



REPUBLIC OF TÜRKİYE
ALTINBAŞ UNIVERSITY
Institute of Graduate Studies
Information Technologies

**SECURE DATA STORAGE IN CLOUD USING
STEGANOGRAPHY AND VISUAL
CRYPTOGRAPHY**

Asmaa Yaareb Hameed ALBAKRI

Master's Thesis

Supervisor

Asst.Prof. Dr. Oğuz KARAN

Istanbul, 2023

SECURE DATA STORAGE IN CLOUD USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

Asmaa Yaareb Hameed ALBAKRI

Information Technologies

Master's Thesis

ALTINBAŞ UNIVERSITY

2023

The thesis titled SECURE DATA STORAGE IN CLOUD USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY prepared by Asmaa Yaareb ALBAKRI and submitted on 27/12/2023 has been **accepted unanimously** for the degree of Master of Science in Information Technologies.

Asst.Prof. Dr. Oguz KARAN

Supervisor

Thesis Defence Committee Members:

Asst.Prof. Dr. Oguz KARAN

Department of Software
Engineering,

Altınbaş University

Academic Title - First/Last Name

Department,

University

Academic Title - First/Last Name

Department,

University

I hereby declare that this thesis meets all format and submission requirements of a Master's Thesis.

Submission date of the thesis to Institute of Graduate Studies: ____/____/____

I hereby declare that all information/data presented in this graduation project has been obtained in full accordance with academic rules and ethical conduct. I also declare all unoriginal materials and conclusions have been cited in the text and all references mentioned in the Reference List have been cited in the text, and vice versa as required by the abovementioned rules and conduct.

Asmaa Yaareb Hameed ALBAKRI

Signature

ABSTRACT

SECURE DATA STORAGE IN CLOUD USING STEGANOGRAPHY AND VISUAL CRYPTOGRAPHY

ALBAKRI, Asmaa Yaareb Hameed

M.Sc., Information Technologies, Altınbaş University,

Supervisor: Asst. Prof. Dr. Oğuz KARAN

Date: December / 2023

Pages: 76

Due to the fact that digital images include sensitive data from a variety of sources, including human, medical, satellite, and biometric, among others, they necessitate the highest level of security. The images in question include a multitude of vulnerabilities. In this era of cloud computing and virtualization, securing data from hackers requires an effective method that employs a hybrid algorithm to preserve data from several sorts of hackers. Visual image encryption and LSB steganography are two essential security techniques for protecting sensitive images from unauthorized access and modification. Image encryption transforms the image data into an unintelligible form, while steganography embeds the image data in a cover image to conceal its existence. The study of the behavior of dynamic systems that are extremely sensitive to initial conditions is chaos theory. Chaotic systems are useful for image encryption and steganography due to their unpredictable and erratic behavior.

This thesis proposes a new and improved system for color image encryption and steganography based on chaos theory. Using a novel chaotic-based encryption algorithm, the proposed approach uses the Lorenz system to generate a random key to encrypt the color image. The encrypted image is then embedded in a cover image using a novel chaotic-based steganography algorithm. The stego image is then transmitted or stored securely.

The proposed system has several advantages over existing methods. First, it is more secure and resistant to attacks because it uses two chaotic systems, the Lorenz system, the Henon map, and the novel encryption and steganography algorithms. Second, it is more scalable

and efficient due to using the Lorenz system, which is a relatively simple chaotic system. Third, it is more compatible with existing image and video formats.

This thesis also provides a comprehensive performance evaluation of the proposed system. The experimental results show that the proposed approach is highly secure, scalable, and efficient. The proposed method is also compatible with existing image and video formats.

Keywords: Color Image Encryption, LSB Steganography, Chaos Theory, Lorenz System, Henon Map.



TABLE OF CONTENTS

	<u>Pages</u>
ABSTRACT	v
LIST OF TABLES.....	xi
LIST OF FIGURES.....	xii
ABBREVIATIONS.....	xv
LIST OF SYMBOLS.....	xvii
1. INTRODUCTION	1
1.1 BACKGROUND	1
1.2 MOTIVATION	1
1.3 OVERVIEW OF THE PROPOSED SYSTEM	2
1.4 AIMS OF THE THESIS	2
1.5 IMAGE ENCRYPTION AND STEGANOGRAPHY BASED ON CHAOS.....	3
1.6 THESIS OUTLINE.....	3
2. LITERATURE REVIEW FOR IMAGE SECURITY BASED ON CHAOS.....	5
2.1 INTRODUCTION	5
2.2 CHAOS DEFINITION	5
2.3 TYPES OF CHAOTIC SYSTEMS	6
2.3.1 Chaotic Maps	6
2.3.2 Chaotic Flows	7
2.3.2.1 Rossler system	8
2.3.2.2 Lorenz system.....	8
2.3.2.3 The lorenz system properties.....	10
2.4 CHAOS-BASED CRYPTOGRAPHY	11
2.5 IMAGE ENCRYPTION ALGORITHMS	12

2.5.1 Pixel Value Transform (Changing Pixel Value).....	12
2.5.2 Transform of the Pixel Position (Changing Pixel Coordinate).....	13
2.6 ADVANTAGES OF USING CHAOS IN IMAGE ENCRYPTION.....	14
2.7 STEGANOGRAPHY.....	14
2.7.1 LSB Steganography Advantages	15
2.7.2 LSB Steganography Disadvantages	15
2.7.3 Purposes of Steganography	15
2.7.4 Limitations of the Steganography	16
2.8 THE QUALITY OF IMAGE MEASUREMENTS	16
2.8.1 Histogram Analysis.....	16
2.8.2 The Correlation Coefficient	17
2.8.3 Mean Square Error (MSE).....	17
2.8.4 Peak Signal-to-Noise Ratio (PSNR)	17
2.8.5 Structural Similarity Index Measure (SSIM).....	18
2.8.6 Entropy.....	18
2.8.7 Differential Analysis	19
2.8.7.1 Number of pixels change rate (NPCR).....	19
2.8.7.2 Unified average changing intensity (UACI).....	19
2.8.8 Brute-Force Analysis	20
2.8.8.1 Key sensitivity	20
2.8.8.2 Keyspace analysis.....	20
2.9 CLOUD STORAGE.....	20
2.9.1 Advantages of Cloud Storage	21
2.9.2 The Disadvantages of the Cloud Storage.....	21
2.9.3 Tips for Selecting a Cloud Storage Provider	21

2.10 RELATED WORKS	22
3. THE PROPOSED MODEL BASED ON CRYPTOGRAPHY STEGANOGRAPHY	27
3.1 INTRODUCTION	27
3.2 THE PROPOSED SYSTEM MODEL	27
3.3 GENERATION OF CHAOTIC RANDOM INTEGER NUMBER (CRIN).....	29
3.4 CHAOS-BASED VISUAL ENCRYPTION (CBVE)	30
3.5 CHAOS BASED-LSB STEGANOGRAPHY	32
3.6 CONCLUSION.....	34
4. THE SIMULATION RESULTS	35
4.1 INTRODUCTION	35
4.2 THE IMAGES USE TO EVALUATING THE PROPOSED SYSTEM.....	35
4.3 SIMULATION RESULT OF THE CBVE METHOD	37
4.3.1 Testing Parameters of the Lorenz Based on Lyapunov Exponents	37
4.3.2 The Residual Unintelligibility of Encrypted Image.....	38
4.3.3 Brute-Force Attack for the Lorenz System-Based Chaos-Based Visual Encryption (CBVE) Method	42
2.3.3.1 Key sensitivity	42
2.3.3.2 Keyspace based on lorenz system	43
4.3.4 Advantages of The CBVE Method-Based Image Encryption	44
4.4 RESULTS OF LSB STEGANOGRAPHY BASED ON HENON MAP	45
4.4.1 Embedded and Reconstructed Images Results.....	45
4.4.2 The Brute-Force Attack for LSB Steganography Using Henon Chaotic Map	49
4.4.3 Saved Image Types for the Stego Images.....	51
4.5 THE SIMULATION RESULTS OVER ALL THE PROPOSED SYSTEM.....	51
4.5.1 The Security Results	52

4.5.2 Brute-Force Attacks Over all the Proposed System.....	55
4.5.3 Comparing the Proposed System to Previous Research	56
5. CONCLUSIONS AND FUTURE WORK.....	58
5.1 CONCLUSIONS.....	58
5.2 FUTURE WORKS.....	59
REFERENCES	60



LIST OF TABLES

	<u>Pages</u>
Table 2.1: The Summarize of Related Works.	26
Table 4.1: Details of the Set Images Using in the Proposed System.	35
Table 4.2: Testing the Lorenz Parameters using the Lyapunov Exponent.....	38
Table 4.3: Encryption Results Based on the XOR and Lorenz System.	41
Table 4.4: Decryption Results Based on the XOR and Lorenz System.	41
Table 4.5: The Steganography and De-Steganography Results.	48
Table 4.6: Simulation Results for the Images in Figure 4.18.....	53
Table 4.7: Simulation Results for the Images in Figure 4.19.....	53
Table 4.8: Simulation Results for the Images in Figure 4.20.....	54
Table 4.10: The Simulation Results for Other Research.....	57
Table 4.11: The Keyspace the Proposed System is Compressed with the Other Articles...57	

LIST OF FIGURES

	<u>Pages</u>
Figure 2.1: (A) Time Series and (B) Attractor (X) of Henon Map.	7
Figure 2.2: Sensitivity to Changing of Initial Values.....	7
Figure 2.3: Rössler System Flow (A) the Strange Attractor, (B) the Time Series (T).....	8
Figure 3.1: General Diagram of the Proposed Scheme.	28
Figure 3.2: Increasing Randomness by Multiplying and Mod.	30
Figure 3.3: Image Encryption Based on CBVE.	31
Figure 3.4: Converting the Encrypted Secret Image to Binary form.	32
Figure 3.5: The Flowchart of the Steps of Chaotic Scrambling.....	34
Figure 4.1: (Image 1), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc., and Dec. Images Based on CBVE Method.	39
Figure 4.2: (Image 2), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc., and Dec. Images Based on CBVE Method.	39
Figure 4.3: (Image 8), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc, and Dec. Images Based on CBVE Method.	40
Figure 4.4: (Image 9), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc., and Dec. Images Based on CBVE Method.	40
Figure 4.5: Decrypted Image 8 by Changing the $Z(1)$ by 10^{-15}	43
Figure 4.6: Decrypted Image 8 by Changing the Parameter (b) by 10^{-15}	43
Figure 4.7: The Results of LSB Steganography Based on Henon for Embedded Image 1 Inside Image 3.	46
Figure 4.8: Recovered the Hidden Image 1 from the Stego Image Using the Same Initial Values and Parameters of Henon Map.	46
Figure 4.9: The Results of LSB Steganography Based on Henon for Embedded Image 2 Inside Image 5	46

Figure 4.10: Recovered the Hidden Image 2 from the Stego Image Using the Same Initial Values and Parameters of Henon Map.	47
Figure 4.11: The Results of LSB Steganography Based on Henon for Embedded Image 8 Inside Image 11.	47
Figure 4.12: Recovered the Hidden Image 8 from the Stego Image Using the Same Initial Values and Parameters of the Henon Map.	47
Figure 4.13: The Results of LSB Steganography Based on Henon for Embedded Image 9 Inside Image 10.	48
Figure 4.14: Recovered the Hidden Image 9 from the Stego Image Using the Same Initial Values and Parameters of Henon Map.	48
Figure 4.15: Recovered the Secret Image from the Stego Image at $\Delta x=2e-16$. (A) Original Secret Image 1 and (B) Recovered Secret Image.	49
Figure 4.16: Recovered the Secret Image from the Stego Image at $\Delta y=2e-16$. (A) Original Secret Image 4 and (B) Recovered Secret Image.	50
Figure 4.17: Recovered the Secret Image from the Stego Image at $\Delta r=2e-16$. (A) Original Secret Image 9 and (B) Recovered Secret Image.	50
Figure 4.18: Images and Histogram Plots for A- Secret Image 4 B- Cover Image 11 C- Encrypted Image D- Steg Image E- Rec of Enc Image F- Dec of Rec. Image.	52
Figure 4.19: Images and Histogram Plots for A- Secret Image 1 B- Cover Image 6 C- Encrypted Image D- Steg. Image E- Rec of Enc Image F- Dec of Rec Image.	53
Figure 4.20: Images and Histogram Plots for A- Secret Image 9 B- Cover Image 3 C- Encrypted Image D- Steg Image E- Rec of Enc Image. F- Dec of Rec Image.	54
Figure 4.21: Recovered the Secret Image After Changed X(1) of Lorenz System by $1e-15$	55
Figure 4.22: Recovered the Secret Image After Changed Sigma of Lorenz System by $1e-15$	55
Figure 4.23: Recovered the Secret Image After Changed Y(1) of the Henon Map by $1e-15$	55

Figure 4.24: Recovered the Secret Image After Changed (B) Parameter of the Henon Chaotic Map by $1e-15$	56
---	----



ABBREVIATIONS

AES	:	Advanced Encryption Standard
Corr	:	Correlation Coefficient
CRIN	:	Chaotic Random Integer Numbers
CRP	:	Generation Chaotic Random Position
D	:	Diagonal
Dec.	:	Decryption
DES	:	Data Encryption Standard
DSA	:	Digital Signature Algorithm
E	:	Entropy
EI	:	Encrypted Image
Enc.	:	Encryption
H	:	Horizontal
HCRS	:	Hyper Chaotic Rabinovitch System
HCS	:	Hyper-Chaotic Sequence
IDEA	:	Individuals with Disabilities Education Act
LUT	:	Scrambler Look-Up Table
MSE	:	Mean Square Error
PRNG	:	Pseudo-Random Number Generator
PSNR	:	Peak Signal-to-Noise Ratio
RSA	:	Rivest-Shamir-Adleman
Sec	:	Second
SSIM	:	Structural Similarity Index Measure
V	:	Vertical
LSB	:	Least Significant Bits

CBVE	:	Chaos Based-Visual Encryption
ODEs	:	Ordinary Differential Equations
DSC	:	Distance Scrambling Factor
CCMF	:	Correlation Coefficient Measuring Factor
MD	:	Maximum Deviation Analysis
Ent	:	Entropy
NPCR	:	Number of Pixels Change Rate
UACI	:	Unified Average Changing Intensity
SVD	:	Singular Value Decomposition

LIST OF SYMBOLS

$g(.)$	:	Iterative Function
x_k	:	State Vector
$\sigma, r, \text{ and } b$	:	Parameter
$\dot{x}, \dot{y}, \dot{z}$	:	Parameter for the Lorenz System
$M \text{ and } N$	:	The Image's Dimensions
(i,j)	:	Pixel's Coordinate
$x, \text{ and } y$	:	Unencrypted and Encrypted Versions of the Same Frame
$\mu_x, \mu_y \text{ are the average}$	:	Average of x and y
σ_x^2, σ_y^2	:	Variance of x and y
σ_{xy}	:	Covariance of x and y .
$P(i)$	:	Probability of Event I in Bits
$R \text{ \& } C$	:	Dimensions of Clear and Encrypted Images

1. INTRODUCTION

1.1 BACKGROUND

Visual image encryption [1] [3] and LSB steganography [4] [7] are two important security techniques for protecting sensitive images from unauthorized access and modification. Image encryption transforms the image data into an unintelligible form, while steganography embeds the image data in a cover image to conceal its existence.

