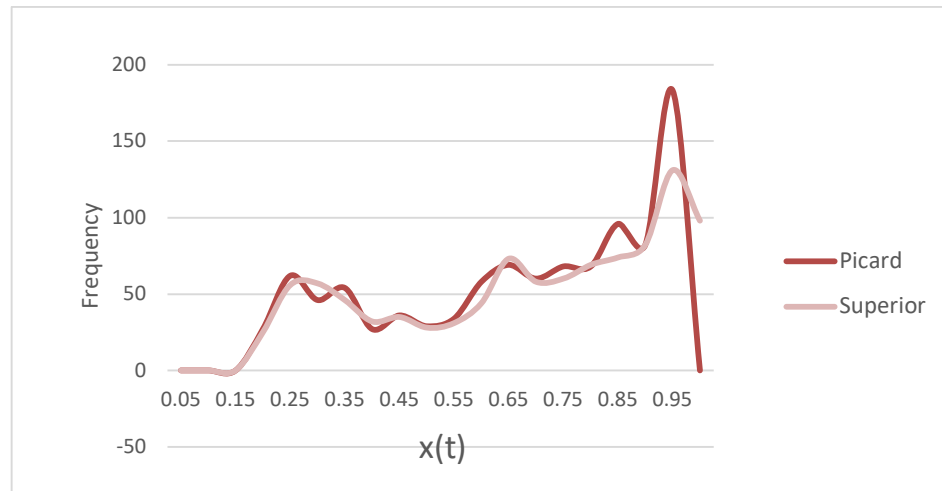


Figure 6.1. Frequency distribution of $x(t)$ for chaotic parameters

The parameter r of superior orbit with initial conditions lies between $x_0 \in [0,1]$, a large set of these values iterates, known as the trajectory. Because of the ergodic property, the interval of $[0,1]$ is visited frequently. The plot in Figure. 1 shows the frequency distribution of the variable $x(t)$ for a sample of 1,000 iterations, where. For cryptography, it is essential to analyse the density invariance of these variables. Logistic map encryption is based on the time-invariant density of such points also it is simple and easy to implement as compare to other chaotic maps . For this, frequency distributions of x and y variables are plotted for a wide range of values between 0 and 1.

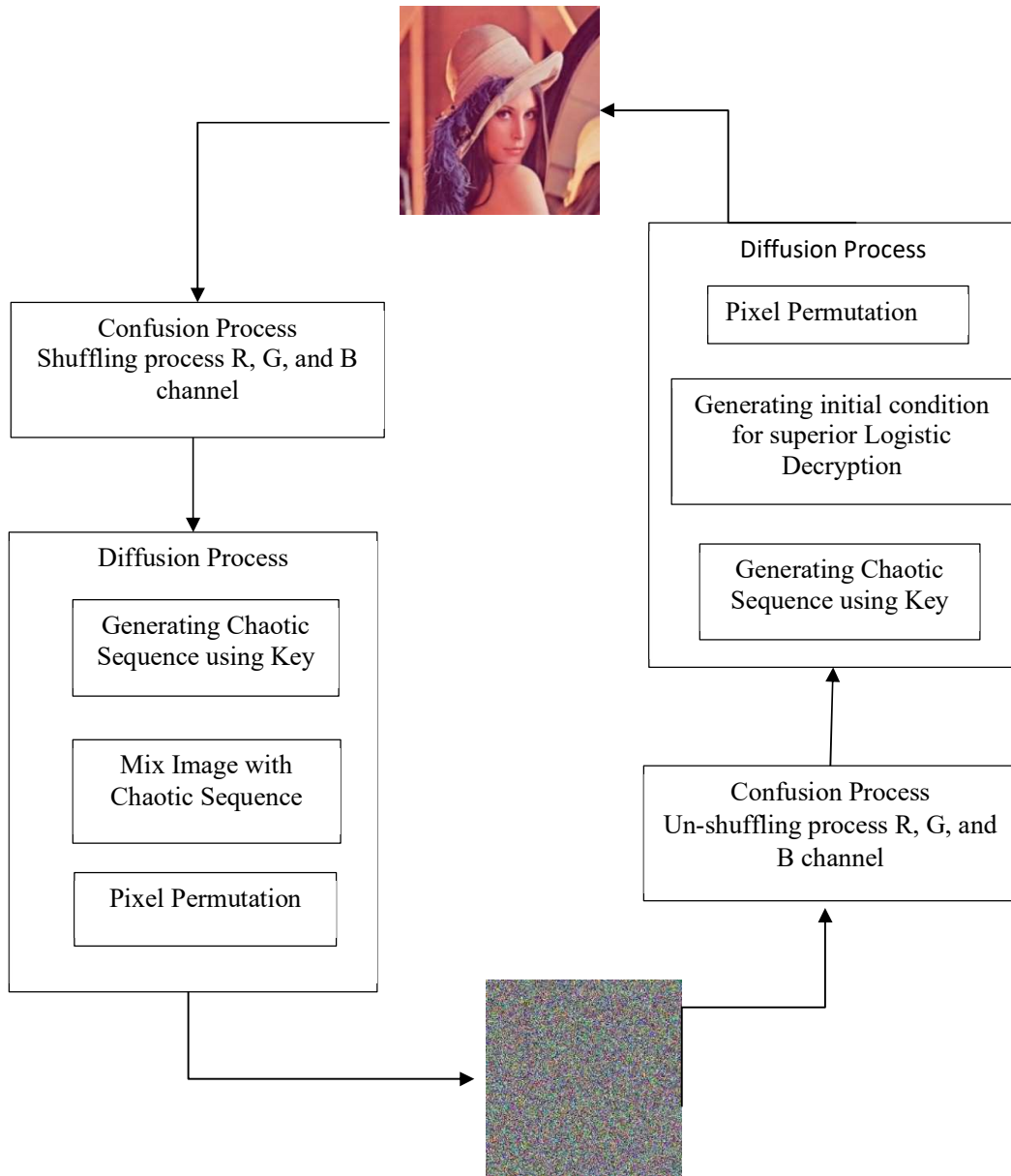


Figure 6.2. Proposed Methodology

This implementation includes key mixing, which recalculates the chaos map's initial values based on the previous encryption value and the key value after every pixel encryption. The value of $\beta=0.9$ and $r=4.1$ are used for the experiment

6.2.1. Algorithm for Generating Chaotic Sequence

Algorithm 1: Key Generation Algorithm using Superior Logistic Map

Result: Chaotic Key sequence

- Input the Number of iterations, Key, Plain Image.
- A secret key of 12 characters is input by the user, each 8-bit is converted into $K=k_1, k_2, k_3, \dots, k_{12}$.
- A sequence S is generated using

$$S = S + G_{(i-1)(j-1)} \times 10^{-j}$$

- Calculate the initial value of x_0 and y_0 using the following where the initial value of $R=1$

$$R = (R \times S) \bmod 1 \quad L_x = (R + K_{12}/256) \bmod 1$$

$$L_y = (V + K_{12}/256) \bmod 1$$

Where $V = k_1 \oplus k_2 \oplus k_3 \oplus k_{12}$

$$x_0 = (k_1 \oplus k_2 \oplus k_3 \oplus L_x \times 10^4) \bmod 256$$

$$y_0 = (k_1 \oplus k_2 \oplus k_3 \oplus \dots \oplus k_{12} \oplus L_y \times 10^4) \bmod 256$$

- Continue to iterate the values of x and y based on Logistic Iterations for all values between

0.2 and 0.8

$$x_n = \theta \times r \times x_{n-1} - \theta \times r \times x^2 + \theta \times r \times y^2 + x_{n-1} \theta \times x_{n-1}$$

$$y_n = -2 \times \theta \times r \times x_{n-1} \times y_{n-1} + \theta \times r \times y_{n-1} - \theta \times y_{n-1}$$

- Here the value of x_n = real part of the iteration, and y_n = imaginary part

6.2.2. Algorithm for Encryption

A pixel-by-pixel operation was applied to scramble the rows and columns of an image. In an image, one permutation can only scramble a column or row. Thus, more than one operation is required to permute both.

Algorithm 2: Encryption using Superior Chaotic Logistic map

Result: Encrypted Image

- Image is converted into channels of red, blue, and green pixel values.
- Partial security is achieved by applying the process of shuffling of pixels.
- The chaotic sequence is converted into a matrix to mix it with the image matrix.
- Each pixel value is reset according to values in an obtained matrix.
- The diffusion sequence is obtained for R, G, and B; the following calculations were performed where $I_{i,j}$ is the image matrix.

$$\begin{aligned}C_1 &= (x_n \times 10^4) \bmod 256 \oplus (k_0 + x_n) \bmod 256 \oplus (x_{n-1} + k_1) \bmod 256 \\C_2 &= (x_n \times 10^4) \bmod 256 \oplus (k_2 + y_n) \bmod 256 \oplus (x_{n-1} + k_3) \bmod 256 \\C_R &= (k_4 + C_1) \bmod 256 \oplus (k_5 + C_2) \bmod 256 \oplus k_6 + I_{i,j}[0] \bmod 256 \\C_G &= (k_4 + C_1) \bmod 256 \oplus (k_5 + C_2) \bmod 256 \oplus (k_6 + I_{i,j}[1]) \bmod 256 \\C_B &= (k_4 + C_1) \bmod 256 \oplus (k_5 + C_2) \bmod 256 \oplus (k_6 + I_{i,j}[2]) \bmod 256 \\C &= (k_4 + C_1) \bmod N \oplus k_5 + C_2) \bmod N \oplus (k_6 + I_{i,j}[0]) \bmod N \oplus (k_7 + C_R) \bmod N\end{aligned}$$

- x_{n+1} and y_{n+1} are calculated by using following equations

$$\begin{aligned}x_{n+1} &= (x_n + C + k_8 + k_9)/256) \bmod 1 \\y_{n+1} &= (y_n + (C + k_8 + k_9)/256) \bmod 1\end{aligned}$$

6.2.3. Algorithm for Decryption

The decryption process is the reverse of the Encryption Process; it contains the following steps.