Chaos theory is a branch of mathematics that studies the behavior of dynamic systems highly sensitive to initial conditions [8][11]. Chaotic systems are characterized by their unpredictable and random behavior, making them ideal for image encryption and steganography.

Chaos-based image encryption algorithms typically use chaotic maps to generate random keys to scramble the image data [12][14]. The encrypted image is then transmitted or stored securely. Chaos-based steganography algorithms use chaotic maps to generate random locations in a cover image where the secret image data can be embedded [15][18]. The stego image is then transmitted or stored in a way that is indistinguishable from the original cover image.

Steganography and image encryption based on chaos have a number of advantages over alternative techniques, including:

- a. Due to the difficulty in predicting chaotic systems, algorithms for steganography and image encryption based on chaos are highly resistant to attacks.
- b. Encryption and embedding algorithms based on chaos-based image steganography are scalable; they can process images of any size.
- c. Efficiency: Encryption and steganography algorithms based on chaos are comparatively effective and can embed and encrypt images in real time.

1.2 MOTIVATION

Color images are increasingly used in various applications, including telemedicine, cloud computing, and military intelligence. However, the widespread use of color images makes them a cyberattack target. Image encryption and steganography are effective techniques for

protecting color images from unauthorized access and modification. Existing color image encryption and steganography methods have several limitations, including:

- a. Security vulnerabilities: Some existing methods are vulnerable to various attacks, such as statistical attacks, brute-force attacks, and steganalysis attacks.
- b. Scalability issues: Some existing methods are not scalable enough to encrypt and embed large color images in real-time.
- c. Efficiency concerns: Some existing methods are not efficient in terms of either time or space complexity.

1.3 OVERVIEW OF THE PROPOSED SYSTEM

The proposed system combines two chaotic systems, the Lorenz system, and the Henon map, to achieve high security for color image encryption and steganography. The Lorenz system is a chaotic system known for its unpredictable and random behavior. The Henon map is another chaotic system known for its simplicity and efficiency.

The proposed system uses the Lorenz system to generate a random key to encrypt the color image. The encrypted image is then embedded in a cover image using the Henon map. The stego image is then transmitted or stored securely.

1.4 AIMS OF THE THESIS

The following aims and objectives for the thesis:

- a. Develop a new and improved Chaos Based-Visual Encryption (CBVE) algorithm based on the Lorenz system that is more secure and resistant to attacks than existing CBVE algorithms.
- b. Develop a new and improved chaos-based LSB steganography algorithm based on the Henon map that is more secure, scalable, and efficient than existing chaos-based LSB steganography algorithms.
- c. Investigate the performance of the proposed CBVE and chaos-based LSB steganography algorithms in terms of security, scalability, and efficiency.
- d. Develop a new and improved method for generating random locations based on the Henon map that is more resistant to attacks.

- e. Improved method for detecting and preventing steganalysis attacks on the proposed CBVE and chaos-based LSB steganography algorithms.
- f. Evaluate the performance of the proposed CBVE and chaos-based LSB steganography algorithms in real-world applications, such as secure storage of images in the cloud.

1.5 IMAGE ENCRYPTION AND STEGANOGRAPHY BASED ON CHAOS

Image encryption is essential for protecting sensitive color images, such as medical images, financial data, and military intelligence. Encrypting these images can prevent unauthorized individuals from accessing them and using them for malicious purposes. Image steganography is important for concealing the existence of sensitive color images. This can be useful for protecting images from unauthorized access, as well as for preventing copyright infringement.

- a. Telemedicine: Chaos-based image encryption can protect the confidentiality of medical images transmitted over public networks.
- b. Cloud computing: Chaos-based image encryption can be used to protect the confidentiality of images stored in the cloud.
- c. Military: Chaos-based image encryption can protect the confidentiality of military images and intelligence data.
- d. Copyright protection: Chaos-based image steganography can embed copyright information in images to protect against copyright infringement.
- e. Digital forensics: Chaos-based image steganography can hide evidence in images to prevent it from being tampered with or destroyed.

1.6 THESIS OUTLINE

- a. Chapter 1: Introduction

Explain color image steganography and encryption. Explain why the proposed system is needed and how existing approaches are limited—summarize the proposed system's major components and their interactions. Clarify thesis research goals. Finally, describe the thesis structure and how each chapter supports the study goals.

b. Chapter 2: Review of Literature

Critically analyses colour image encryption and steganography literature, concentrating on methods, strengths, flaws, and applications. Existing Method Limitations: Identify security, scalability, and efficiency issues with current solutions. Finally, provide the system's security, scalability, and efficiency criteria.

c. Chapter 3: The Proposed System

Briefly explain the CBVE algorithm's mathematical formulation, implementation, and security analysis. Chaos-Based LSB Steganography Method: Briefly describe the chaos-based LSB Steganography algorithm, including its mathematical formulation, performance, and security analysis.

d. Chapter 4: Performance Evaluation

Explain the experimental setting utilized to assess the proposed system. Communicate experimental results and consequences. Finally, evaluate the proposed method against various cutting-edge color image encryption and steganography approaches.

e. Chapter 5: Conclusion and Future Work

Summarize the thesis's main findings and contributions. Future work suggestions: Develop novel chaos-based image encryption and steganography algorithms, improve current techniques' security, and apply the suggested system to new applications.

2. LITERATURE REVIEW FOR IMAGE SECURITY BASED ON CHAOS

2.1 INTRODUCTION

Chaotic nonlinear dynamical systems are introduced in this chapter, and how they may be used to protect communications. A nonlinear or chaotic signal is distinguished by its broad spectrum and high sensitivity to changes in parameter and starting condition values. In addition, they proposed and designed an image encryption scheme with high security based on a double stage of chaos.

In this chapter, we present the basic concepts of chaos, types of chaos, Lyapunov exponents, and general image encryption methods (changing the position of pixels, changing the value of pixels, and changing the values and functions of pixels).

2.2 CHAOS DEFINITION

The word "chaos" has multiple meanings, but in the context of image encryption, it refers to a state of complete disorder and randomness. In an image encryption algorithm, chaos generates a random keystream to encrypt the image. The random keystream makes it difficult for an attacker to decrypt the images without knowing the key.

Chaos theory is a branch of mathematics that studies the behavior of dynamic systems susceptible to initial conditions, and this means that even a tiny change in the initial conditions can lead to a significant difference in the system's behavior over time. This property of chaos makes it difficult to predict the future behavior of a chaotic system, which is why it is often used in image encryption [1] [2] [3]:

There are three main parts to this definition:

- a. Aperiodic long-term behavior” refers to trajectories that do not arrive at fixed locations or orbits that are periodic or quasi-periodic throughout time.
- b. Deterministic” signifies that neither the system's inputs nor settings are random or noisy. The nonlinearity of the system alone is the source of all abnormal behavior.

- c. Sensitive dependence on initial conditions” indicates that the system has at least one positive Lyapunov exponent, which signifies that neighboring trajectories diverge exponentially.

2.3 TYPES OF CHAOTIC SYSTEMS

There are two types of chaotic systems: chaotic flows, and maps [4], [5]:-

2.3.1 Chaotic Maps

A chaotic map is a discrete-time chaotic system in which a set of difference equations generates the chaotic sample at the k^{th} iteration.[4], i.e.

$$x_k = g(x_{k-1}) \quad (2.1)$$

where x_k is the state vector, and $g(.)$ is used to indicate the iterative function, often known as the "chaotic map." The logistic map, the Hénon map, the Cat map, and the Standard Map are examples of a few well-known maps.

The Henon Chaotic map

The following difference equations may be used to create the Henon map, a 2D chaotic map:

$$\begin{aligned} x_{n+1} &= 1 - r * (x_n)^2 + y_n \\ y_{n+1} &= b * x_n \end{aligned} \quad (2.2)$$

Figure 2.1 displays the system's time series (x) and attractor and Figure 2.2 display the initial value sensitivity. The system depends on the parameters r and b , called system parameters. Typically, the Henon map behaves as a chaotic map with $r=1.4$ and $b=0.3$. The initial circumstances and the value of the parameter r that causes the system to exhibit an odd attractor or infinite divergence must be carefully chosen [6], [7].

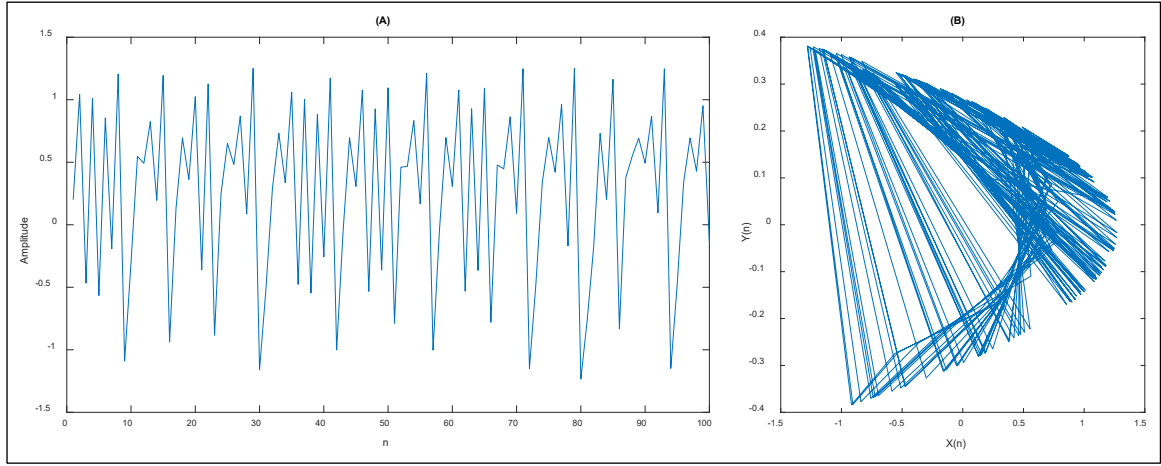


Figure 2.1: (A) Time Series and (B) Attractor (X) of Henon Map.

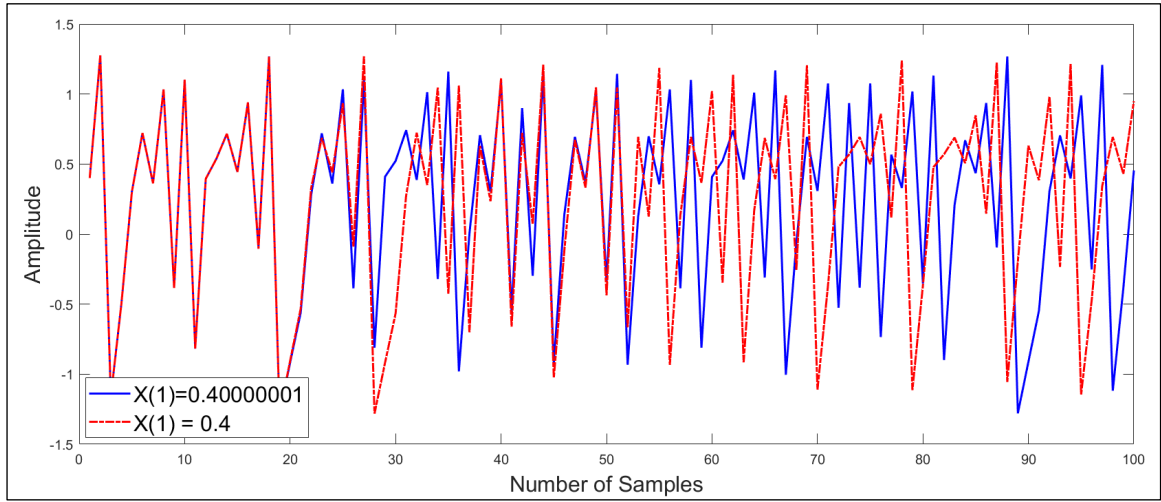


Figure 2.2: Sensitivity to Changing of Initial Values.

2.3.2 Chaotic Flows

For the continuous-time system of chaotic flow, the chaotic signal is generated by a set of differential equations [8] i.e.

$$\dot{x} = g(x, t) \quad x(t_0) = x_0 \quad (2.3)$$

Where $\dot{x}$ The system's current status vector at the time (t), and g represents the set of differential equations that regulate the dynamical system [9].

Additional illustrations of some of the well-known flows are “The Lorenz System,” [2], “Rössler System,” [10], “Chen’s System” [11], and “The Lü system” [12].