Algorithm 3: Decryption using Superior Chaotic Logistic map

Result: Decrypted Image

- Cipher Image is converted into channels of red, blue, and green pixel values.
 - Pixels are shuffled, and a chaotic sequence is generated.
 - The chaotic sequence is converted into a matrix to mix it with the cipher image matrix.
 - The obtained matrix is mixed with key to get the original image.
-

6.3. Experimental Result and Analysis

Python 3.7 on the Intel Core i5 processor with 4 GB RAM and 1.6GHz speed with Windows-10 Operating system is used for implementing the proposed technique. All the images used are available in the SIPI image database. To assess the performance of the system criterion measures like Entropy, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Histogram Analysis, Unified Averaged Changed Intensity (UACI), Correlation Analysis etc. are used.

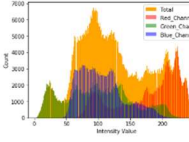
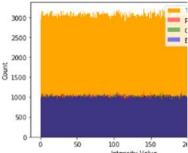
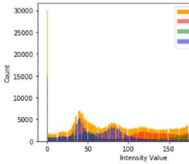
Table 6.1. Performance Analysis of Superior Logistic Map based Encryption

Image	Iterations	PSNR	MSE	Entropy
Lenna Image	Superior	8.6219	0.1374	7.9998
	Picard	8.6185	0.13745	7.9988
Pepper Image	Superior	8.8549	0.1277	7.9997
	Picard	8.07997	0.15559	7.9995

Tree Image	Superior	8.1666	0.15252	7.9989
	Picard	8.1528	0.153	7.998
Women 1 Image	Superior	8.83422	0.13079	7.9991
	Picard	8.83074	0.13089	7.9986
Women 2 Image	Superior	7.28569	0.18682	7.9989
	Picard	7.27383	0.18733	7.9982

An efficient image encryption algorithm tends to encrypt a plain image to a random incomprehensible form; thus, generating a cipher image with a uniformly distributed intensity histogram proves the quality of an image. Many algorithms have uneven histograms that make them vulnerable to attacks as energy transformed is centralized, making a non-uniform histogram. Table 6.2. shows the histogram of a Plain Image and Cipher image of the proposed algorithm are different from each other. The cipher image displays the uniform distribution of RGB channels.

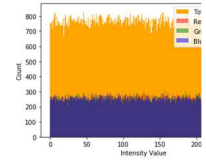
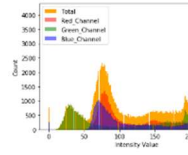
Table 6.2. Histogram Analysis

Input Image	Size	Histogram of Input Image	Histogram of Encrypted Image
 Lenna.png	512×512		
 Pepper.tiff	512×512		



Tree.png

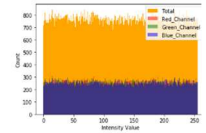
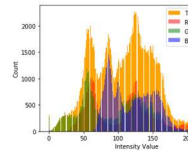
256×256



Women

1.png

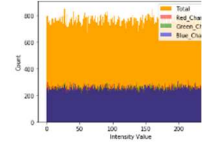
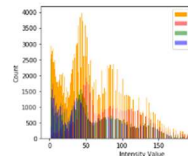
256×256



Women


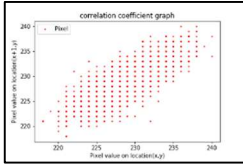
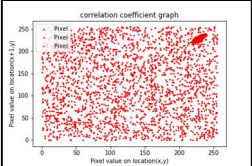


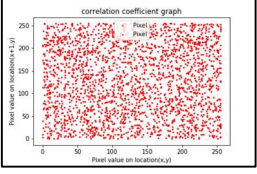


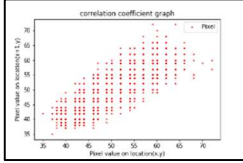
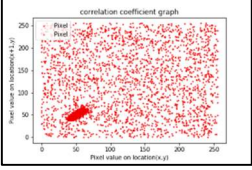
2.png

256×256



As the classical encryption methods like AES or DES have high redundancy of data, they cannot be used in image encryption as it leads to a statistical attack. The correlation between any two adjacent pixels needs to be minimum on any excellent image encryption algorithm. Thus, as a metric of encryption performance, the adjacent pixel association is found in Vertical, Horizontal, and Diagonal direction. Random pixels are picked up from the image, and the association between its rightmost neighbors is found and plotted. It can be seen from Table 6.3. the correlation plot of the encrypted image appears random with no discernible pattern.

Table 6.3. Correlation Analysis

Input Image	Original Image	Encrypted Image
 <p data-bbox="329 657 444 688">Lenna.png</p>		
 <p data-bbox="329 936 444 968">Pepper.tif</p>		
 <p data-bbox="289 1230 383 1262">Tree.png</p>		
 <p data-bbox="289 1461 431 1493">Women1.png</p>		
 <p data-bbox="289 1698 431 1730">Women2.png</p>		

The proposed scheme shows the Encrypted Lenna image's correlation coefficient

decreases when using superior iterations compared to Picard iterations. Therefore, it can be inferred that the proposed scheme is better resistant to a statistical attack than the algorithms with Picard iterations.




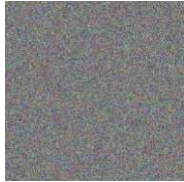
Table 6. 4. Correlation Analysis of Original and Encrypted Image

Image	Iterations	Input Image	Encrypted Image
Lenna Image	Superior Iterations	0.9673	0.006161
	Picard Iterations		0.006618
Pepper Image	Superior Iterations	0.9786	0.00823
	Picard Iterations		0.00856
Tree Image	Superior Iterations	0.9487	0.00781
	Picard Iterations		0.00829
Women 1 Image	Superior Iterations	0.92436	0.00868
	Picard Iterations		0.01446

Women 2 Image	Superior Iterations	0.9588	0.01077
	Picard Iterations		0.01105

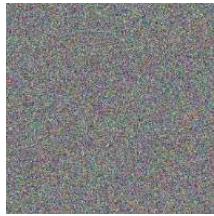
Behaviour of the key in an encryption algorithm predicts the security of an algorithm. Even a one-bit change in Key must not result in a plain image. Figure – shows the proposed scheme's results for $\beta = 0.9$ and $r=4.1$ with Key 1='supersecretke' and Key 2 =' supersecretkd'. When decrypted with a wrong key with minor changes, the proposed algorithm does not result in a plain image. Table 5 shows the difference between the decrypted image with correct as well as wrong key.

Table 6.5. Key Sensitivity Analysis

INPUT IMAGE	ENCRYPTED IMAGE	DECRYPTED IMAGE WITH CORRECT KEY (Key 1)	DECRYPTED IMAGE WITH WRONG KEY (Key 2)	DIFFERENCE BETWEEN DECRYPTED IMAGE
				99.56
Lenna.png				



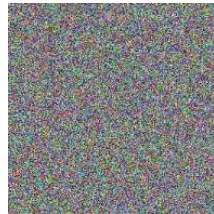
Pepper.tiff



98.89



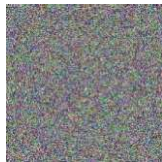
Tree.png



99.36



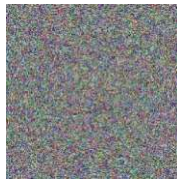
Women1.png



99.87



Women2.png



98.95

Differential crypto-analysis attack, assure minute variation in the pixel in an input image would make a significant difference in encrypted image. NPCR and UACI are two meters of checking the effect of this one-pixel variation in an image. NPCR gives the change rate of the pixels values in an image. If the value is nearing 100 presents, the system is highly sturdy against differential crypto analysis attack.

Table 6.6. Differential cryptanalysis

Image	Iterations	NPCR	UACI
Lenna Image	Superior	99.6976	33.65381
	Picard	99.59234	33.02445
Pepper Image	Superior	99.6064	29.947
	Picard	99.593	28.732
Tree Image	Superior	99.61446	33.464
	Picard	99.6190	30.041
Women 1 Image	Superior	99.63633	33.4698
	Picard	99.61598	31.1398
Women 2 Image	Superior	99.6164	32.225
	Picard	99.61395	31.966

Table 6.6 shows that the suggested technique can effectively withstand differential cryptanalysis attack and is better than Picard iterations. An encrypted image may lose information blocks when transmitted over an unsecured channel, known as an occlusion attack. The proposed scheme has been proven robust by applying the different percentages of occlusion on an enciphered image. MSE and PSNR can be used to evaluate this; it can be proved from Table 6.7. that the suggested scheme can withstand an occlusion attack by reconstructing the image similar to the original image. In the experiment, the original images are corrupted using noise like Salt and Pepper with density 0.05 and Gaussian Noise with

mean 0 and variance 0.001. Figure 6.3. shows decrypted images.

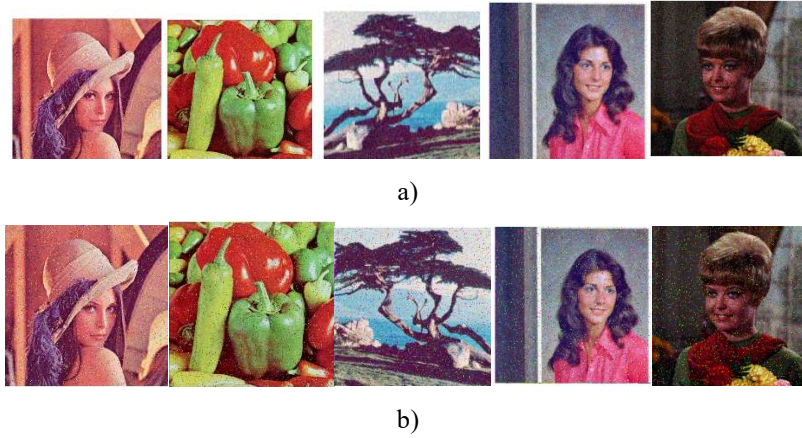


Figure 6.3. Noise attack: a) Gaussian Noise with mean 0 and variance 0.001 b) Salt and Pepper noise of density 0.05

Table 6.7. Noise Attack

	Gaussian noise with mean 0 and variance 0.001		Salt and Pepper noise of density 0.05	
	MSE	PSNR	MSE	PSNR
Lenna	0.12438	71.831	0.1253	71.513
Pepper	0.14738	64.463	0.14803	64.271
Tree	0.15198	63.129	0.15232	63.03
Women1	0.17095	58.019	0.17114	57.972
Women2	0.18854	56.286	0.18974	56.106

A good cryptographic algorithm needs a key size of more than 2^{100} to resist brute force attacks. Almost all chaos-based algorithms have. Any chaotic function uses three parameters starting value(x0), the total number of iterations, and control parameters. In the Picard iteration, only one control parameter is used, and superior iterations use two parameters. Each parameter uses 64 bits of space; hence key space size of the proposed scheme is 2^{256} ; sufficient to withstand brute force attack.

6.4. Comparative Analysis of Lenna Image

The suggested scheme demonstrates a significant increase in histogram accuracy relative to the equivalent transformations. If the encrypted image shows non-uniformity of pixel intensity distribution, this may result in information leakage. This makes the system vulnerable to a potential attacker to draw a statistical attack.

Table 6.8. Comparative Performance Analysis of proposed scheme

	NPCR	UACI	Entropy	Correlation
Proposed	99.69	33.653	7.9998	0.006161
[1]	99.66	33.62	8.3655	0.0026
[2]	99.6	33.476	7.9997	0.000027
[3]	99.62	3.51	7.9974	-0.23
[4]	98.36	27.97	7.997	0.002
[5]	98.68	33.46	-	0.0067
[6]	98.47	33.45	7.992	0.0036
[7]	99.622	33.5887	7.9995	-0.237

Correlation, Entropy, NPCR, and UACI values are compared for Lenna Image. The suggested scheme shows better Entropy results and is resistant to differential cryptanalysis attack. The highest value is shown in bold for all parameters in Table 8.

6.5 Conclusion

The proposed scheme introduces a symmetric cryptographic approach for image security, the algorithm based on a superior logistic map. Researchers' work is on the higher-dimensional chaotic map that takes more time and higher complexity. In the proposed scheme, we have used chaotic key sequence generated using the real and imaginary part of a 1-dimensional superior logistic map with β as 4.1 and r as 0.9. The proposed scheme was explicitly designed to ensure the cipher image's randomness, the high degree of uncertainty, and the complete diffusion of image pixels, making it computationally effective for image encryption. Shuffling of pixels was done to apply confusion and diffusion. The empirical results showed that the suggested scheme has a uniformly distributed histogram and entropy

near the ideal value 8. The correlation among image pixels in cipher image is close to 0; hence, it can withstand statistical attack.

The value of NPCR is above 99%, and UACI is above 33%; therefore, the proposed technique can resist differential cryptanalysis attacks. Gaussian and salt and pepper are applied to the images, and MSE and PSNR were calculated; the result shows that the proposed scheme can stand up to occlusion attack. A contrastive study of the suggested scheme is made with some existing algorithms, and with Picard, iterations show the method is secure and has a robust, practical application. In the future, we plan to develop further systems for diverse media types, using the scope of the chaos-based superior iterations to symmetric key encryption. Some of the desired features to be addressed and enhanced in potential scope include the speed of encryption, size, bandwidth and substantive security. With this pandemic, most of the work is done online and may require sending and receiving audio and video data across unsecured channels. Such schemes may also be built for videos and audio in the future.

CHAPTER 7: CHAOS-BASED ASYMMETRIC KEY CRYPTOGRAPHY

7.1. Introduction

With the advent of Internet technology and its universal applications, a large amount of information has been presented in the form of digital images. There have therefore been a number of image encryption algorithms proposed to ensure the security of images during transmission. There are some security prerequisites that must be met before images can be transferred safely. In much existing Research work Various Security algorithm implemented to secure the images. In this work, the Chaos tent map function is used to propose. Initially input images are considered to sequence generation process, to enchasing the security level. Once image sequence generated Chaotic Cryptosystem used to encrypted images. In the proposed methodology, we use the Chaotic tent map function to secure the image. The tent map is a discrete-time dynamical system composed of iterated functions that form a tent shape. The key optimization process is carried out using an improved Salp Swarm Algorithm (ISSA). Based on these two phases, encryption and decryption were performed and basic keys and control parameters were used to control the behavior of the proposed system. To enhance the unpredictability of the cipher-image, the presented Chaos function was combined with an XOR operation during encryption. This proposed model compared to other existing research work and Conventional techniques.

Encryption is the most commonly used tool for checking the transfer of images from unapproved. Image protection is increasingly considered these days because images may contain classified data in remote detection. With the advancement of paper innovation, current safe correspondence is widely noted in pharmaceuticals, aviation, instruction, the military and various other sectors. As a fictional letter, computerized image data has become main stream. By preparing and organizing correspondence with the rapid advancement of computerized image, data security issues have gradually become obscure Image encoding has become a significant research subject computerized images placed on the PC architecture

are created from a limited number of elements as an exhibit; each component has its specific area and value, most of which are called pixels. Generally, image highlight encryption techniques involve two stages: extraction and highlight encryption.

7.2. Methodology

7.2.1. Chaos-based Key Generation

Tent map is an iterated function between $[0,1]$ interval. The shape of this map is like a tent; the map is given by the following Equation:

$v_{(i+1)} = f(v_i, \lambda)$ where f is given by

$$f = f(v_i, \lambda) = \begin{cases} f_L(v_i, \lambda) = \lambda v_i, & \text{if } v_i < 0.5 \\ f_R(v_i, \lambda) = \lambda(1 - v_i) & \text{otherwise} \end{cases} \quad Eq (7.1)$$

Where $\{v_i \in [0,1], \text{ for } i \geq 0, v_0 \text{ is the starting value of system}\}$. Tent Map contains the control parameter $\lambda \in [0,2]$; depending on the control parameter λ , the map ranges from predictable to chaotic when $\lambda = 1.99999, v_0=0.000001$ (Gora, 2003). Following are statistical characteristics of the chaotic tent map in the interval $[0,1]$ that makes it suitable for the image encryption applications:

- $f(v_i \lambda) = 1$, a consistent invariant distribution density function.
- The Lyapunov index >0 .
- Output rail approximation of the autocorrelation function $\sigma(a) = \gamma(a)$.

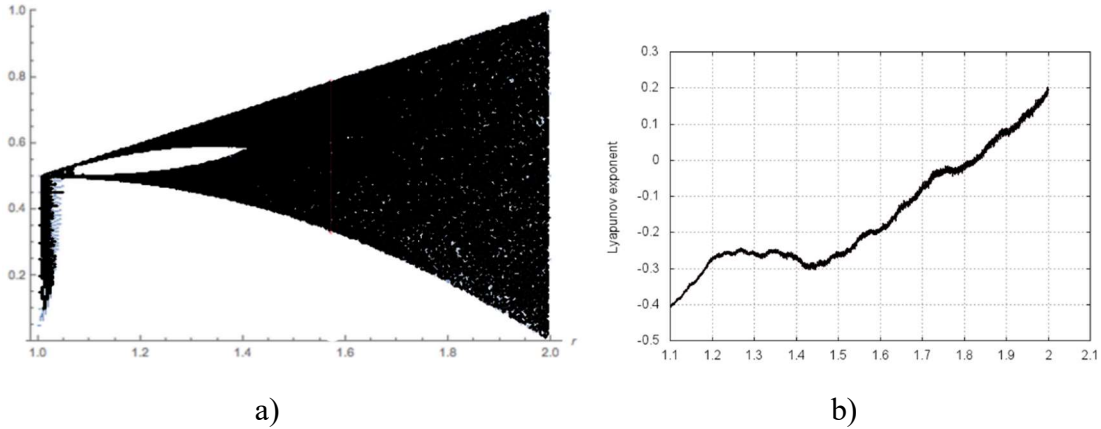


Figure 7.1. a) Bifurcation diagram of Tent Map b) Lyapunov exponent of Tent Map

Chaotic systems can be studied using bifurcation diagrams. Lyapunov exponents have several advantages over other methods for analyzing chaotic behavior in a system. Quantitative analysis is based on Lyapunov exponents. System predictability and sensitivity to changes in initial conditions are measured by this metric. There must be at least one positive Lyapunov component for every chaotic system. A tent map with a bifurcation diagram and Lyapunov exponent can be seen in figure 7.1. When the mapping is applied to a chaotic sequence, periodicity is observed under finite precision. The chaotic tent maps (Gora, 2003), show periodicity at large values. Chaotic sequences become more random as the output of the random sequence turns into zero after a finite number of iterations. Piecewise linear functions always have a limited precision value, so the value is close to 2. The proposed methodology is shown in Figure 7.2, and the primary chaos function is shown in Figure 7.3. Cryptography and decryption are performed using chaos-based methods in this proposed methodology. Double keys were created for the encryption and decryption procedures using 16-character byte keys entered by the user in order to increase the security of the chaotic function.