2.3.2.1 Rossler system

The Rössler chaotic system is an example of a flow Equation that describes the dynamics of the Rossler chaotic system. Moreover, as shown in Figure 2-3.

$$\begin{aligned}\frac{\partial x}{\partial t} &= -(y + x) \\ \frac{\partial y}{\partial t} &= ay + x \\ \frac{\partial z}{\partial t} &= b - cz + xz\end{aligned}\tag{2-4}$$

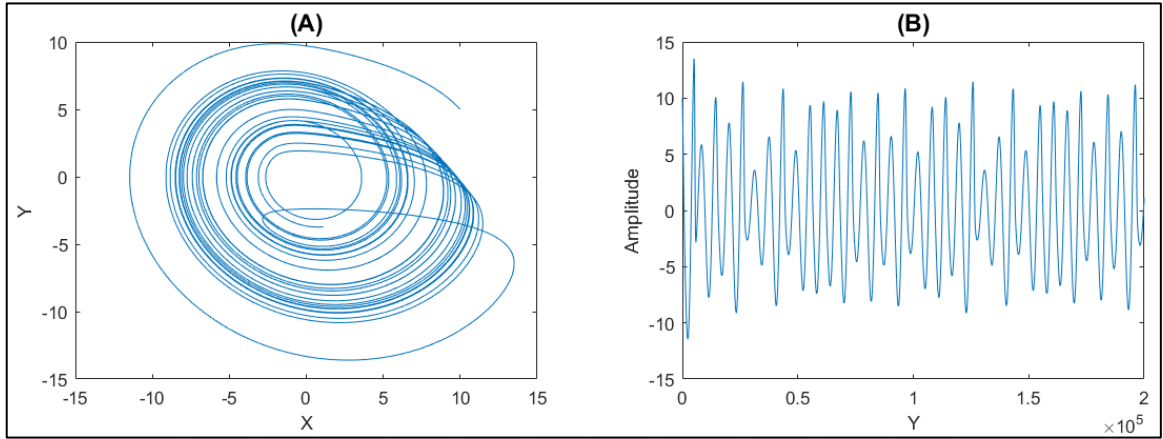


Figure 2-3: Rössler System flow (a) The strange attractor, (b) The time series x(t).

The "time series graph" is just the signal's amplitude shown against time. By graphing two of the system's state variables against one another, the "strange attractor graph" is produced. The system's state variables are typically determined using the first or second derivative of the time series or a combination of the two [10].

2.3.2.2 Lorenz system

A meteorologist and mathematician, Edward Lorenz was the first to examine the Lorenz system, a collection of ODEs (Ordinary Differential Equations). In 1963, a simpler mathematical model of atmospheric convection was developed. The model consists of three ordinary differential equations called Lorenz equations. [2],[13].

$$\begin{aligned}\dot{x} &= \sigma(y - x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz\end{aligned}\tag{2.5}$$

Where the $\dot{x}, \dot{y}$ and $\dot{z}$ are the vector of states for the Lorenz system; this is known as the Lorenz system. The Lorenz system parameters σ , r , and b are used to raise chaotic dynamics and should meet [14]:

$$\sigma, r, b > 0 \quad (2.6)$$

$$\sigma > b \quad (2.7)$$

$$r > \frac{\sigma(\sigma + b + 3)}{(\sigma - b - 1)} \quad (2.8)$$

The variable r_c in equation (2.8) is the essential value for r . where the actual r value should be greater than r_c .

$$r_c = \frac{\sigma(\sigma + b + 3)}{(\sigma - b - 1)} \quad (2.9)$$

To demonstrate this equation Let $b = 8/3$, and $\sigma = 10$, according to equation (2.9) because $\sigma > b$ to get chaotic state.

$$r_c = \frac{10(10 + (8/3) + 3)}{(10 - (8/3) - 1)} = 24.7386 \quad (2.10)$$

Since $r > r_c$, then we choose $r = 28$ demonstrates the outcomes of analyzing these parameters as Lyapunov exponents [15][16][17]. And the all state vectors are shown in Figure 2.,

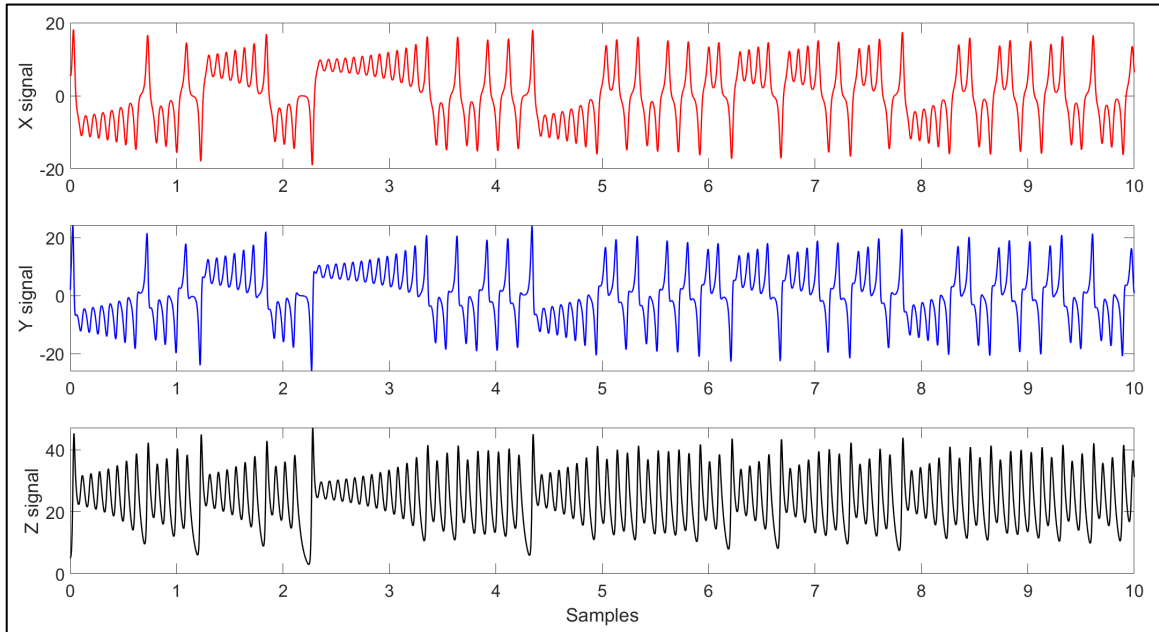


Figure 2.4: Time SERIES State of Lorenz System X, Y & Z Respectively.

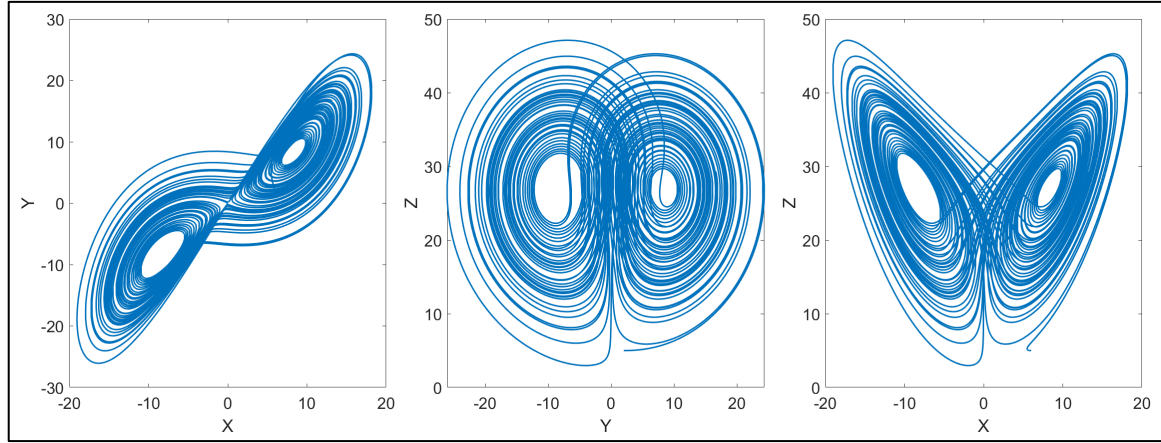


Figure 2.5: (X, Y), (Y, Z), and (X, Z) Strange Attractors for Lorenz System.

2.3.2.3 The Lorenz system properties

The chaotic Lorenz system has several characteristics [18]:

- a. Nonlinear system Lorenz: In the second and third equations, respectively, the nonlinear variables xz and yz characterize the nonlinearity of the Lorenz system.
- b. System Lorenz is symmetric: This indicates that the Lorenz System is invariant, which means that the equation is unaffected by the substitution of (x, y, z) for $(-x, -y, z)$. Because of this characteristic, the Lorenz system is symmetric. In particular, $x(t)$, $y(t)$, and $z(t)$ appear to be the Lorenz equations solution, while $x(t)$, $y(t)$, and $z(t)$ appear to be the Lorenz systems solution.
- c. System Lorenz is very sensitive to the initial conditions: demonstrates how another closely approaches one trajectory and how their characteristics differ. Figure 2., which depicts this phenomenon, displays the state's time domain waveforms and the Lorenz system solution, $\mathbf{x}(t)$ of both paths; Figure 2. displays the solid line as the starting point. ($X_0=3$, $Y_0=3$ & $Z_0=0$), the dashed line represents the initial condition $X_0=3$, $Y_0=3.000001$ & $Z_0=0$). Even though there is just a one-in-a-million variation between the initial conditions, only one state $\mathbf{y}(t)$, the paths separate exponentially faster another bath de-correlated.

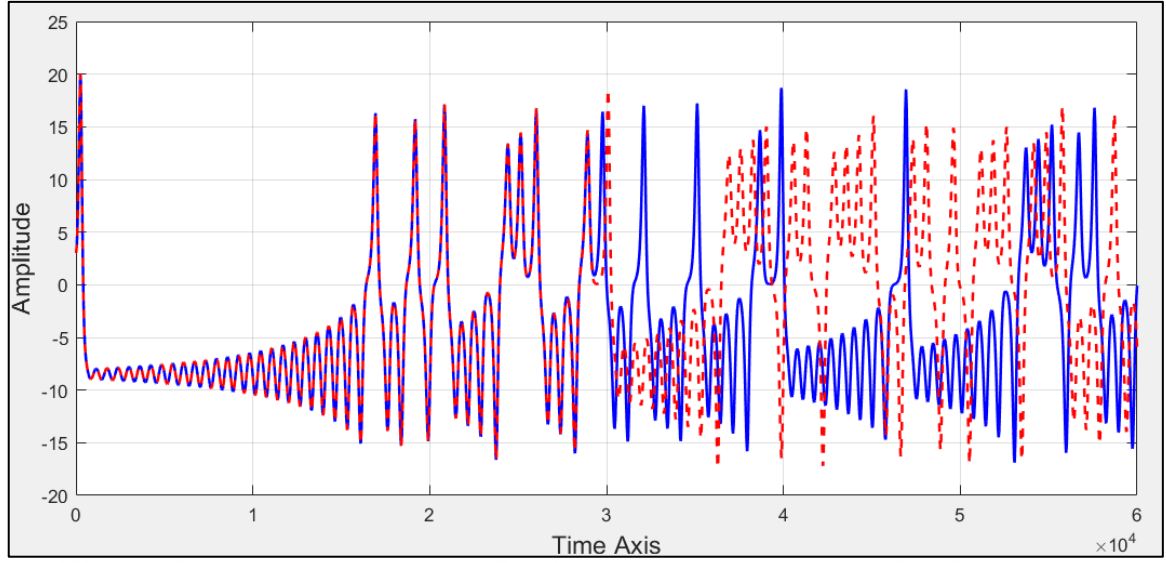


Figure 2.6: Sensitivity to Initial Condition for Lorenz System.

- d. System Lorenz Sensitive to Parameters”: as the above point displays the state's time domain waveforms and the Lorenz system, $\mathbf{x}(t)$ as seen in Figure 2., the dotted line indicates the parameters ($\sigma = 10$, $r=28$, and $b=2.6000001$), whereas the solid blue line represents the parameters ($\sigma = 10$, $r=28$, and $b=2.6$).

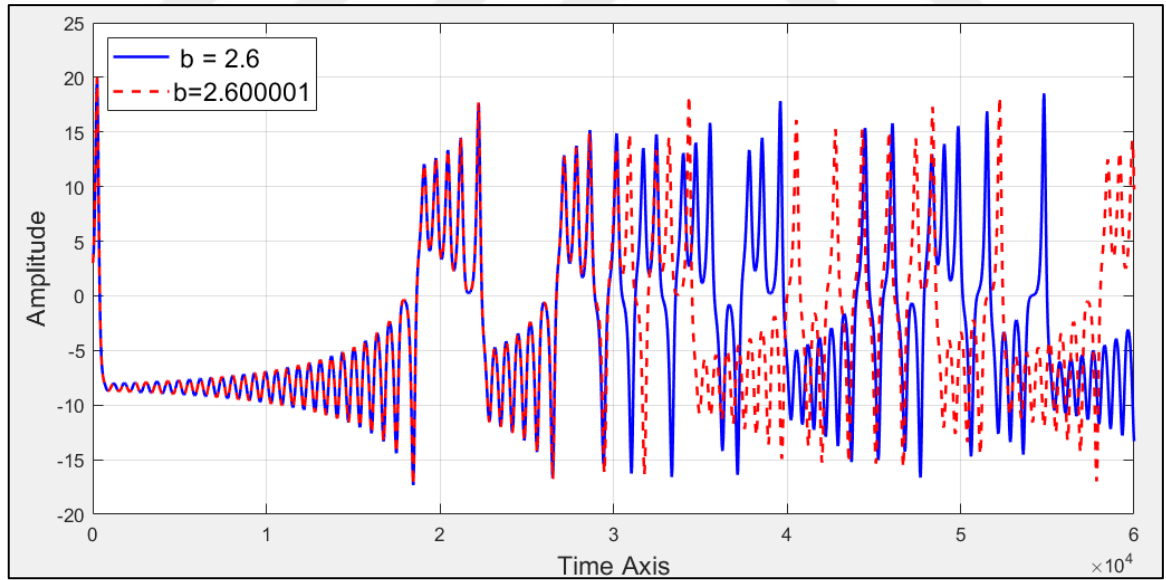


Figure 2.7: Sensitivity to Slightly Changing Parameter for Lorenz System.

2.4 CHAOS-BASED CRYPTOGRAPHY

Chaos-based cryptography practitioners use chaotic systems' characteristics to encrypt and decrypt data. In chaos theory, researchers examine complex and unpredictable strategies

with chaotic behavior highly sensitive to beginning circumstances. Several natural phenomena, including weather patterns, fluid dynamics, and population dynamics, are examples of chaotic systems [19], [20] [21].

To create cryptographic keys or encrypt and decrypted data, chaos-based cryptography uses the chaotic behavior of specific systems. Since it is difficult for an adversary to anticipate or evaluate the encryption process without knowing the beginning circumstances or key, chaotic systems are well-suited for cryptography applications. Chaotic maps and iterations, in which a chaotic function is repeatedly applied to a plain-text message or a cryptographic key, are prominent techniques in chaos-based cryptography. The output is then encrypted using the same chaotic map and related settings, yielding ciphertext. Complexity in the chaotic map's behavior gives this encryption method its security, making it hard to crack for an opponent [22].