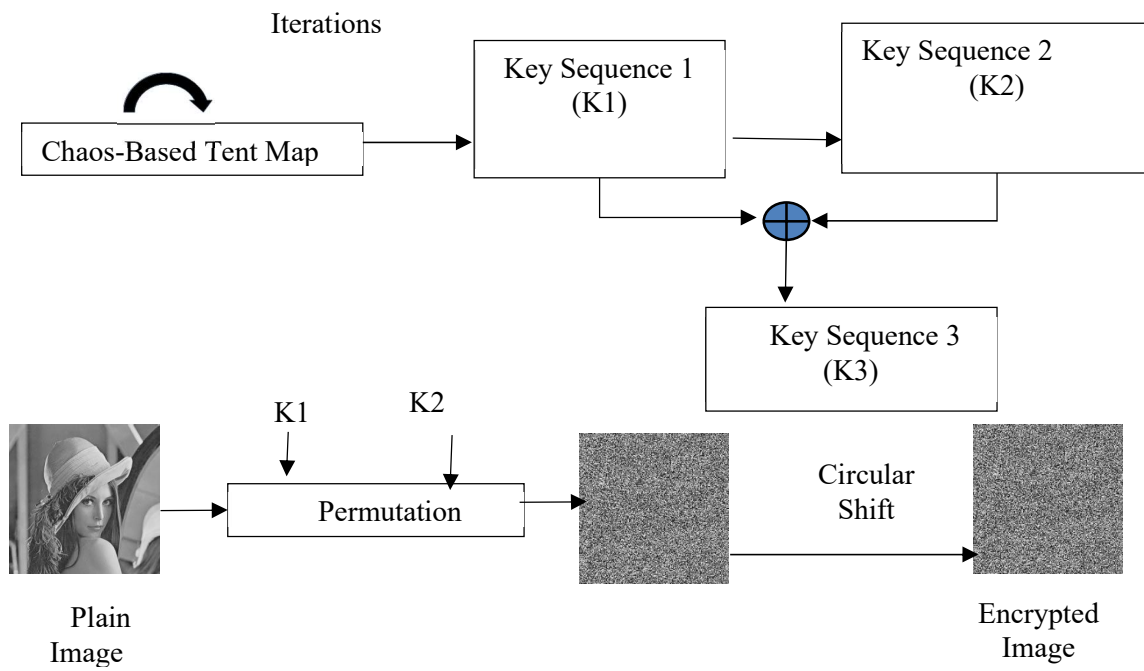


Figure. 7.2. Methodology

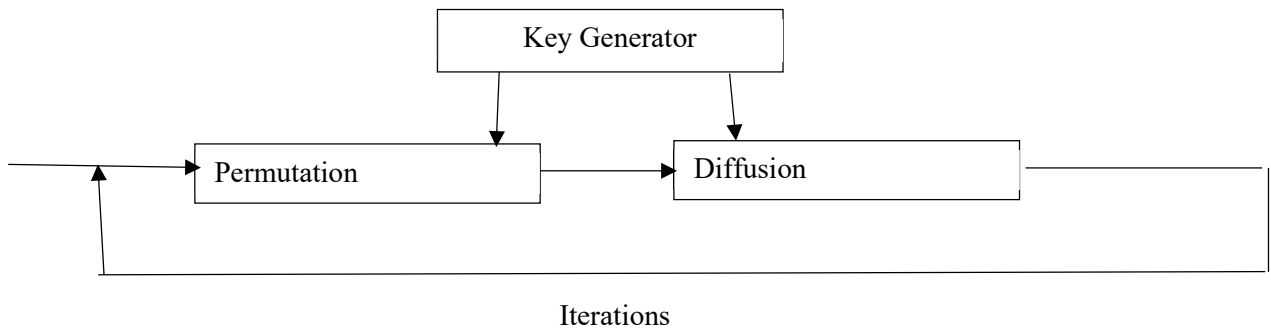


Figure. 7.3. Basic Chaos Function

Algorithm 1: Key generation using Tent Map

- **Result: Chaotic Key Sequence**
- Key Parameters, Initial Parameters of Tent Map, Input Image
- Let $I = M \times N$, the number of pixels that represent the input image.
- Iterate the tent map function using

$$v_{i+1} = f(v_i, \lambda) \quad \text{where } f \quad \text{is given by}$$

$$f = f(v_i, \lambda) = f_L(v_i, \lambda) = \lambda v_i, \quad \text{if } "v_i < 0.5"$$
$$f_R(v_i, \lambda) = \lambda(1 - v_i) \quad \text{"otherwise"}$$

I times to create the first sequence of the Key called K_1 . The key sequence 1 is used for permutation of the rows.

- Convert it into 8-bit blocks
 - Apply 3-bit alternate right and left circular shift to create the second key sequence K_2 of the size I , from secret Key. K_2 is used for column permutation, both sequences are created are very random and fast to calculate.
 - These two sequences are XORed to generate a third sequence K_3 .
-

7.2.2. Improved Salp Swarm Algorithm (ISSA)

A recent development in optimization techniques is Salp based swarm optimization. We are using this technique to optimize the Key for decryption. Salps are barrel-shaped planktonic tunicates. They have similar movements and filigree like jellyfish. Salps form a chain in the ocean; this helps Salp coordinate movements and be fast. The crossover and mutation process from the Genetic Algorithm (GA) is adapted in this SSA to improve the salp swarms' behaviour. This improved formulation increases the accurate solution and reduces the iterations (Sayed, 2018). The step-by-step process is given below.

Steps:

- i. **Key Initialization:** Randomly generate the initial population of salp using the chaotic tent map $s_i = s_1, s_2, \dots \dots s_n$, where $i = 1, 2, \dots \dots n$ and n =total number of key values considering upper and lower bound values.
- ii. **Fitness Function:** It is used for the assessment of the performance of the system. In this research, the objective function is formulated as in Eq (2):

$$F_{fn} = \min \left[\frac{1}{n} \sum_1^n (y_i - \bar{y}_i)^2, \sum_1^n \frac{|y_i - x_i|}{n} \right] \quad Eq (7.2)$$

Where, F_{fn} represents the fitness function, y gives the actual value, and \hat{y} represents the predicted value, and x_i gives the original key values.

- iii. **Updating Function:** To update the circumstance of the leader salp position the accompanying condition is proposed in Equation 7.3

$$p_j^1 = \begin{cases} f_j + r_1((u_j - l_j) \times r_2 + l_j)r_3 \geq 0.5 \\ f_j - r_1((u_j - l_j) \times r_2 + l_j)r_3 < 0.5 \end{cases} \quad Eq (7.3)$$

Where $r_1 = 2e^{-\left(\frac{4t}{t_{max}}\right)^2}$

p_j^1 Possition of the leader in j^{th} dimension, u_j is the upper bound, l_j shows the lower bound, r_1, r_2, r_3 are the random numbers, t is the current iteration, and t_{max} represents the maximum no of iterations. The position of the follower's updated equation is given below in Eq (4),

$$p_j^i = \frac{1}{2} (p_j^i + p_j^{i-1}) \quad Eq (7.4)$$

Where, $i \geq 2$ and p_j^i is the i -th follower salp in the j -th dimension.

- iv. **Cross Over & Mutation:** After updating the follower's position from the SSA crossover, and mutation procedure is applied. A cross over point inside a chromosome creates the offspring. After the crossover, the child chromosome is changed for raising the viability of the arrangement to the modified quality of the chromosome. The mutation is the way toward creating novel offspring from a single parent. Researchers have used many different mechanisms for mutation. (Wang, 2013) presented an improved Particle Swarm Optimization technique using Levy, Cauchy, and Gaussian mutations given by: $p_g = p_g + \eta$ and (Lu, 2004) a mutation function using Gaussian distribution $p_g = (0.5\eta + 1)p_g$ Where p_g is global optimum and η is a Gaussian random number. In this paper, we use a uniformly distributed random number r

$$F = F + F \times r \quad \text{Eq (7.5)}$$

Where F is the global optimum. The mutation is triggered if $c < p$ where c is the chaotic tent map given by Eq(1) and p is mutation probability given by,

$$p = p_{min} + (p_{max} - p_{min}) \times 1/L \quad \text{Eq(7.6)}$$

Where L is presumed maximum number of iterations and p_{max} and p_{min} are maximum and minimum probabilities.

The selection of mutation likelihood, on the other hand, is difficult to understand. If p is sufficiently small, the mutation will have little effect on convergence performance. If p is too large, the population search will be hampered. As a result, the mutation probability expression is shown as Eq(6), with the value of

probability increasing as the number of iterations rises.

- v. **Termination Criteria:** The optimal keys are selected with the help of ISSA to improve their crossover and mutation procedure in GA. It adds resilience to the SSA for analyzing the population and its diversity to reach the optimal solution.

The pictorial working principal of improved salp swarm optimization algorithm (ISSA) the proposed methodology is given in Fig 7.4.

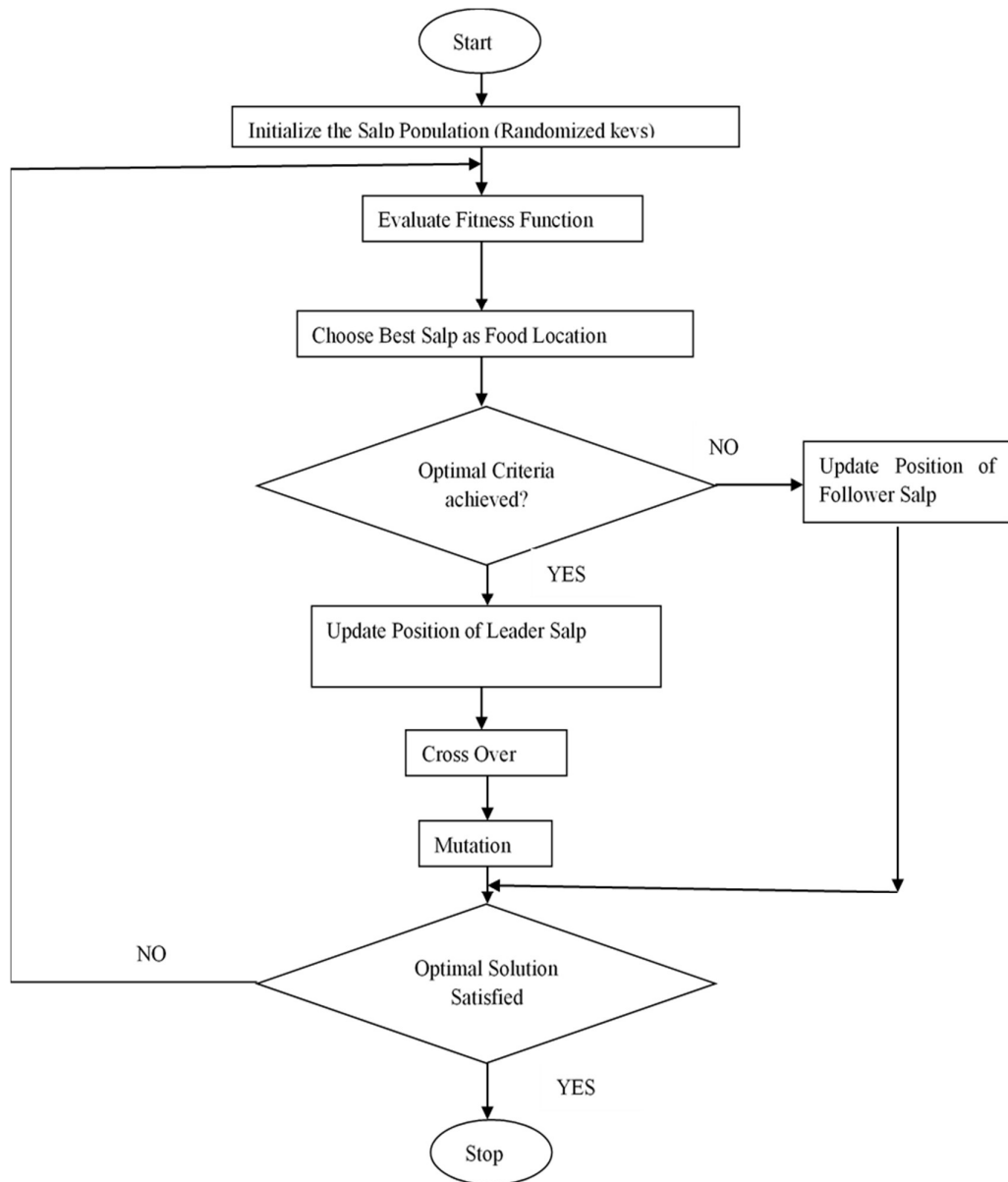


Figure 7.4. Working Principal ISSA

7.2.3. Encryption Phase

Algorithm 2: Encryption using ISSA and Tent Map

Result: Encrypted Image

- Input the Chaotic Key Sequence, Plain Image
- Apply the row permutations using K_1 and column permutation using K_2 .

- Divide the key sequence and Plain Image into an 8-bit block.
 - Circular shift operation is applied on each block, on the basis of K_3 , the first bit of third keysequence determines the direction of the shift.
 - If its 0 apply left shift if its 1 apply the right shift operation. The next 3 bits of K_3 determines how many bits are to be shifted. If the value of K_3 is 4 then apply circular shiftoperations by 4 bits.
 - Each block of plain Image is XOR-ed with an 8-bit block of key values to get a cipherimage.
-

7.2.4. Decryption Phase

Algorithm 3: Decryption using ISSA and Tent Map

Result: Decrypted Image

- Input the optimized key and Ciphertext Image
 - Divide the key sequence and Encrypted Image into 8 bits.
 - Apply circular bit shift operation.
 - Apply XOR between a block of cypher images and optimal key-value obtained by applyingISSA algorithm
-

7.3. Experimental Results and Performance Evaluation

We used MATLAB 7.12 on the Windows-10 Operating system with an Intel Core i5 processor with 4 GB RAM and 1.6GHz speed for the experimental setup. We used all the images of size “512×512”; those are available in the SIPI image database. Some reference images are shown in Figure. 7.5. Encryption and decryption output of all the referenced images are shown in Table 7.1.



Figure 7.5. Reference input database images

Table 7.1: Overall Image Sequence Encryption and Decryption

Input Image		Encrypted Image		Decrypted Image	
<i>SSA</i>	<i>ISSA</i>	<i>SSA</i>	<i>ISSA</i>	<i>SSA</i>	<i>ISSA</i>

To measure the performance of the proposed methodology, we used the following parameters: We evaluate encryption time, decryption time, Entropy, peak signal to noise ratio (PSNR), unified averaged changed intensity (UACI),

mean square error (MSE), cross-correlation to measure the performance of the proposed algorithm as shown in Table 7.3, 7.3 and 7.4.

Table 7.2: Encryption and Decryption Time of ISSA Algorithm

Images	Encryption Time(ms)	Decryption Time(ms)
Lena	0.22882	0.21817
Baboon	0.21191	0.23375
Cameraman	0.23999	0.26605
Barbara	0.24919	0.22539
Puppy	0.33818	0.24624

Table 7.3. Entropy, PSNR, and MSE ISSA Algorithm

Input Image	Entropy	PSNR	MSE
Lena	7.9975	34.43	0.00036
Baboon	7.9963	33.51	0.00045
Camera Man	7.9986	39.88	0.0001
Barbara	7.9962	32.8	0.00052
Puppy	7.9981	35.95	0.00025

By cross-correlation, an image's adjacent pixels are ranked according to their relationship. To break the redundancy of data in images, any image encryption algorithm must minimize the correlation between neighboring pixels. Therefore,

we use the correlation between adjacent pixels in a particular direction (Horizontal, Vertical, or Diagonal) as a metric for assessing encryption performance. The correlation between a random pixel and the rightmost neighbor of the image is found and plotted. In Table 7.5 and Figure 7.6, you can see that the correlation plot of the encrypted Image appears random with no discernible pattern in the horizontal and vertical directions.

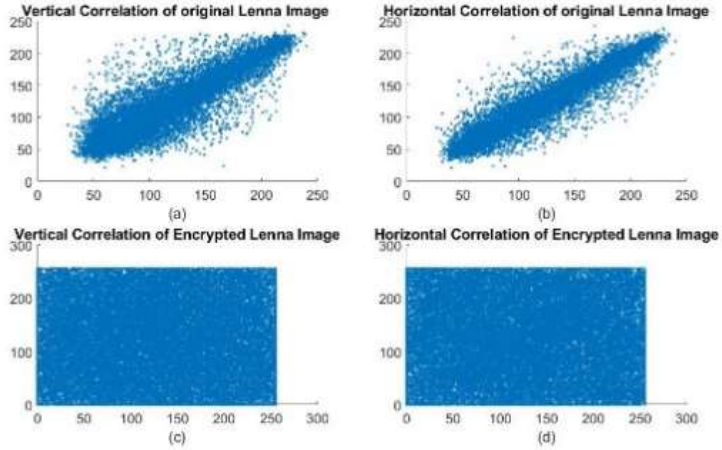
Table 7.4. Differential Cryptanalysis

Image	NPCR	UACI
Lena	99.65	33.471
Baboon	99.56	33.462
Camera Man	99.63	33.43
Barbara	99.62	33.465
Puppy	99.65	33.464

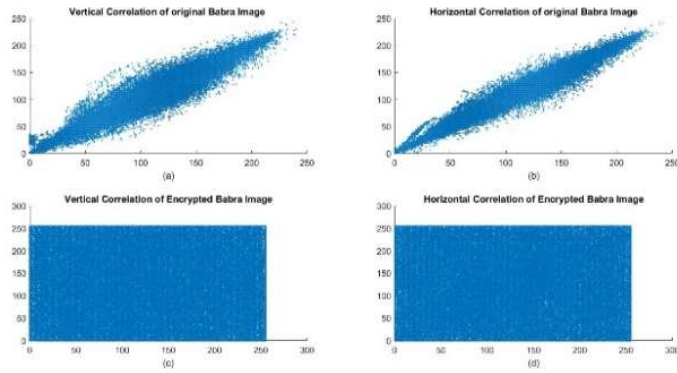
Table 7.5. Cross-Correlation Analysis

Input Image	Cross-correlation Original Image			Cross-correlation Cipher Image		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	0.9917	0.9923	0.9917	0.0016	0.0021	0.0003
Baboon	0.9859	0.9976	0.9828	0.0019	0.0019	-0.0012
Camera Man	0.9946	0.9945	0.9897	0.0011	-0.0021	0.0013

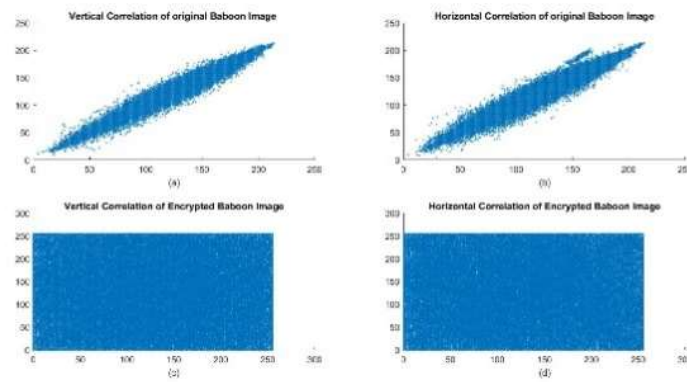
Barbara	0.9922	0.9927	0.9949	0.0017	0.0025	0.0005
Puppy	0.9936	0.9896	0.9925	0.0023	0.0013	0.0006



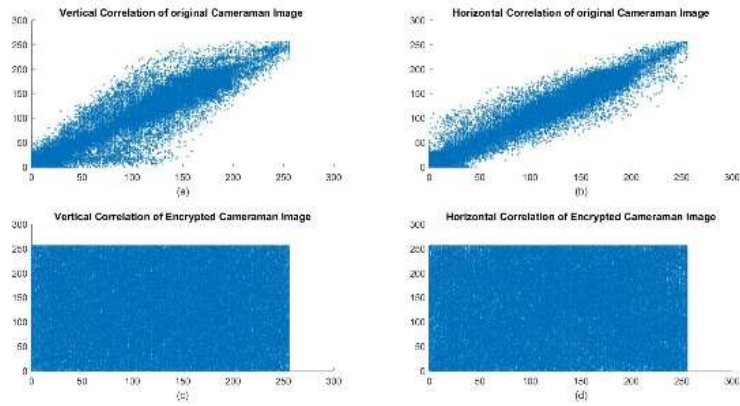
a)



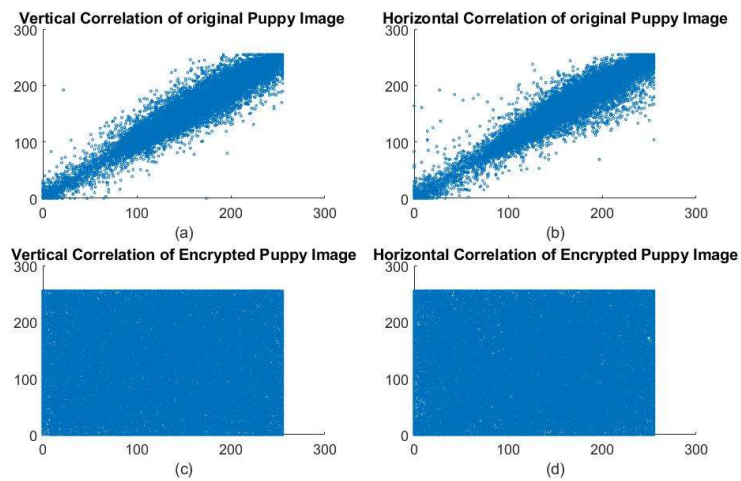
b)



c)



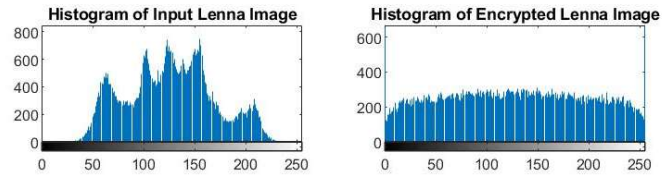
d)



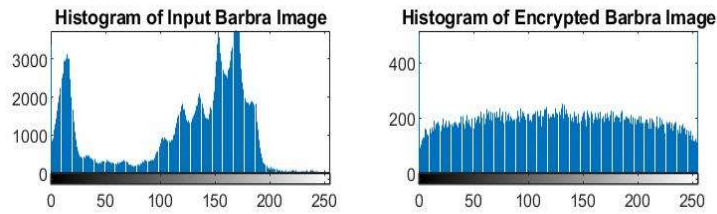
e)

Figure.7.6: Correlation Analysis for input and Encrypted Image: (a) Lenna Image, (b) Babra Image (c) Baboon Image (d) Cameraman Image (e) Puppy Image

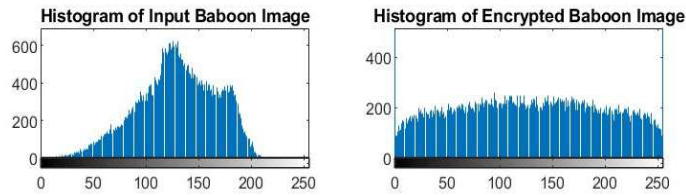
Analyzing a histogram of an image shows how the pixels are distributed; both plain and cypher images must have different histograms. The results of encryption are better when the histogram of a cypher image is uniformly distributed. The non-uniform histograms of many algorithms make them vulnerable to attacks since energy is transformed centralized, so they have uneven histograms. A histogram of a plain image, an encrypted image, and a decrypted image can be seen in Figure 7.7. It can be seen that the algorithm is effective based on the uniform distribution of the encrypted images.