The benefits of chaos-based encryption include increased security and less vulnerability to statistical assaults. It facilitates a speedier encrypting and decrypting procedure compared to standard cryptographic techniques. The fascinating field of chaos-based cryptography investigates the potential of chaotic systems for secure communication and data protection. However, it faces challenges such as the need for precise control over chaotic systems, vulnerability to attacks exploiting system parameters, and susceptibility to synchronization attacks. Ongoing studies attempt to overcome chaos-based encryption systems' limits and security problems while developing more robust and efficient encryption algorithms [23].

2.5 IMAGE ENCRYPTION ALGORITHMS

The chaotic encryption method has two forms of image encryption: modifying the value and location of individual pixels [24].

2.5.1 Pixel Value Transform (Changing Pixel Value)

Pixel value transforming is the first type of image encryption used to transfer the plain text to a ciphertext by changing the value of the pixels, as shown in Figure 2..

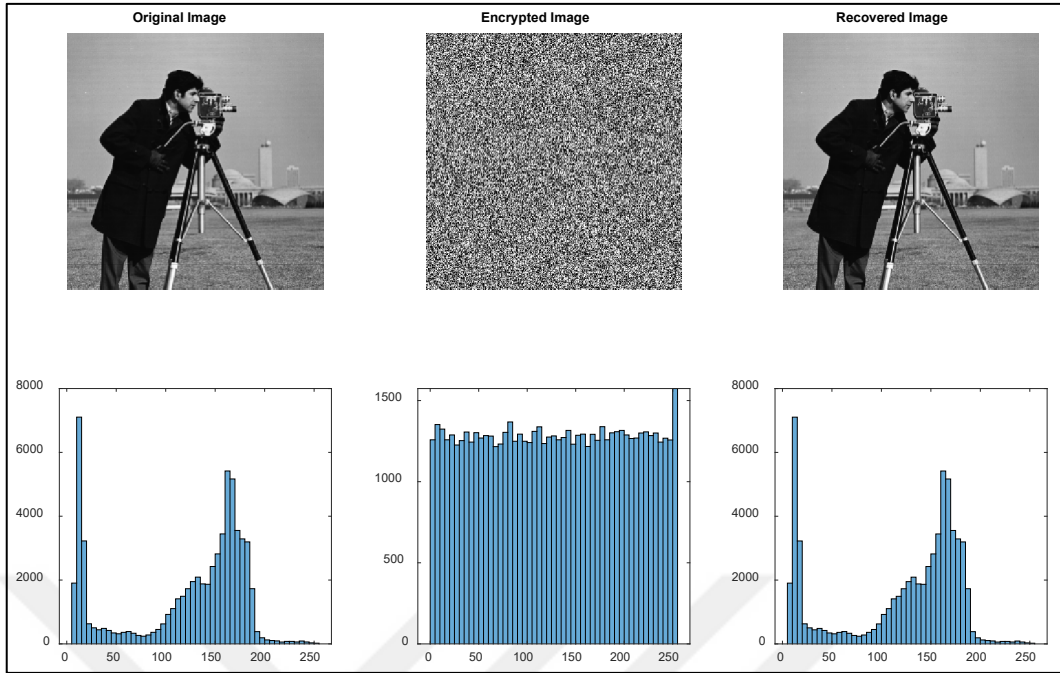


Figure 2.8: Image Encryption Based on Pixel Value Changing [25].

2.5.2 Transform of the Pixel Position (Changing Pixel Coordinate)

The ciphertext is produced by altering the locations of the pixels rather than their values, which is the second kind of digital image encryption procedure, as shown in Figure 2..

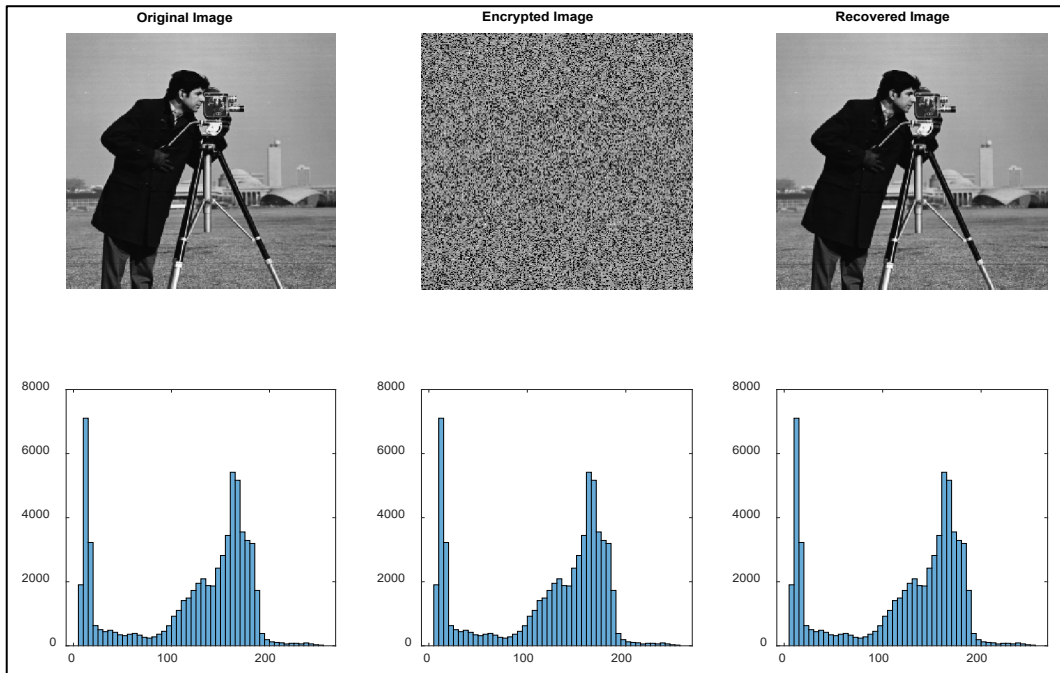


Figure 2.9: Image Encryption Based on Pixel Position Changing [25].

2.6 ADVANTAGES OF USING CHAOS IN IMAGE ENCRYPTION

There are some of the specific advantages of using chaos in image encryption:

- a. High security: Chaos is a mathematical phenomenon characterized by extreme sensitivity to initial conditions and unpredictable behavior. This makes it ideal for image encryption, as even a tiny change in the encryption key will result in a completely different encrypted image.
- b. Large key space: The key space of a chaotic image encryption algorithm is the number of possible encryption keys that can be used. A large key space makes the algorithm more challenging to crack, as an attacker must try many keys to find the correct one.
- c. Fast encryption and decryption: Chaotic image encryption algorithms can be implemented efficiently, resulting in fast encryption and decryption times. This is important for real-time applications, such as secure video transmission.
- d. Resistance to attacks: Chaotic image encryption algorithms resist various attacks, including brute-force attacks, statistical attacks, and differential attacks.
- e. Flexibility: Chaotic image encryption algorithms can be easily modified to improve security or performance.
- f. Scalability: Chaotic image encryption algorithms are scalable to images of any size.
- g. Low complexity: Chaotic image encryption algorithms are relatively simple to implement and understand.

2.7 STEGANOGRAPHY

LSB steganography is a type of steganography that hides data in the least significant bits of a digital image. The least significant bits of an image are those bits that have the most negligible impact on the overall quality of the image. By embedding data in the least essential bits, LSB steganography can hide a large amount of data in an image without significantly affecting the image quality.

LSB steganography replaces the least significant bits of the image pixels with the data bits to be hidden. This is done by replacing the LSB of the pixels with the data bits. To extract

the hidden data from the *stego image*, the reverse process is performed. The least significant bits of the *stego image* pixels are removed and combined to form the secret data.

LSB steganography is a very popular technique for hiding data in images because it is simple to implement and can hide a large amount of data without significantly affecting the image quality. However, LSB steganography is also a relatively easy technique to detect. Several methods can be used to detect LSB steganography, such as statistical analysis and visual inspection.

2.7.1 LSB Steganography Advantages

- a. Ease of implementation: LSB steganography is a relatively simple technique, even for users with limited technical expertise.
- b. High capacity: LSB steganography can hide a large amount of data in an image without significantly affecting the image quality.
- c. Robustness to noise: LSB steganography is relatively robust, meaning the hidden data is less likely to be corrupted if the image is compressed or processed.

2.7.2 LSB Steganography Disadvantages

- a. Vulnerability to detection: LSB steganography is a relatively easy technique, especially if a large amount of data is embedded in the image.
- b. Potential for image quality degradation: If too much data is embedded in the image, it can reduce its quality.
- c. Limited security: LSB steganography is not a secure technique for hiding data, as several methods can detect and remove hidden data.

2.7.3 Purposes of Steganography

- a. Hiding data in images for transmission over a network: LSB steganography can hide data in images for transmission over a network, such as the Internet. This can be useful for hiding confidential data from unauthorized users.

- b. Embedding copyright information in images: LSB steganography can embed copyright information. This can help to protect copyright owners from unauthorized use of their images.
- c. Creating digital watermarks: LSB steganography can be used to create digital watermarks. Digital watermarks are hidden messages embedded in images to identify the owner of the image.

2.7.4 Limitations of the Steganography

- a. Capacity: Steganography can only hide a limited amount of data in a cover object. This limitation is because the hidden data must not significantly affect the quality or size of the cover object.
- b. Security: Steganography is not a secure way to hide data. Several steganalysis techniques can be used to detect the presence of hidden data in a cover object.
- c. Robustness: Steganographic techniques are not always robust to noise or compression. This means the hidden data may be corrupted or lost if the cover object is compressed or processed.

2.8 THE QUALITY OF IMAGE MEASUREMENTS

There would not be any statistical assault that could crack a cryptosystem. The suggested method is statistically tested in the following ways to demonstrate its stability. Many techniques and algorithms exist for evaluating the efficacy of image-frame encryption schemes. The Correlation Coefficient Measuring Factor, DSC “Distance Scrambling Factor,” The CCMF “Correlation Coefficient Measuring Factor,” MD “Maximum Deviation analysis,” Ent “Entropy,” PSNR “Peak Signal-to-Noise Ratio” and SSIM “Structural similarity index measure.”

2.8.1 Histogram Analysis

An image's histogram is a bar chart showing how its pixels' values are spread out. To prevent an adversary from gleaning meaningful information from the histogram of an encrypted

image's streaming, the perfect encrypted picture must have a uniform distribution and be utterly distinct from the plain image [26].

2.8.2 The Correlation Coefficient

The correlation coefficient is a statistical measure that indicates the strength and direction of a linear relationship between two variables. It ranges from -1 to 1, with 1 indicating perfect positive correlation and -1 indicating perfect negative correlation. Three types of correlations are vertical (V), horizontal (H), and diagonal (D): vertical, horizontal, and diagonal. High correlation indicates a perfect relationship, while low correlation indicates no correlation. In image encryption, these correlations measure the effectiveness of the encryption scheme, as a good scheme scrambles pixel values without correlation, making it difficult to recover the original image without the key. To calculate the correlation coefficient, one may do the following:

$$Corr = \frac{\sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^N ((x_i - E(x)))^2} \sqrt{\sum_{i=1}^N ((y_i - E(y)))^2}} \quad (2.10)$$

where $E(x) = (\frac{1}{N}) \sum_{i=1}^N x_i$, x and y are the pixel values of the original and the encrypted image, respectively [11], [27].

2.8.3 Mean Square Error (MSE)

The most popular metric estimate used to measure picture quality is MSE. It is a comprehensive reference measure, and as the following equation demonstrates, the closer values are to zero, the better.

$$MSE = \frac{1}{MN} \sum_{n=0}^N \sum_{m=1}^M (x(n, m) - y(n, m))^2 \quad (2.12)$$

x and y represent the original, encrypted, or decrypted images [28].

2.8.4 Peak Signal-to-Noise Ratio (PSNR)

Using the difference in pixel value between the original image and the encrypted image, the peak signal-to-noise ratio (PSNR) may be used to assess the efficacy of the encryption strategy. Use the following equation to determine it:

$$PSNR(dB) = 10 \log_{10} \left[\frac{M*N*255^2}{\sum_{i=0}^{M-1} \sum_{j=0}^{N-1} (x(i,j)-y(i,j))^2} \right] \quad (2.13)$$

$$PSNR(dB) = 10 \log_{10} \left[\frac{255^2}{MSE} \right] \quad (2.14)$$

where M and N are the image's dimensions, x, and y are the unencrypted and encrypted versions of the same frame, and (i,j) is the pixel's coordinate. Encryption is more efficient with a lower PSNR [29].

2.8.5 Structural Similarity Index Measure (SSIM)

SSIM is a method for predicting the perceived quality of digital images and videos. It measures image similarity using a complete reference metric based on an initial uncompressed or distortion-free image. The SSIM index is calculated on various windows of an image, measuring between two windows of standard size N*M.

$$SSIM(x, y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \quad (2.15)$$

μ_x, μ_y are the average of x and y respectively.

σ_x^2, σ_y^2 the variance of x and y , σ_{xy} The covariance of x and y .

$c_1 = (k_1L)^2, c_2 = (k_2L)^2$ two variables to stabilize the division with a weak denominator.

L the dynamic range of the pixel values (typically is $2^{bits \text{ per pixel}} - 1$)

$k_1 = 0.01, k_2 = 0.03$ by default [30].

2.8.6 Entropy

One common method of evaluating the robustness of a symmetric cryptosystem is information entropy. Source message m's information entropy H (m) is given by: (2-15). In a message with 8 bits, an entropy value of 8 is ideal, indicating that the information from the message source is random [14][31].

$$E = \sum_{i=0}^{2^n-1} [P(i) * \log_2 \left(\frac{1}{P(i)} \right)] \quad (2.11)$$

Where: P(i) is the probability of event I in bits, denoted by the symbol I.

2.8.7 Differential Analysis

A common tactic for discovering a cipher's secret key is for an adversary to briefly alter the plain picture and then compare it to the ciphered ones [32][31]. If even a slight change in the clear image may result in a considerable shift in the encrypted image in terms of dispersion and confusion, then this differential attack becomes utterly ineffective. The encrypted version of the image needs to be noticeably different from the original. Two metrics the Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity can be used to quantify this variation (UACI)

2.8.7.1 Number of pixels change rate (NPCR)

NPCR refers to the percentage of encrypted picture pixels that shift in value when a single pixel's value shifts. When comparing cipher pictures to their original counterparts, this metric calculates the proportion of differences in pixel numbers when there is a single changed pixel. The greater the degree to which NPCR approaches 100%, the more successfully the cryptosystem will withstand a plain-text assault. Let x and y be the cipher images. Using the dimensions of an image as your guide, define a bipolar array Q [33], [31].

$$\begin{aligned} Q(i, j, w) &= 0 & \text{if } x(i, j, w) = y(i, j, w) \\ Q(i, j, w) &= 1 & \text{if } x(i, j, w) \neq y(i, j, w) \end{aligned} \quad (2.12)$$

$$NPCR = \frac{\sum_{i=1}^R \sum_{j=1}^C \sum_{w=1}^D Q(i, j, w)}{R * C * D} * 100\% \quad (2.18)$$

R & C are the dimensions of clear and encrypted images, and (D) equals 3 for the color image and 1 for the gray-scale image.

2.8.7.2 Unified average changing intensity (UACI)

To determine the average intensity difference between the plain text picture and the encrypted image, UACI uses a formula [33], [34]. The more excellent the UACI, the better the cryptosystem's resistance to a differential attack. In mathematical terms,

$$UACI = \frac{1}{R * C * D} \sum_{i=1}^R \sum_{j=1}^C \sum_{w=1}^D \frac{|x(i, j, w) - y(i, j, w)|}{255} * 100\% \quad (2.13)$$

R & C are the dimensions of clear and encrypted images. D equals 3 for the color image and equals 1 for gray-scale images.

2.8.8 Brute-Force Analysis

The quality of an image encryption technique relies on the cipher keys' strength and the key space's size, both of which must be sufficiently vast to render brute-force assaults impossible.

2.8.8.1 Key sensitivity

Whether or not a cryptosystem is vulnerable to a brute-force assault can be gauged by how sensitive its keys are to guessing.

2.8.8.2 Keyspace analysis

The key space size is the total number of possible keys used for encryption and decryption. A big enough keyspace will render brute-force attempts futile. The keyspace size should be at least 2^{100} for maximum cryptographic security [35] [36].

2.9 CLOUD STORAGE

Cloud storage refers to a service model wherein data is securely stored in remote servers hosted on the internet. The system enables users to retrieve their data via an internet connection remotely. Cloud storage has emerged as a highly advantageous and economically viable data storage and retrieval solution, gaining significant traction in individual and organizational contexts. Two primary categories of cloud storage exist: public cloud storage and private cloud storage. Public cloud storage services are accessible to the wider populace, whereas personal cloud storage services are restricted to a designated group of users.

Public cloud storage services are commonly provided under a payment model that allows users to pay for the services they consume on a usage basis. This implies that individuals are solely responsible for covering the costs associated with the amount of storage space and bandwidth they utilize. Public cloud storage services are highly scalable, allowing users to conveniently adjust their capacity by adding or removing storage space as required.

Private cloud storage services generally cost more than their public cloud counterparts, yet they provide enhanced security measures and increased control over data management. Personal cloud storage services can be hosted either on-premises or off-premises.

2.9.1 Advantages of Cloud Storage

- a. Cloud storage can be accessed from any location with an internet connection. This makes it excellent for consumers who require data access from multiple locations.
- b. Cloud storage is often more cost-effective than on-premises storage, particularly for organizations with changing storage needs.
- c. The scalability of cloud storage makes it simple to add or delete storage capacity as needed.
- d. Multiple redundancy procedures are in place to prevent data loss or corruption among cloud storage providers.

2.9.2 The Disadvantages of the Cloud Storage

- a. The system is not secure, while cloud storage providers provide several security measures. In recent years, many high-profile data breaches have involved cloud storage services.
- b. Cloud storage providers have access to all of the data saved on their servers. This raises privacy concerns, particularly for firms that store sensitive information in the cloud.
- c. After migrating the data to a cloud storage service, transferring it to a different provider can be difficult and expensive.

2.9.3 Tips for Selecting a Cloud Storage Provider

- a. Consider your safety requirements: Ensure the cloud storage company you select delivers the security safeguards to safeguard your data.
- b. Think about your safety needs: Ensure that the cloud storage company you select provides the security measures necessary to protect your data.
- c. Consider your security needs: Ensure that the cloud storage company you select provides the necessary security safeguards to protect your data.

- d. Numerous suppliers of cloud storage provide free trials. This is an excellent method for evaluating a service before committing to a paying plan.

2.10 RELATED WORKS

In 2023, S. Salunke, et al. Proposed A technique for digital picture compression-encryption employing a quad key-secured 3D Gauss chaotic map with singular value decomposition (SVD) and hybrid chaos is provided. This approach utilizes SVD for picture compression and four-key-protected encryption using a new 3D Gauss, logistic, Arnold, or sine maps. The technique has three advantages: user-selectable compression settings, confusion mechanism, and nonlinear and chaotic key spaces. The 3D Gauss map fulfils the Lyapunov exponent distribution, making it highly secure and space-efficient. The experimental results demonstrate a reliable reconstruction with a high PSNR for various singular values. The suggested approach is very safe and resistant to assault. [37].

In 2023, R. J. Rasras, et al, demonstrated a data encryption-decryption approach employing a complicated PK for picture and decryption utilizing the XOR operation. The PK is reordered using a secret ordering sequence, and any changes made during decryption are regarded as hacking efforts. The approach offers a vast key space that resists hacking efforts. It will be evaluated and compared to DES and AES, and its throughput and speed will be determined. The approach is simple to employ and maintains acceptable MSE and PSNR values.[38]

In 2023, H. Wen and Y. Lin presented an improved color image code (ICIC-DNA) using various deoxyribonucleic acid sequence operations and chaos. A cryptanalysis, however, uncovered significant security weaknesses. The encryption sequences are independent of the plain-text, simplifying the complex DNA procedure. ICIC-DNA also provides replacement and permutation of DNA domains, which can be attacked independently. Proposed is a chosen-plaintext attack approach that uses differential analysis to break the DNA-base permutation process, eliminates DNA domain encryption, and employs an analogous key for comprehensive cracking. The system has minimal computational and data complexity and is effective. [39]

In 2023, H. R. Shakir, et al., A novel four-dimensional hyper-chaotic system capable of permutation and substitution operations is offered for key generation in image encryption. The technology permutes color bands and diffuses pixel values using dynamic S-boxes. The

effectiveness of the strategy is evaluated using keyspace and histogram. It is safe and resistant to assaults, with a high sensitivity to changes in secret keys, as determined by a security study. Encryption and decoding are also accomplished quickly. [40]

In 2023, V. Patidar and G. Kaur proposed a novel conservative chaotic standard map-driven dynamic DNA coding technique for picture encryption, providing a hybrid DNA- and chaos-based strategy with an unbounded keyspace. The approach arbitrarily selects encoding, addition/subtraction, and decoding rules using pseudo-random sequences generated by the conservative chaotic standard map. The method uses feed-forward and feedback processes to create and modify dynamic one-time pixels, assuring cleartext and ciphertext sensitivity. Various parameter values generate controlled pseudo-random sequences, resulting in a sensitive keypad. Performance and security assessments have been conducted using histogram, correlation, information entropy, DNA sequence-based, perceptual quality, key sensitivity, plain-text sensitivity, and classical attack analysis. The outcomes are encouraging and indicate the algorithm's resistance to prevalent cryptanalytic assaults. [41]

In 2023, M. Majid Msallam and Fayez Aldoghan proposed a three-step way to safeguard data utilizing cryptography and steganography. The critical message will be encrypted in two halves, one using the Caesar Cipher and the other using the Vigenere Cipher. The ciphertext will be converted to Morse code before being concealed in a cover picture using the Least Significant Bits (LSB) method. Based on the peak signal-to-noise ratio (PSNR) established in this study, our approach has an increased degree of security and resilience. Due to the combination of cryptography and steganography, our study gives a higher level of protection. [42]

In 2022, X. Zhang and J. Tian provided an algorithm for encrypting multiple images using genetic central dogma and three-dimensional bit planes. The technique starts by converting the original pictures into an 8-bit binary format, and then it permutes the matrix, encodes the permuted matrix as DNA codes, and decodes the encrypted images using RNA decoding. The findings and analysis of the experiments indicate high levels of security and satisfactory performance [43].

In 2023, B. Zhang and L. Liu, studied the process of developing chaos-based picture encryption algorithms were investigated, with a particular emphasis placed on symmetric and asymmetric algorithms, block ciphers, and integration with other technologies. Cross-referencing and further developing picture encryption methods are made possible by chaos's

distinctive characteristics, which include sensitivity to beginning circumstances, topological transitivity, and pseudo-randomness. The study discusses real-world application scenarios and the obstacles that are now being faced, and it encourages academics to keep generating new circumstances and adding to those that already exist [44].

In 2021, H. Tian, et al. They investigated a three-dimensional jerk chaotic system with a secret attractor by studying its dissipativity, equilibrium, and stability. Different attractor types, Lyapunov exponents, and the Poincare section of the system are investigated while varying several parameters. Testing is done on a circuit, and then, utilizing finite-time stability theory, a robust feedback controller is built. This controller ensures synchronization and asymptotically convergent convergence to the origin. In addition to this, the study offers proof through the use of numerical simulation [45].

In 2023, A. A. Rashid and K. A. Hussein, Built a secure method for encrypting black-and-white and color photographs. The proposed system consists of two stages: the encryption process, in which keys are generated based on chaotic logistics and picture density to encrypt gray-scale and color pictures, and the decryption process, which is the inverse of the encryption process to recover the original image. The proposed method was evaluated on two publicly accessible black-and-white and color images. According to the test findings, the maximum values for peak signal-to-noise ratio (PSNR), unified average changing intensity (UACI), and number of pixel change rate (NPCR) are 7.7267, 50.2012, and 100, respectively. Encryption and decryption times have been decreased to 0.6320 and 0.5304 seconds, respectively [34].

In 2023, D. E. Mfungo, et al., a unique picture encryption system, employs chaotic maps and fuzzy integers for safe information transfer. The approach integrates logistic and sine maps, fuzzy notions, and Hénon maps to produce secure secret keys. During diffusion, a fuzzy triangular membership function alters the initial circumstances. Scrambling picture pixels, summing neighbouring row values, and XORing with randomly generated integers are all part of the encryption process. Statistical, local, Entropy, differential, signal-to-noise, distortion, mean error square, brute force, and information entropy attacks are all investigated. The scheme has a high key sensitivity, ensuring secure information transmission[46].

In 2023, H. Mahalingam, et al, proposed a two-layer image encryption system employing bit-level encryption in the time-frequency domain. The top layer consists of a plane slicing

the image, which is subsequently scrambled with a chaotic map and encrypted with a key derived from the same chaotic map. The low-frequency components of each segment are then scrambled and encrypted using a Lifting Wavelet Transform after image segmentation. Afterward, the last layer is jumbled and encrypted using a chaotic hybrid map. Multiple investigations were conducted on the procedure, and the recommended work attained a maximum entropy of 7.99 and a correlation close to zero, proving its resistance to statistical assaults. In addition, the keyspace of the cryptosystem reaches 2^{128} [47].

In 2023, A. P. Kari and T. Ghomian suggested a new method for encrypting gray-scale digital photos using the residue number system combined with chaotic maps. This approach improves processing speed and encryption security while eliminating the necessity for high-dimensional chaotic maps. The method uses a two-phase pixel content diffusion step, and Arnold's cat map for image pixel coordinate confusion. The residue number system improves evaluation parameters and processing time, averaging 0.15 seconds for encryption. A uniform histogram, an entropy of roughly 8, and a correlation coefficient close to zero demonstrate the method's outstanding security [48].

In 2023, N. Elkhailil, et al., the one-dimensional Beta chaotic map was used to generate a new two-dimensional chaotic map named two-dimensional Beta Chaotic Map(2D-BCM) (1D-BCM). This study describes a novel 2D-BCM-based picture encryption method. Chaotic sequences are generated using the new 2D-BCM. The encryption key was created using these sequences. Permutation, diffusion, and substitution are the three key processes of the proposed method. The suggested approach successfully determines the commonly used security metrics and sensitivity to beginning circumstances utilizing a selection of standard simulation findings. The collected results of various forms of security analysis reveal that the newly constructed 2D-BCM has excellent sensitivity and security compared to earlier schemes[49].

In 2023, A. Dawood, Q. Thabit, and T. Fahad, provided a complete study of picture encryption methods and classified them based on numerous ideas, such as chaotic maps, DNA, and other similar examples, along with comparisons between current approaches to accessing various types of security parameters. In addition, the many forms of encryption keys, as well as some typical types of attacks and the essential methods for testing the effectiveness of encryption, were covered in this article [50].

In 2023, S. T. Allawi and N. A. A. Mustafa, a unique approach to the encryption of visual data, utilizes a two-stage process that combines chaotic maps with linear feedback shift registers. In the first stage, the image is cut in half, and its pixels are redistributed using keys corresponding to random integers. The second stage divides the image into its component primary colors, denoted by the letters RGB, then encrypts the data associated with each hue using three-dimensional chaotic maps. This strategy is superior in terms of safety and effectiveness compared to other approaches [51].

Table 2.1: The Summarize of Related Works.