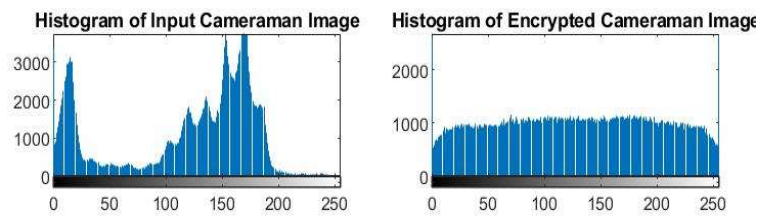
a)



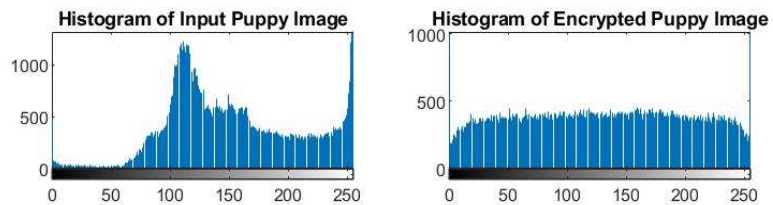
b)



c)



d)



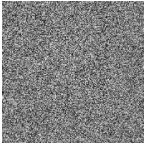


e)

Figure 7. 7: Histogram Analysis for input and Encrypted Image: (a) Lenna Image, (b) Babra Image (c) Baboon Image (d) Cameraman Image (e) Puppy Image

The Confidentiality of the chaotic encryption algorithm depends on the input key-value as it is susceptible to its initial parametric values. Even a one-bit change in Key will not generate the same or even approximate input image, as shown in Table 7.6.

Table 7.6. Key sensitivity Analysis

Input Image	Cypher Image	Decrypted Image Key 1	Decrypted Image Key 2
			

7.4. Comparative analysis

A comparison analysis is performed to investigate the competitiveness of our proposed plan. For Lena image, the values of correlation, entropy, NPCR, and UACI are compared.

Table 7.7. Performance analysis of the SSA and ISSA

Image	SSA			ISSA		
	Entropy	PSNR	MSE	Entropy	PSNR	MSE
Lena	7.9771	33.3	0.00047	7.9975	34.43	0.00036
Baboon	7.9817	32.31	0.00059	7.9963	33.51	0.00045

Camera Man	7.9911	32.02	0.00063	7.9986	39.88	0.0001
Barbara	7.9199	32.47	0.00057	7.9962	32.8	0.00052
Puppy	7.9913	31.96	0.00064	7.9981	35.95	0.00025

Table 7.8. NPCR and UACI Analysis of SSA and ISSA

Image	SSA		ISSA	
	NPCR	UACI	NPCR	UACI
Lena	99.50	33.463	99.60	33.471
Baboon	99.52	33.356	99.56	33.462
Camera Man	99.61	33.343	99.63	33.432
Barbara	99.61	33.464	99.62	33.465
Puppy	99.61	33.433	99.65	33.4635

From table 7.7 and 7.8, we can see that the level of key optimization is accomplished in ISSA was much better than the existing SSA method.

7.4. Conclusion

A secured chaotic tent map-based, improved Salp swarm optimization algorithm is introduced for encrypting an image. The optimal Key was determined by the Improved Salp Swarm Algorithm (ISSA), and the result was discussed. The chaotic functions are applied in confusion and diffusion phases in this scheme for encrypting and lowering the coefficient of correlation between pixels, as well as to enhance the security level of the encryption system as much as feasible. There are some performance metrics to analyze the proposed method's performance,

i.e., encryption time, Entropy, cross-correlation, UACI, PSNR, MSE. The entropy of the proposed technique is close to ideal value eight and is better than SSA. Also, the NPCR and UACI values of ISSA give better results and are resistant to differential cryptanalysis attacks. The experimental results show that Chaotic ISSA significantly enhances the results of chaotic Salp Swarm optimization-based encryption.

CHAPTER 8: CONCLUSION AND FUTURE PRESPECTIVE

The thesis focuses on chaos-based cryptography, using chaotic dynamics to create secure and dependable chaos-based cryptosystems. A unique characteristic of nonlinear dynamical systems is chaotic dynamics. The chaotic system is naturally well suited for cryptography applications due to its complicated nature, random-like behavior, great sensitivity to initial conditions, and ergodicity. We introduced the basics of chaotic maps in Chapter 2. We explained the excellent chaotic features like complex dynamics, random-like behavior, and high sensitivity to the initial conditions that are suitable for encryption purposes. A study of the singularities, fixed points, and periodic points, which should be avoided during the design of cryptosystems, was carried out. Chapter 3 analyzes state-of-the-art and the foundation of chaos-based cryptosystems. We have covered the current issues and potential remedies in the literature review. However, there are still numerous issues that need to be resolved in terms of the cryptosystems' security. The problems that must be addressed include poor or unreliable confusion and diffusion properties, undependable key stream, and complexity. Chapter 4 gives a brief overview of all security analysis that was done on the different methodologies proposed in the system. In the thesis, we propose effective methods and secure chaos-based cryptosystems to overcome the existing problems and enhance the security of cryptosystems. The contributions can be summarized as follows.

In chapter 5, a symmetric key cipher based on chaos has been proposed and tested; it is based on a logistic map with three parameters. Most of the previous work has been done on Picard iterations of the logistic map, picard iterations only use one parameter for key generation and hence have limited chaotic range. In the first methodology, we used three parameters logistic map in the key generation process that increased the key. The proposed technique only uses XOR operators and a single round to solve the complexity problem in chaos-based systems, which is fast and easy to implement. Tests have shown that the proposed scheme has good cryptographic properties and passes the different analyses.

The problem with the methodology proposed in chapter 5 was, using a 3-dimensional Logistic map to secure an image. As our main aim was to reduce the complexity by reducing the number of dimensions, in Chapter 6, we propose a chaos-based symmetric key encryption technique, which is based on superior iterations was implemented. We used both real and imaginary parts of the Superior logistic map. Only one logistic map was used; this reduced the complexity of a higher dimension map, and still provided a similar level of security.

Most of the work done in chaos-based cryptography was in creating symmetric key ciphers; hence in chapter 7, we proposed a secure and robust chaos-based asymmetric key cryptosystem based on chaotic components and a Tent map. A tent map is also a one-dimensional map and is easy to implement. The proposed technique is made up of a new efficient salp swarm optimization, a global diffusion, and a block cipher. Good cryptographic features include a sizeable key space to stop a brute-force attack, a high sensitivity to the secret key, and pseudo-randomness from hiding the relationship between the secret key, the plaintext, and the cipher text. The security analyses and experiment results have shown that the proposed chaos-based cryptosystem has secure and complicated confusion and diffusion.

In the end, this thesis has looked at the problems that already exist in the designs of chaos-based cryptosystems and come up with new ideas and plans to solve them. The analyses and tests that have been done have shown that the proposed solutions are safe and reliable. Most of the work is done on symmetric-key cryptography, and public-key cryptography is unattained. In the future, a cryptographic framework can be designed by using hyperchaotic systems or quantum chaotic systems to create more complex ciphers, and this can increase the key size. Furthermore, an evolutionary algorithm can add potential to the cryptographic process and be applied to other chaotic maps. With the high development of information technology and computer science, computing speed will become faster and faster, accelerating cryptanalysis advances and rendering any cryptographic mechanism or algorithm insecure. Therefore, facing an

increasingly massive amount of confidential information, it is a significant subject to establish a better dialogue between chaos and information security and to explore more efficient and secure technology to ensure information security.

REFERENCES

- [1] Abdulraheem, M., Awotunde, J. B., Jimoh, R. G., & Oladipo, I. D. (2020, November). An efficient lightweight cryptographic algorithm for IoT security. In *International Conference on Information and Communication Technology and Applications* (pp. 444-456). Springer, Cham.
- [2] Agrawal, M., Zhou, J., & Chang, D. (2019). A survey on lightweight authenticated encryption and challenges for securing industrial IoT. In *Security and Privacy Trends in the Industrial Internet of Things* (pp. 71-94). Springer, Cham.
- [3] Ahmad, M., Doja, M. N., & Beg, M. M. S. (2021). Security analysis and enhancements of an image cryptosystem based on hyperchaotic system. *Journal of King Saud University-Computer and Information Sciences*, 33(1), 77-85.
- [4] Antonik, P., Gulina, M., Pauwels, J., & Massar, S. (2018). Using a reservoir computer to learn chaotic attractors, with applications to chaos synchronization and cryptography. *Physical Review E*, 98(1), 012215.
- [5] Arroyo, D., Hernandez, F., & Orúe, A. B. (2017). Cryptanalysis of a classical chaos-based cryptosystem with some quantum cryptography features. *International Journal of Bifurcation and Chaos*, 27(01), 1750004.
- [6] Bader, A. S., & Sagheer, A. M. (2018). Modification on AES-GCM to increment ciphertext randomness. *transactions of International Journal of Mathematical Sciences and Computing*, 4, 34-40.
- [7] Bansal, R., Gupta, S., & Sharma, G. (2017). An innovative image encryption scheme based on chaotic map and Vigenère scheme. *Multimedia Tools and Applications*, 76(15), 16529-16562.
- [8] Belazi, A., Abd El-Latif, A. A., Diaconu, A. V., Rhouma, R., & Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Optics and Lasers in Engineering*, 88, 37-50.
- [9] Cao, J., & Chugh, R. (2018). Chaotic behavior of logistic map in superior orbit and an improved chaos-based traffic control model. *Nonlinear Dynamics*, 94(2), 959-975.
- [10] Çavuşoğlu, Ü., Kaçar, S., Pehlivan, I., & Zengin, A. (2017). Secure image encryption algorithm design using a novel chaos-based S-Box. *Chaos, Solitons & Fractals*, 95, 92-101.