Ref.	Author/s	Year	Key Contributions
[37]	Salunke et al.	2023	It has proposed a novel image encryption technique that uses a quad key-secured 3D Gauss chaotic map for encryption and SVD for compression. The method has a large key space and is resistant to statistical attacks.
[38]	Rasras et al.	2023	It proposed a simple and efficient image encryption technique that uses a complicated PK for encryption and the XOR operation for decryption. The method is resistant to brute force attacks.
[39]	Wen and Lin	2023	It proposed an improved image encryption technique that uses DNA sequences and chaos. The method is resistant to chosen-plaintext attacks.
[40]	Shakir et al.	2023	It has proposed a novel image encryption technique that uses a four-dimensional hyper-chaotic system for key generation. The method is resistant to statistical attacks and has ample key space.
[41]	Patidar and Kaur	2023	Proposed a novel image encryption technique that uses a conservative chaotic standard map and DNA coding. The method has an unbounded key space and is resistant to statistical attacks.
[42]	Msallam and Aldoghan	2023	It proposed a three-step image encryption technique that uses cryptography and steganography. The method is resistant to statistical attacks and has a large key space.
[43]	Zhang and Tian	2022	It proposed an image encryption technique that uses genetic central dogma and three-dimensional bit planes. The technique is resistant to statistical attacks and has a large key space.
[44]	Zhang and Liu	2023	Conducted a comprehensive study of chaos-based image encryption algorithms. The study identified the key challenges and opportunities in developing chaos-based image encryption algorithms.
[45]	Tian et al.	2021	Conducted a theoretical study of a three-dimensional jerk chaotic system with a secret attractor. The study found that the system has a large key space and is resistant to statistical attacks.
[34]	Rashid and Hussein	2023	Proposed a secure image encryption technique for black-and-white and color photographs. The technique is based on a 6D chaotic system, is resistant to statistical attacks, and has a large key space.
[46]	Mfungo et al.	2023	Proposed a novel image encryption technique that uses chaotic maps and fuzzy integers. The technique is resistant to statistical attacks and has a large key space.
[47]	Mahalingam et al.	2023	Proposed a two-layer image encryption system that uses bit-level encryption in the time-frequency domain. The technique is resistant to statistical attacks and has a large key space.
[48]	Kari and Ghomian	2023	Proposed a new image encryption technique for gray-scale digital photos that uses the residue number system and chaotic maps. The technique is resistant to statistical attacks and has a large key space.
[49]	Elkhalil et al.	2023	Proposed a novel image encryption technique that uses a two-dimensional chaotic map generated from a one-dimensional chaotic map.

3. THE PROPOSED MODEL BASED ON CRYPTOGRAPHY AND STEGANOGRAPHY

3.1 INTRODUCTION

The cloud has become an increasingly popular platform for storing data but is also a target for attackers. It is essential to use secure storage methods to protect the data stored in the cloud. This chapter will introduce the proposed promising approach of visual encryption based on chaos and LSB steganography to protect the data stored in the cloud. Visual encryption generates multiple shares of an encrypted image, which can only be reconstructed by combining all the shares. LSB steganography hides data in the least significant bits of a digital image.

3.2 THE PROPOSED SYSTEM MODEL

The suggested method uses visual encryption based on chaotic signals and LSB steganography for superior security. First, chaos-based visual encryption encrypts data. The encrypted shares are encoded in a cover image using LSB steganography. The cloud storage server receives the *stego image*. To access the secret data, the user must have all encrypted and cover image shares. Decrypting the shares and reconstructing the image is possible with the chaos-based visual decryption technique. The LSB steganography extraction algorithm extracts the secret data from the source image. Figure 3.1 illustrates the general block diagram of the proposed encryption, steganography, and the cloud storage scheme.

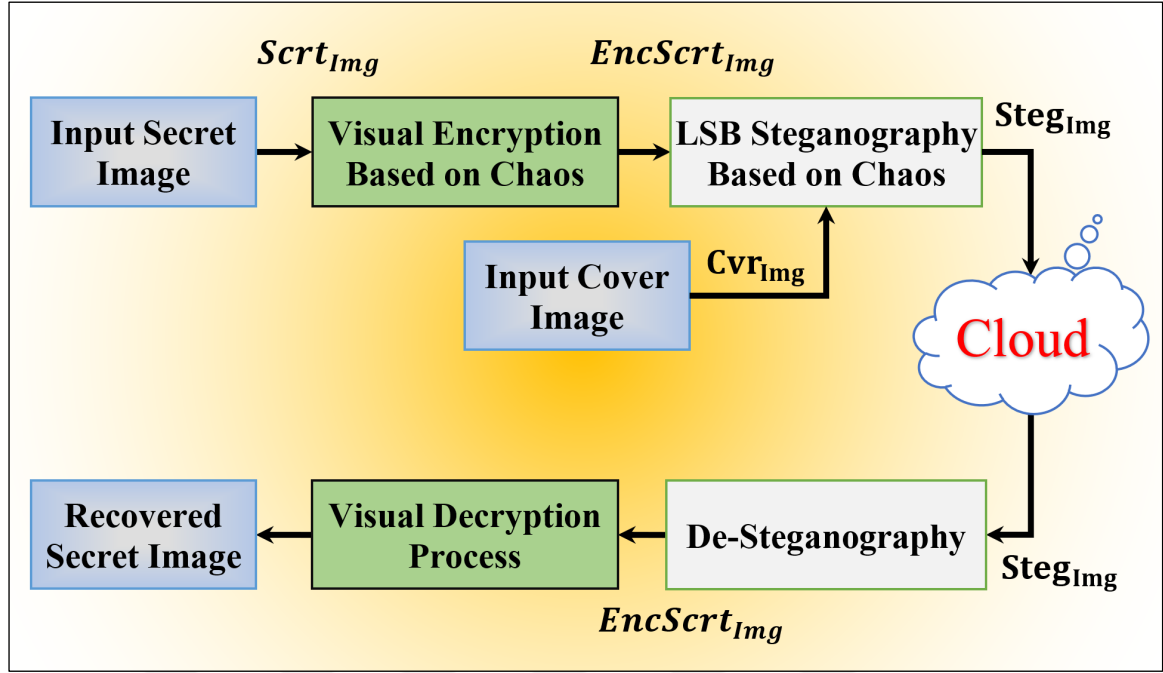


Figure 3.1: General Diagram of the Proposed Scheme.

As shown in Figure 3.1, the proposed scheme is a hybrid system that combines the strengths of two well-established techniques: chaos-based visual encryption (CBVE) and least significant bit (LSB) steganography. This system can securely store data in the cloud, even when the cloud server is not trusted. The system works as follows:

- Chaos-Based Visual Encryption:** The secret data is first encrypted using chaos-based visual encryption. This technique generates two or more shares of the encrypted image such that the original can only be reconstructed by combining all the shares.
- LSB Steganography:** The encrypted shares are then embedded in a cover image using LSB steganography. This technique hides the secret data in the least significant bits of the cover image, making it difficult for attackers to detect.
- Cloud Storage:** The steganography image (Stego. Image) is then uploaded to the cloud storage server.

The advantages of the proposed scheme over other secure data storage methods:

- High security:** The combination of Chaos-Based Visual Encryption (CBVE) and LSB steganography makes it difficult for attackers to access the secret data, even if they can obtain the *stego image*.

- b. Scalability: The proposed system can support large datasets, making it suitable for various applications.
- c. Ease of use: The proposed system is relatively easy to implement and use, even for users with limited technical expertise.
- d. Flexibility: The proposed system can secure various data types, including financial data, healthcare data, and intellectual property.

3.3 GENERATION OF CHAOTIC RANDOM INTEGER NUMBER (CRIN)

This process converts the chaotic signal to a random integer number as indicated in the following steps: -

- a. Multiplying the chaotic value by the maximum number (such as 10^{12}).
- b. The result should be rounded up to the following whole number.
- c. Apply the mod operation on the number to 255. (The result will be between 0 and 254).
- d. As demonstrated in the equation (3.1), by adding 1 to the development, the resulting integers will be between 1 and 255.

$$CRIN = [Round (ChaoticNum * 10^{12}) \% 255] + 1 \quad (3.1)$$

Where: CRIN is a Chaotic Random Integer Number.

Figure 3.2 is the correlation before and after applying the previous equation to the chaotic sequence.

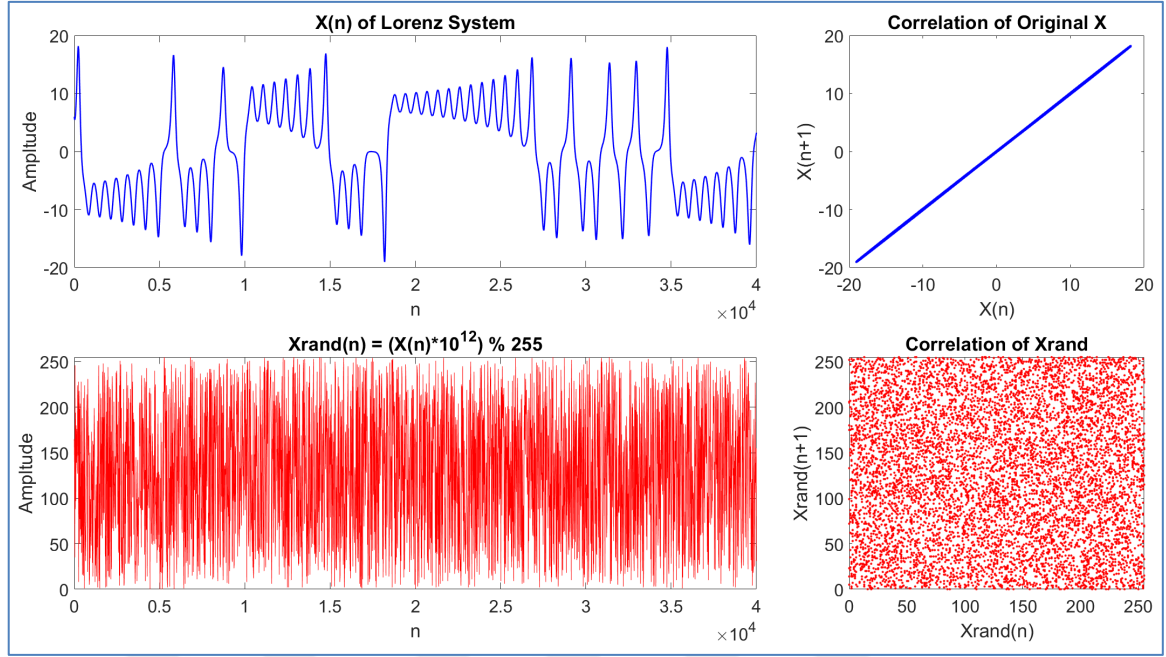


Figure 3.2: Increasing Randomness by Multiplying and Mod.

3.4 CHAOS-BASED VISUAL ENCRYPTION (CBVE)

The CBVE is a type of encryption that uses chaotic signals to generate two or more shares of an encrypted image. The original image can only be reconstructed by combining all of the shares. Chaotic systems are dynamic systems highly sensitive to initial conditions and system parameters, which means that even a small change in the initial conditions or system parameters can result in a completely different output; this makes chaotic systems ideal for encryption, as it is challenging to attack an encrypted image without knowing the exact chaotic map and parameters used to encrypt it.

The image encryption depends on changing the pixel value by “Chaotic Random Number Generator (CRIN)” using the chaotic Lorenz signals and doing XOR between the CRIN and the image pixels to encrypt the secret data using the CBVE, the following steps are performed:

- Firstly, insert the image to be encrypted (Secret image).
- The image consists of three shares: red, green, and blue share. Split the image into three parts.
- Using the number of pixels in the color image and the Lorenz equations, a chaotic signal is generated and converted to CRIN (as explained in the previous section).

- d. The XOR operations between the image pixels and the chaos-generated CRINs are essential to the encryption process.
- e. The pixels from the first share (R-color) are encrypted by the X signal of the Lorenz system CRIN(X), the Y signal CRIN(Y) encrypts the pixels from the second share (G-color), and the Z signal CRIN(Z) of the Lorenz system encrypts the pixels from the third share (B-color).
- f. The three encrypted shares combine to get the encrypted image with the same original image size, as shown in Figure 3.3.

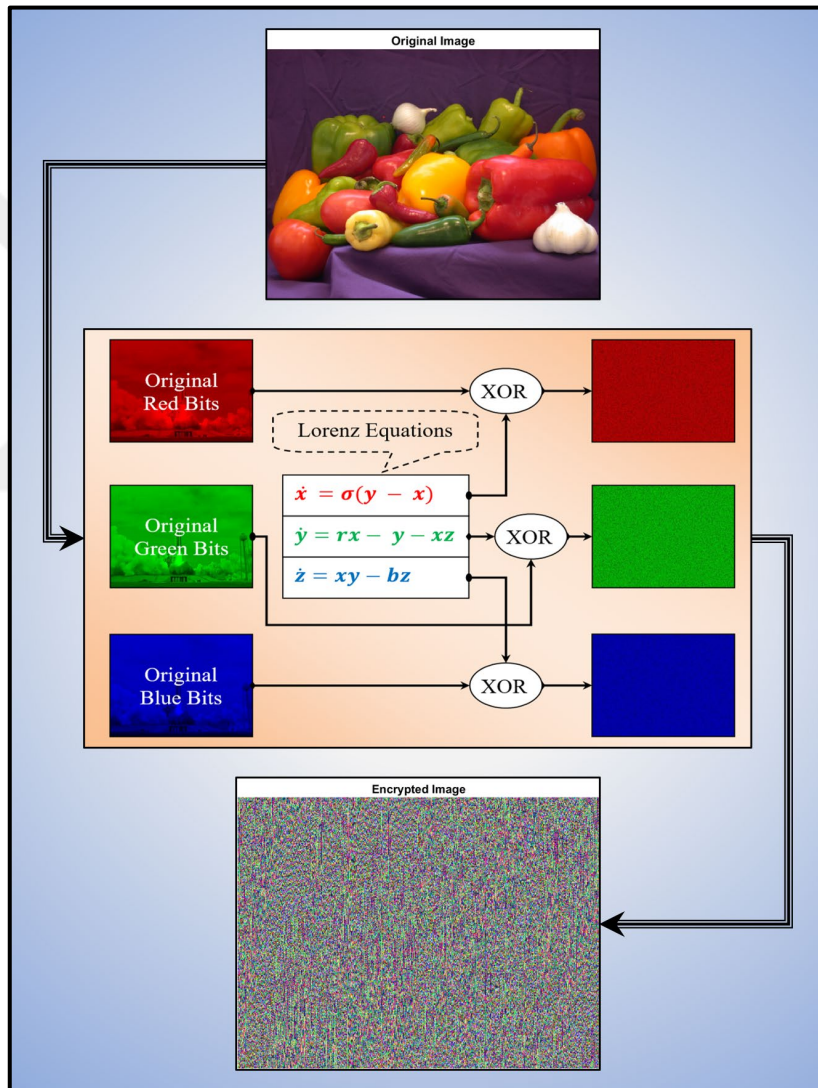


Figure 3.3: Image Encryption Based on CBVE.

3.5 CHAOS BASED-LSB STEGANOGRAPHY

It is a type of steganography that embeds data in the least significant bits of a cover image. The least significant bits of an image are those bits that have the most negligible impact on the overall quality of the image, which means that data can be embedded in the least significant bits of a cover image without significantly affecting the quality of the image; this makes LSB steganography an excellent way to hide data in plain sight.

Embedding the bits of an encrypted color image into the LSBs of the cover image in a semi-random location generated by a Henon chaotic signal using a lookup table (LUT) as the following steps:

- a. Converting the encrypted color image to binary form
The first step is to convert the encrypted color image to binary form, resulting in a binary stream of N_b bits, where N_b is the number of bits in the encrypted image.

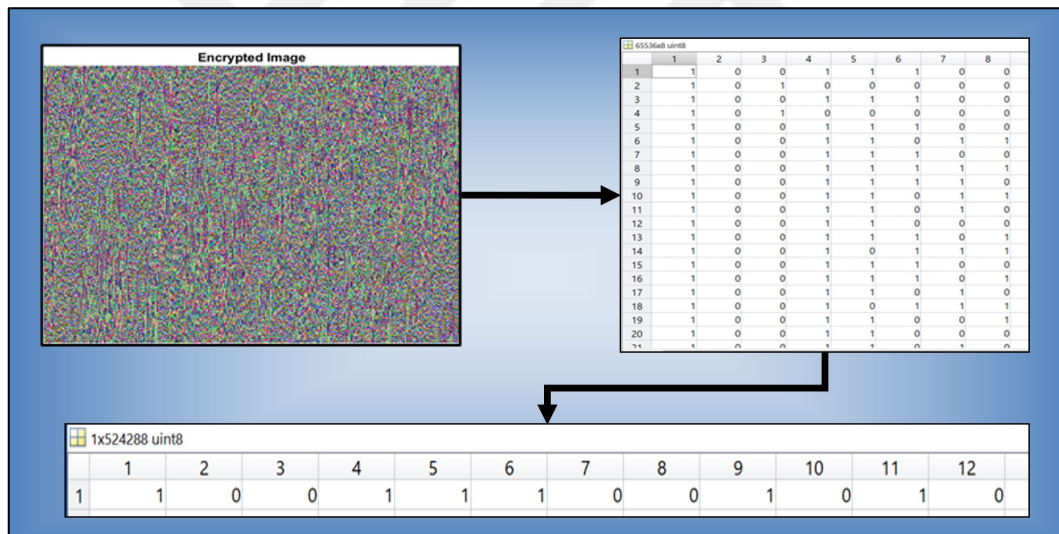


Figure 3.4: Converting the Encrypted Secret Image to Binary Form.

- b. Generating a chaotic signal by the Henon map
The next step is to generate a chaotic signal by the Henon map. The Henon map is a chaotic map that produces a sequence of numbers that are unpredictable and difficult to compress. The generated chaotic signal's length should equal the number of pixels in the cover image (N_c).

- c. Sorting the chaotic signal descend.

Once the chaotic signal has been generated, it is sorted from biggest to smallest. This will create a sorted list of chaotic numbers, which will be used to generate the random locations in the cover image where the bits of the encrypted image will be embedded.

- d. Creating a lookup table (LUT)

A lookup table (LUT) is an array of size N , where N is the length of the chaotic signal. The LUT maps the sorted chaotic numbers to their original positions in the chaotic signal.

- e. Embedding the bits of the encrypted image in the LSBs of the cover image at LUT locations

To embed the bits of the encrypted image in the LSBs of the cover image at LUT locations, start at the first bit of the encrypted image and embed it in the LSB of the cover image at the location specified by the first element in the LUT. We continue this process until all of the bits of the encrypted image have been embedded in the cover image. The final result is the *stego image*.

- f. Save and then upload the *stego image* to the cloud

The *stego image* is uploaded to the cloud so that it can be accessed from anywhere with an internet connection, such as Google Drive, Dropbox, or iCloud.

The proposed algorithm for embedding the bits of an encrypted color image into the LSBs of the cover image in a semi-random location generated by a Henon chaotic signal using a lookup table (LUT) has several advantages over other image steganography algorithms. First, it provides a high level of security by embedding the bits of the encrypted image in the cover image in a semi-random location. This makes it difficult for attackers to detect the presence of the embedded image. Second, this algorithm is scalable and can embed images of any size. Finally, this algorithm is relatively easy to implement.

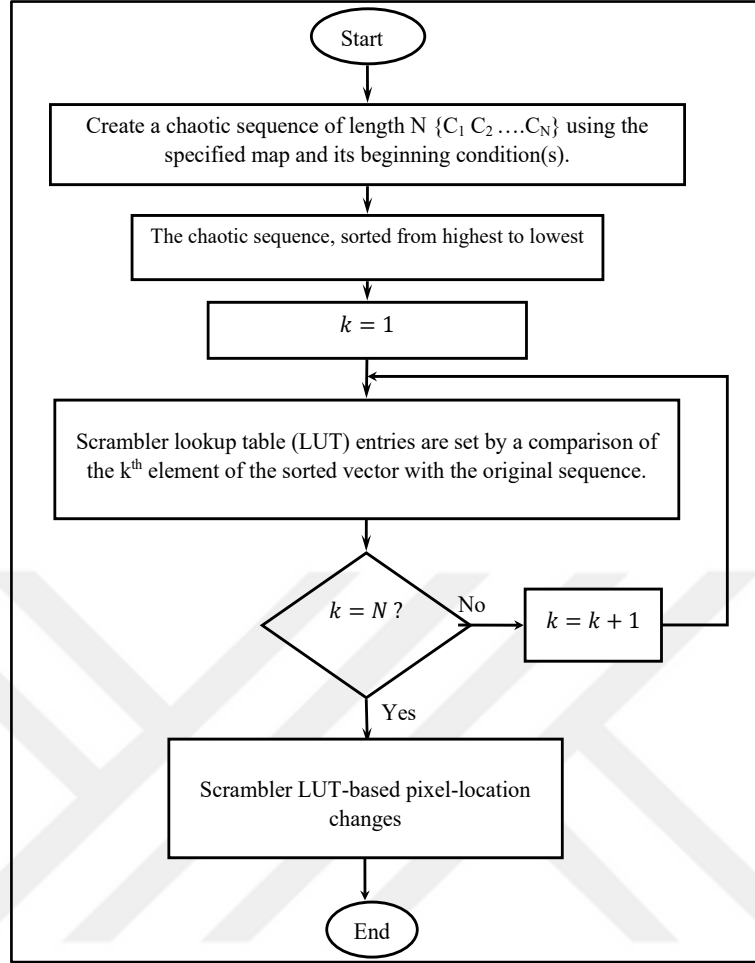


Figure 3.5: The Flowchart of the Steps of Chaotic Scrambling.

3.6 CONCLUSION

The proposed system for secure data storage in the cloud, which utilizes visual encryption based on chaos and LSB steganography, demonstrates considerable potential in safeguarding data within cloud environments. This approach synergistically leverages the advantages of two established security techniques to attain heightened security. The system exhibits characteristics of scalability, user-friendliness, and adaptability.

4. THE SIMULATION RESULTS

4.1 INTRODUCTION

In the previous chapters, there are detailed explanations of the most important aspects of security, which are encryption and decryption, as well as the importance of a chaotic system to encrypt the image data efficiently. This chapter presents the results obtained from the simulation of proposed image encryption based on chaos techniques. The results are given in terms of objective measures that measure the ability of the proposed method to encrypt images effectively. It is also shown in terms of key sensitivity and keyspace.

All the proposed algorithms are programmed in MATLAB software version (R2022a) with a 2.6 GHz CPU (i7-12700H) computer specification with 16GB of RAM running Windows 11.

4.2 THE IMAGES USE TO EVALUATING THE PROPOSED SYSTEM

Four images are used to evaluate the performance of the proposed system's first and second levels of image encryption. The list of images is as follows:

Table 4.1: Details of the Set Images Using in the Proposed System.

	Image and Histogram	Resolution and Size	Entropy
1		384*512*3 576 KB	7.3785

Table 4.2: Details of the Set Images Using in the Proposed System "Table Continued".

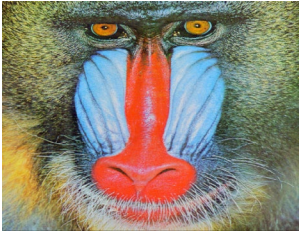
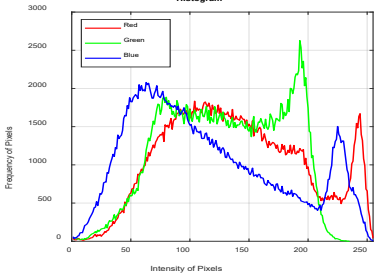
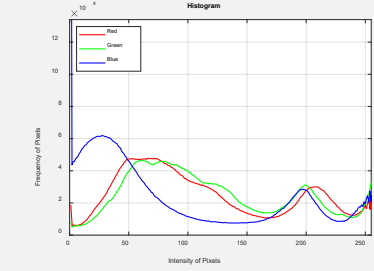
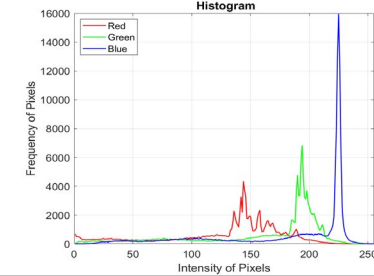
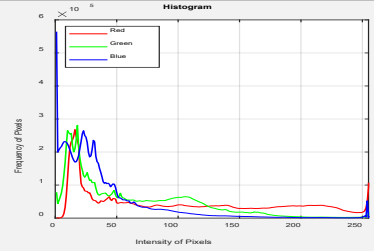
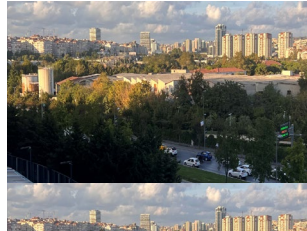
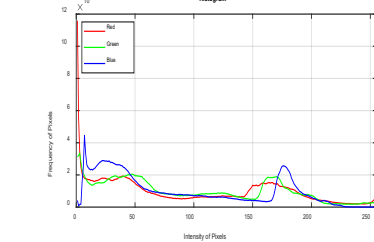
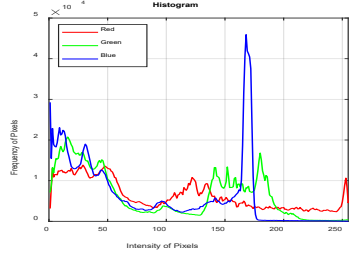
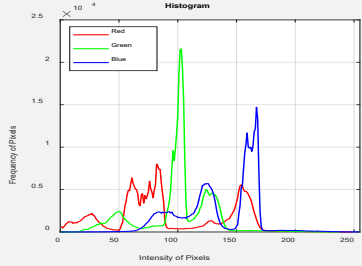
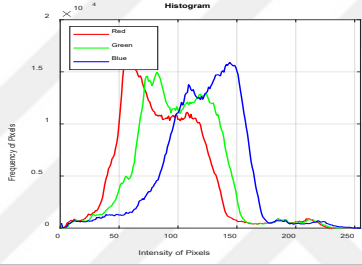
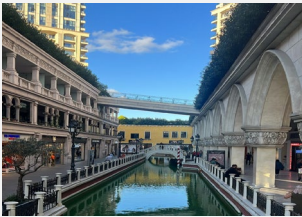
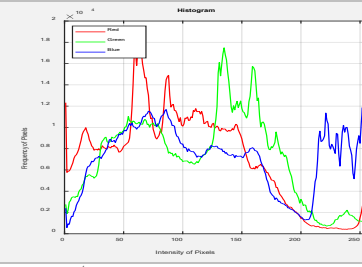
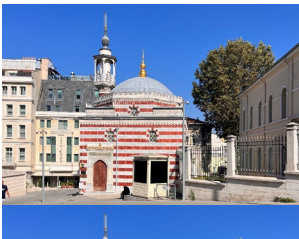
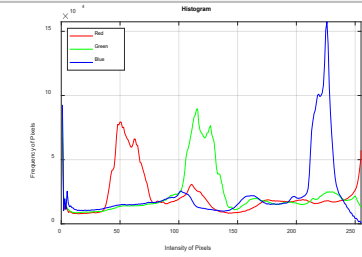
2			512*512*3 768KB	7.7629
3			2189*2972*3 18.61MB	7.8458
4			328*407*3 0.382MB	7.3600
5			3964*3023*3 34.2MB	7.3331
6			160*2422*3 7.3452MB	7.6699

Table 4.3: Details of the Set Images Using in the Proposed System "Table Continued".

7			1284*1275*3 4.6838MB	7.5813
8			600*600*3 1.03MB	7.1103
9			400*400*3 0.458MB	7.2046
10			1437*1437*3 5.22MB	7.8494
11			1916*3013*3 16.51MB	7.8233

4.3 SIMULATION RESULT OF THE CBVE METHOD

4.3.1 Testing Parameters of the Lorenz based on Lyapunov Exponents

With a big positive Lyapunov exponent, the chaotic system parameters are carefully selected. A chaotic system with a significant Lyapunov exponent value indicates that the system is very sensitive to the starting state and is acting chaotically for particular parameter values.

Computing and testing these parameters (σ , r and b) for integer order Lorenz system by Lyapunov exponent and the testing results are shown in Table (4.4). The system is chaos if it meets the following conditions:

- The system must contain three state vectors or above, which means four values of λ . Lorenz's system has three dimensions, 'state vectors' (x, y, and).
- At least one λ value must be positive.
- The addition of all Lyapunov exponents (λ_1 to λ_3) values must be negative summation.

Table 4.4: Testing the Lorenz Parameters Using the Lyapunov Exponent.

σ	R	b	λ_1	λ_2	λ_3
10	28	8/3	1	0	-14.5
16	45.92	4	1.5	0	-22.44
20	57	7	2.0522	0	-29.95
35	91	11	3.337	0.001	-50.188
51	86	7.6	2.856	0	-60.266

4.3.2 The Residual Unintelligibility of Encrypted Image

In this sub-section, we test images and display the original, encrypted, decrypted images and histogram figures. And then determine the Correlation, PSNR, and Entropy for encrypted and decrypted images, as shown in the figures and tables.