- [11] Chaudhury, P., Dhang, S., Roy, M., Deb, S., Saha, J., Mallik, A., ... & Das, R. (2017, August). ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm. In *2017 8th Annual Industrial Automation and Electromechanical Engineering Conference (IEMECON)* (pp. 332-337). IEEE.
- [12] El-Haii, M., Chamoun, M., Fadlallah, A., & Serhrouchni, A. (2018, October). Analysis of cryptographic algorithms on iot hardware platforms. In *2018 2nd Cyber Security in Networking Conference (CSNet)* (pp. 1-5). IEEE.
- [13] Essaid, M., Akharraz, I., Saaidi, A., & Mouhib, A. (2019, April). A novel image encryption scheme based on permutation/diffusion process using an improved 2D chaotic system. In *2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS)* (pp. 1-6). IEEE.
- [14] Facon, A., Guilley, S., Lec'Hvien, M., Schaub, A., & Souissi, Y. (2018, July). Detecting cache-timing vulnerabilities in post-quantum cryptography algorithms. In *2018 IEEE 3rd International Verification and Security Workshop (IVSW)* (pp. 7-12). IEEE.
- [15] Garcia-Bosque, M., Pérez-Resca, A., Sánchez-Azqueta, C., Aldea, C., & Celma, S. (2018). Chaos-based bitwise dynamical pseudorandom number generator on FPGA. *IEEE Transactions on Instrumentation and Measurement*, 68(1), 291-293.
- [16] Gatta, M. T., & Abd Al-latif, S. T. (2018, May). Medical image security using modified chaos-based cryptography approach. In *Journal of Physics: Conference Series* (Vol. 1003, No. 1, p. 012036). IOP Publishing.
- [17] Halagali, B. P., & Desai, V. V. (2018, April). Implementation of chaos-based cryptography in kasumi block cipher. In *2018 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0165-0169). IEEE.
- [18] Harba, E. S. I. (2017). Secure data encryption through a combination of AES, RSA and HMAC. *Engineering, Technology & Applied Science Research*, 7(4), 1781-1785.
- [19] Hoang, T. M. (2019, October). A Chaos-based image cryptosystem using nonstationary dynamics of logistic map. In *2019 International Conference on Information and Communication Technology Convergence (ICTC)* (pp. 591-596). IEEE.

- [20] Ilayaraja, M., Shankar, K., & Devika, G. (2017). A modified symmetric key cryptography method for secure data transmission. *International Journal of Pure and Applied Mathematics*, 116(10), 301-308.
- [21] Iqbal, A., & Iqbal, T. (2018, October). Low-cost and secure communication system for remote micro-grids using AES cryptography on ESP32 with LoRa module. In *2018 IEEE Electrical Power and Energy Conference (EPEC)* (pp. 1-5). IEEE.
- [22] Karthick, S., Sankar, S. P., & Prathab, T. R. (2018, July). An approach for image encryption/decryption based on quaternion fourier transform. In *2018 International Conference on Emerging Trends and Innovations in Engineering and Technological Research (ICETIETR)* (pp. 1-7). IEEE.
- [23] Kaur, G., Agarwal, R., & Patidar, V. (2020). Chaos based multiple order optical transform for 2D image encryption. *Engineering Science and Technology, an International Journal*, 23(5), 998-1014.
- [24] Kaur, G., Singh, K., & Gill, H. S. (2021). Chaos-based joint speech encryption scheme using SHA-1. *Multimedia Tools and Applications*, 80(7), 10927-10947.
- [25] Kumar, T. M., & Karthigaikumar, P. (2018). FPGA implementation of an optimized key expansion module of AES algorithm for secure transmission of personal ECG signals. *Design Automation for Embedded Systems*, 22(1), 13-24.
- [26] Kumar, T., & Chauhan, S. (2018). Image cryptography with matrix array symmetric key using chaos-based approach. *International Journal of Computer Network and Information Security*, 10(3), 60.
- [27] Kumar, V., & Girdhar, A. (2021). A 2D logistic map and Lorenz-Rosler chaotic system based RGB image encryption approach. *Multimedia Tools and Applications*, 80(3), 3749-3773.
- [28] Lawnik, M. (2017, December). Generalized logistic map and its application in chaos-based cryptography. In *Journal of Physics: Conference Series* (Vol. 936, No. 1, p. 012017). IOP Publishing.
- [29] Li, C., Luo, G., & Li, C. (2019). An Image Encryption Scheme Based on The Three-dimensional Chaotic Logistic Map. *Int. J. Netw. Secur.*, 21(1), 22-29.
- [30] Li, Z., Peng, C., Tan, W., & Li, L. (2020). A novel chaos-based colour image encryption scheme using bit-level permutation. *Symmetry*, 12(9), 1497.

- [31] Liu, H., Kadir, A., Sun, X., & Li, Y. (2018). Chaos based adaptive double-image encryption scheme using hash function and S-boxes. *Multimedia Tools and Applications*, 77(1), 1391-1407.
- [32] Lu, Q., Zhu, C., & Deng, X. (2020). An efficient image encryption scheme based on the LSS chaotic map and single S-box. *IEEE Access*, 8, 25664-25678.
- [33] Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*, 78(15), 22023-22043.
- [34] Maddodi, G., Awad, A., Awad, D., Awad, M., & Lee, B. (2018). A new image encryption algorithm based on heterogeneous chaotic neural network generator and dna encoding. *Multimedia Tools and Applications*, 77(19), 24701-24725.
- [35] Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., & Ahmad, W. (2020). Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. *IEEE Access*, 8, 35682-35695.
- [36] Manisekaran, P., Dhivakar, M. A., & Kumar, P. (2020, March). Enhanced Image Encryption using multiple iterated Arnold Coupled Logistic Map Lattices. In *2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC)* (pp. 514-521). IEEE..
- [37] Mezher, A. E. (2018). Enhanced RSA cryptosystem based on multiplicity of public and private keys. *International Journal of Electrical and Computer Engineering*, 8(5), 3949.
- [38] Murillo-Escobar, M. A., Meranza-Castillón, M. O., López-Gutiérrez, R. M., & Cruz-Hernández, C. (2019). Suggested integral analysis for chaos-based image cryptosystems. *Entropy*, 21(8), 815.
- [39] Nardo, L. G., Nepomuceno, E. G., Bastos, G. T., Santos, T. A., Butusov, D. N., & Arias-Garcia, J. (2021). A reliable chaos-based cryptography using Galois field. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, 31(9), 091101.
- [40] Nesa, N., Ghosh, T., & Banerjee, I. (2019). Design of a chaos-based encryption scheme for sensor data using a novel logarithmic chaotic map. *Journal of Information Security and Applications*, 47, 320-328.
- [41] Noura, H., Chehab, A., Sleem, L., Noura, M., Couturier, R., & Mansour, M. M. (2018). One round cipher algorithm for multimedia IoT devices. *Multimedia tools and applications*, 77(14), 18383-18413.

- [42] Özkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption. *Nonlinear Dynamics*, 92(2), 305-313.
- [43] Preishuber, M., Hütter, T., Katzenbeisser, S., & Uhl, A. (2018). Depreciating motivation and empirical security analysis of chaos-based image and video encryption. *IEEE Transactions on Information Forensics and Security*, 13(9), 2137-2150.
- [44] Raza, S. F., & Satpute, V. (2019). A novel bit permutation-based image encryption algorithm. *Nonlinear Dynamics*, 95(2), 859-873.
- [45] Rfifi, S., Maafiri, A., Choug dali, K., & Gueddana, A. (2021). A new efficient model of quantum image cryptography based on sampled GNEQR storage presentation. *Journal of the Korean Physical Society*, 78(7), 618-626.
- [46] Rodríguez, J., Corredor, B., & Suárez, C. (2019). Genetic Operators Applied to Symmetric Cryptography. *International Journal of Interactive Multimedia & Artificial Intelligence*, 5(7).
- [47] Safi, H. W., & Maghari, A. Y. (2017, October). Image encryption using double chaotic logistic map. In *2017 International Conference on Promising Electronic Technologies (ICPET)* (pp. 66-70). IEEE.
- [48] Saha, R., & Geetha, G. (2017). Symmetric random function generator (SRFG): A novel cryptographic primitive for designing fast and robust algorithms. *Chaos, Solitons & Fractals*, 104, 371-377.
- [49] Saho, N. J. G., & Ezin, E. C. (2020). Survey on Asymmetric Cryptographic Algorithms in Embedded Systems. *IJISRT*, 5, 544-554.
- [50] Santos, T. A., Magalhaes, E. P., Fiorio, D. R., & Nepomuceno, E. G. (2019). On the reliability of computational chaos-based cryptography for information exchange. *arXiv preprint arXiv:1910.06116*.
- [51] Sasikaladevi, N., Geetha, K., Sriharshini, K., & Aruna, M. D. (2020). H3-hybrid multilayered hyper chaotic hyper elliptic curve-based image encryption system. *Optics & Laser Technology*, 127, 106173.
- [52] Sato, M., & Matsuo, S. I. (2017, July). Long-term public blockchain: Resilience against compromise of underlying cryptography. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1-8). IEEE.
- [53] Scholz, D., Oeldemann, A., Geyer, F., Gallenmüller, S., Stubbe, H., Wild, T., ... & Carle, G. (2019, September). Cryptographic hashing in p4 data planes. In *2019*

ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS) (pp. 1-6). IEEE.

- [54] Shah, A. A., Parah, S. A., Rashid, M., & Elhoseny, M. (2020). Efficient image encryption scheme based on generalized logistic map for real time image processing. *Journal of Real-Time Image Processing*, 17(6), 2139-2151.
- [55] Shankar, K., Elhoseny, M., Chelvi, E. D., Lakshmanaprabu, S. K., & Wu, W. (2018). An efficient optimal key based chaos function for medical image security. *IEEE Access*, 6, 77145-77154.
- [56] Sharma, M., & Bharti, V. (2020, July). Image encryption using a new 2D bit reversed logistic map. In *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.
- [57] Taha, M. A., Assad, S. E., Queudet, A., & Deforges, O. (2017). Design and efficient implementation of a chaos-based stream cipher. *International Journal of Internet Technology and Secured Transactions*, 7(2), 89-114.
- [58] Teh, J. S., Alawida, M., & Sii, Y. C. (2020). Implementation and practical problems of chaos-based cryptography revisited. *Journal of Information Security and Applications*, 50, 102421.
- [59] Teh, J. S., Tan, K., & Alawida, M. (2019). A chaos-based keyed hash function based on fixed point representation. *Cluster Computing*, 22(2), 649-660.
- [60] Tuna, M. (2020). A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: Design and its FPGA implementation. *Analog Integrated Circuits and Signal Processing*, 105(2), 167-181.
- [61] Vyakaranal, S., & Kengond, S. (2018, April). Performance analysis of symmetric key cryptographic algorithms. In *2018 International Conference on Communication and Signal Processing (ICCSP)* (pp. 0411-0415). IEEE.
- [62] Wu, M., Li, Y., Liu, W., & Huang, M. (2020, November). A Novel Color Image Encryption Mechanism Based on Visual Cryptography, SHA-512 and One-time Password. In *Proceedings of the 2020 4th International Conference on Electronic Information Technology and Computer Engineering* (pp. 438-443).
- [63] Xiang, H., & Liu, L. (2020). An improved digital logistic map and its application in image encryption. *Multimedia Tools and Applications*, 79(41), 30329-30355.

- [64] Xu, Q., Sun, K., & Zhu, C. (2020). A visually secure asymmetric image encryption scheme based on RSA algorithm and hyperchaotic map. *Physica Scripta*, 95(3), 035223.
- [65] Yang, B., & Liao, X. (2018). A new color image encryption scheme based on logistic map over the finite field \mathbb{Z}_N . *Multimedia Tools and Applications*, 77(16), 21803-21821.
- [66] Ye, G., Jiao, K., Pan, C., & Huang, X. (2018). An effective framework for chaotic image encryption based on 3D logistic map. *Security and Communication Networks*, 2018.
- [67] Zhang, X., Nie, W., Ma, Y., & Tian, Q. (2017). Cryptanalysis and improvement of an image encryption algorithm based on hyper-chaotic system and dynamic S-box. *Multimedia Tools and Applications*, 76(14), 15641-15659.
- [68] Zhou, B., Egele, M., & Joshi, A. (2017, September). High-performance low-energy implementation of cryptographic algorithms on a programmable SoC for IoT devices. In *2017 IEEE High Performance Extreme Computing Conference (HPEC)* (pp. 1-6). IEEE.
- [69] Zhou, L., Chen, J., Zhang, Y., Su, C., & James, M. A. (2019). Security analysis and new models on the intelligent symmetric key encryption. *Computers & Security*, 80, 14-24.
- [70] Khan, J. S., & Ahmad, J. (2019). Chaos based efficient selective image encryption. *Multidimensional Systems and Signal Processing*, 30(2), 943-961.
- [71] Kumari, M., Gupta, S., & Sardana, P. (2017). A survey of image encryption algorithms. *3D Research*, 8(4), 37.
- [72] Kumar, T., & Chauhan, S. (2018). Image cryptography with matrix array symmetric key using chaos-based approach. *International Journal of Computer Network and Information Security*, 10(3), 60.
- [73] Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. *Journal of Information and Telecommunication*, 2(2), 181-191.
- [74] Li, C., Luo, G., Qin, K., & Li, C. (2017). An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics*, 87(1), 127-133.
- [75] Luo, Y., Yu, J., Lai, W., & Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools and Applications*, 78(15), 22023-22043.

- [76] Masood, F., Ahmad, J., Shah, S. A., Jamal, S. S., & Hussain, I. (2020). A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map. *Entropy*, 22(3), 274.
- [77] Mekki, N., Hamdi, M., Aguilu, T., & Kim, T. H. (2018, April). A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system. In 2018 International Conference on Advanced Communication Technologies and Networking (CommNet) (pp. 1-10). IEEE.
- [78] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. *International Journal of Applied Engineering Research*, 12(23), 13265-13280.
- [79] Munir, F. A., Zia, M., & Mahmood, H. (2019). Designing multi-dimensional logistic map with fixed-point finite precision. *Nonlinear Dynamics*, 97(4), 2147-2158.
- [80] Suneja, K., Dua, S., & Dua, M. (2019, March). A review of chaos-based image encryption. In 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC) (pp. 693-698). IEEE.
- [81] Tutueva, A. V., Karimov, T. I., Moysis, L., Nepomuceno, E. G., Volos, C., & Butusov, D. N. (2021). Improving chaos-based pseudo-random generators in finite-precision arithmetic. *Nonlinear Dynamics*, 104(1), 727-737.
- [82] Elmanfaloty, Rania. A., & Abou-Bakr, E. (2020). An image encryption scheme using a 1D chaotic double section skew tent map. *Complexity*, 2020.
- [83] Pham, V. T., Vaidyanathan, S., Volos, C. K., Jafari, S., & Gotthans, T. (2017). A three-dimensional chaotic system with square equilibrium and no-equilibrium. In *Fractional order control and synchronization of chaotic systems* (pp. 613-635). Springer, Cham.
- [84] Facon, A., Guilley, S., Lec'Hvien, M., Schaub, A., & Souissi, Y. (2018, July). Detecting cache-timing vulnerabilities in post-quantum cryptography algorithms. In 2018 IEEE 3rd International Verification and Security Workshop (IVSW) (pp. 7-12). IEEE.
- [85] Ilayaraja, M., Shankar, K., & Devika, G. (2017). A modified symmetric key cryptography method for secure data transmission. *International Journal of Pure and Applied Mathematics*, 116(10), 301-308.

- [86] Gatta, M. T., & Abd Al-latief, S. T. (2018, May). Medical image security using modified chaos-based cryptography approach. In *Journal of Physics: Conference Series* (Vol. 1003, No. 1, p. 012036). IOP Publishing.
- [87] Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos*, 8(06), 1259-1284.
- [88] Abbasi S.F., Ahmad J., Khan J.S., Khan M.A., Sheikh S.A. (2019) Visual Meaningful Encryption Scheme Using Intertwining Logistic Map. In: Arai K., Kapoor S., Bhatia R. (eds) *Intelligent Computing. SAI 2018. Advances in Intelligent Systems and Computing*, vol 857. Springer
- [89] Ahmad, M., Alam, M.Z., Umayya, Z. et al. An image encryption approach using particle swarm optimization and chaotic map. *International Journal of Information Technology* 10, 247–255 (2018).
- [90] Batool, S.I., Waseem, H.M. A novel image encryption scheme based on Arnold scrambling and Lucas series. *Multimedia Tools and Appl* 78, 27611–27637 (2019).
- [91] Broumandnia, A. “The 3D modular chaotic map to digital color image encryption” *Future Generation Computer Systems* 99, 489-499(2019).
- [92] C. E. Shannon, "Communication theory of secrecy systems," in *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, Oct. 1949, doi: 10.1002/j.1538-7305.1949.tb00928.x.
- [93] Cavusogul, U., Kacar, S. “A Novel Parallel Image Encryption Algorithm based on chaos.” *Cluster Computing*, 22(4) , 1211(2019).
- [94] Chen, C. ,Sun H.K. and S. B. He, ``A class of higher-dimensional hyperchaotic maps," *Eur. Phys. J. Plus*, 134, 410, (2019).
- [95] Chen, J., Han, F. and Qian, W. “Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map”, *Nonlinear Dyn* 93, 2399–2413 (2018).
- [96] X. Zhang, L. Wang, Z. Zhou and Y. Niu, "A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals," in *IEEE Access*, vol. 7, pp. 74734-74746, 2019.
- [97] Wu, Y., Yang, G., Jin, H., and Noonan, J. P., “Image encryption using the two-dimensional logistic chaotic map”, *Journal of Electronic Imaging*, vol. 21, no. 1, 2012.
- [98] Abdullah, M.Z., Khaleefah, Z.J., 2017. Design and implement of a hybrid cryptography textual system. In: *2017 International Conference on Engineering and*

Technology (ICET), IEEE, pp. 1–6.

- [99] Alawida, M., Samsudin, A., Teh, J.S., 2019. Enhancing unimodal digital chaotic maps through hybridisation. *Nonlinear Dyn.* 96 (1), 601–613.
- [100] Alawida, M., Samsudin, A., Teh, J.S., Alkhaldeh, R.S., 2019. A new hybrid digital chaotic system with applications in image encryption. *Signal Process.* 160, 45– 58.
- [101] Abdel-Aziz, M.M.; Hosny, K.M.; Lashin, N.A. Improved data hiding method for securing color images. *Multimed. Tools Appl.* **2021**, 80, 12641–12670.
- [102] Li, N.; Huang, F. Reversible data hiding for JPEG images based on pairwise nonzero AC coefficient expansion. *Signal Process.* **2020**, 171, 107476.
- [103] Hosny, K.M.; Darwish, M.M.; Li, K.; Salah, A. Parallel Multi-Core CPU and GPU for Fast and Robust Medical Image Watermarking. *IEEE Access* **2018**, 6, 77212–77225.
- [104] Hosny, K.M.; Darwish, M.M. Robust color image watermarking using invariant quaternion Legendre-Fourier moments. *Multimed. Tools Appl.* **2018**, 77, 24727–24750.
- [105] Hosny, K.M.; Darwish, M.M. Invariant image watermarking using accurate Polar Harmonic Transforms. *Comput. Electr. Eng.* **2017**, 62, 429–447.
- [106] Mekki, Neila & Hamdi, Mohamed & Aguil, Taoufik & Kim, Tai-hoon. (2018). A real-time chaotic encryption for multimedia data and application to secure surveillance framework for IoT system.