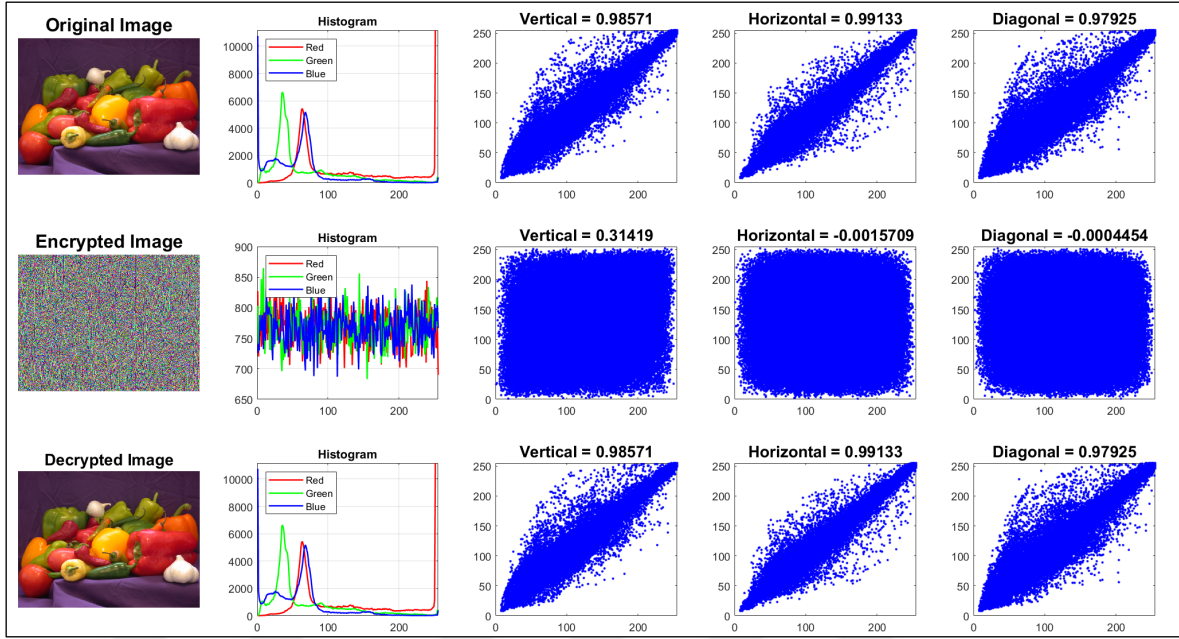


Figure 4.1: (Image 1), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc, and Dec Images Based on CBVE Method.

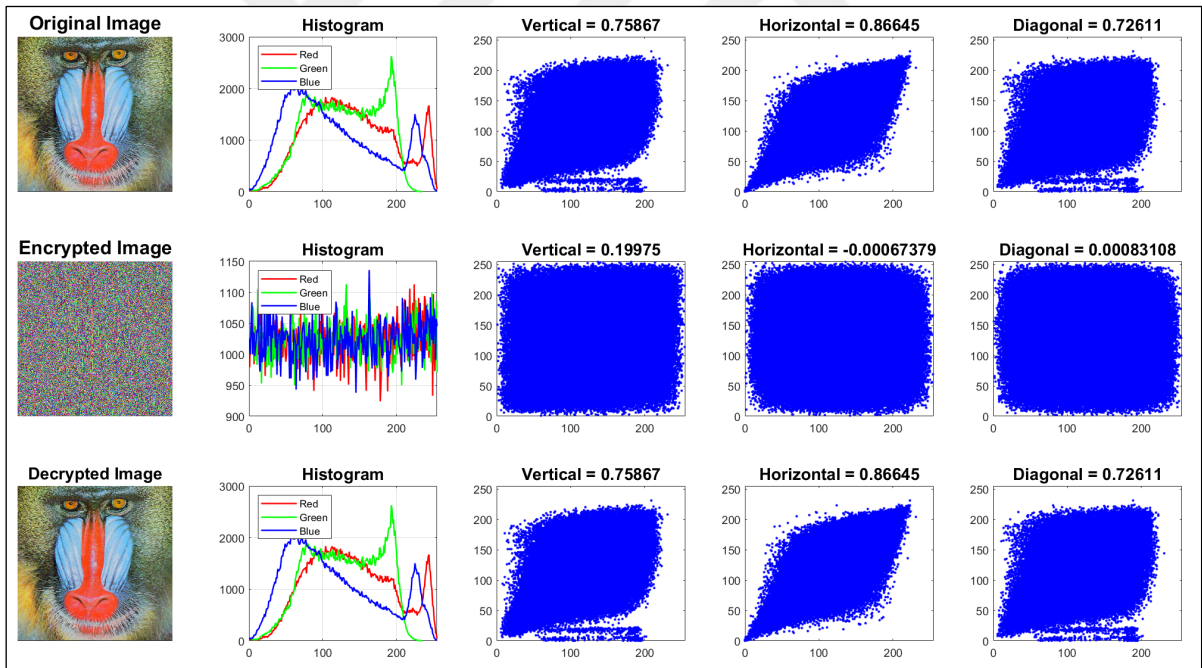


Figure 4.2: (Image 2), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc, and Dec Images Based on CBVE Method.

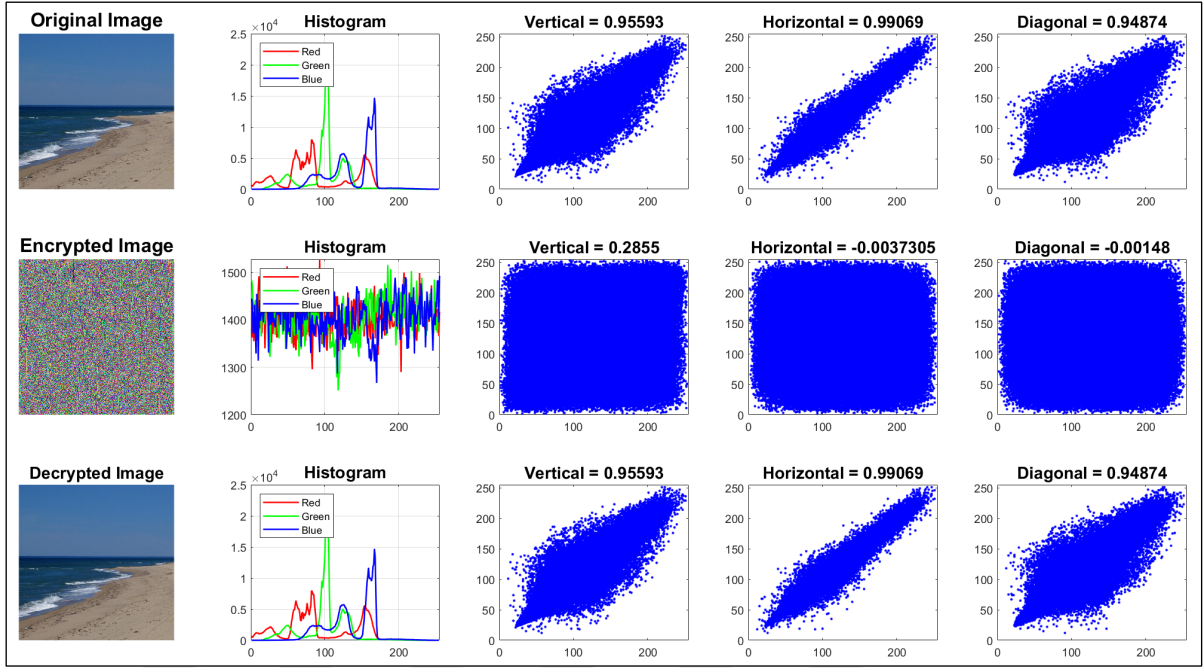


Figure 4.3: (Image 8), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc, and Dec Images Based on CBVE Method.

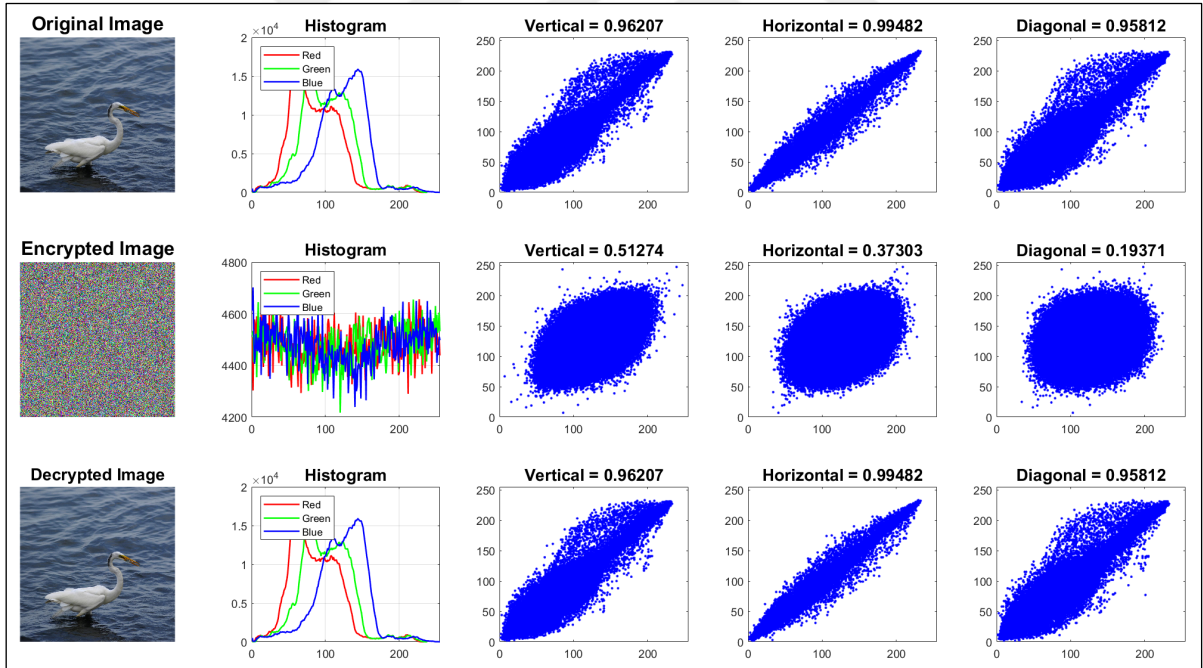


Figure 4.4: (Image 9), Histogram, and (V, H, and D) Correlation Plots and Results for Original, Enc, and Dec Images Based on CBVE Method.

Table 4.5: Encryption Results Based on the XOR and Lorenz System.

Image	MSE	PSNRdB	SSIM	Entropy	UACI	NPCR	Delay (Sec)
Image 1	11307	7.5973	0.0007	9.9996	34.113	100	0.0149
Image 2	8627	8.7723	0.0026	7.9998	30.008	100	0.0211
Image 8	7368	9.4572	0.0005	7.9998	28.097	100	0.0169
Image 9	7506	9.3767	0.0006	7.9999	28.322	100	0.0465

The results presented in the Table illustrate the efficacy of the XOR operation applied to the combination of the CRIN and image pixels. The encrypted image exhibits notable dissimilarities compared to the original image, as shown by the decreased PSNR, SSIM, and correlation values. The high values of Mean Squared Error (MSE), Entropy, Unified Average Change Intensity (UACI), and Normalized Pixel Change Rate (NPCR) indicate a lack of significant correlation between the encrypted images and their corresponding original images. The encryption algorithms exhibit high efficiency, as evidenced by the shallow delay values. The data presented in the Table demonstrates that the algorithm for encrypting images is secure and efficient.

Table 4.6: Decryption Results Based on the XOR and Lorenz System.

Image	MSE	PSNRdB	SSIM	Entropy	UACI	NPCR	Delay (Sec)
Image 1	0	Inf	1	7.3785	0	0	0.0036
Image 2	0	Inf	1	7.7629	0	0	0.0727
Image 8	0	Inf	1	7.1103	0	0	0.0627
Image 9	0	Inf	1	7.2046	0	0	0.0963

The effectiveness of the decryption process is enhanced as the Mean Squared Error (MSE) decreases. Decryption quality improves as the Peak signal-to-noise ratio (PSNR) increases. The effectiveness of the decryption process is directly proportional to the proximity of the Structural Similarity Index (SSIM) to a value of 1. The significance of decryption surpasses that of the UACI and NPCR. The rate at which decryption occurs is directly proportional to the reduction in delay. The Table displays the MSE, UACI, and NPCR values for all four images, which indicate that the decryption method effectively restores the original image, as all values are zero.

4.3.3 Brute-Force Attack for the Lorenz System-Based Chaos-Based Visual Encryption (CBVE) Method

A brute force attack is an attack where an attacker tries all possible combinations of keys until they find the correct one. In the context of CBVE, a brute force attack would involve the attacker trying all possible combinations of the Lorenz system parameters until they find the parameters used to encrypt the secret image. To illustrate how a brute force attack could be carried out on CBVE, consider the following scenario:

- a. an attacker intercepts an encrypted ciphertext image using CBVE, knowing the Lorenz system was used.
- b. They generate a random set of Lorenz system parameters to decrypt the image. If successful, they find the correct parameters. If unsuccessful, they repeat until they find the correct parameters.
- c. The number of attempts required depends on the possible combinations of Lorenz system parameters, making brute-force attacks impractical for large secret images.

For a secure system, the key space should be large enough to ensure that brute force attack is infeasible. They are increasing the keyspace exponentially. Increases the time it takes an attacker to perform a brute force attack, when the attacker tries all possible key combinations to break the system. Significantly longer key lengths increase the time it takes for an attacker to carry out an attack when an attacker attempts to destroy the system using all possible key combinations.

4.3.3.1 Key sensitivity

The encryption based on the proposed CBVE method is implemented using the Lorenz system, and then the Lorenz system has three initial conditions and three parameters. Any slight change in the value of any initial state or parameters makes a new trajectory, as illustrated in chapter two (See Figure 2. and Figure 2.). From this sensitivity, a unique chaotic random number is generated, and these numbers do not allow the original image to be recovered. (See Figure 4.5 and Figure 4.6).

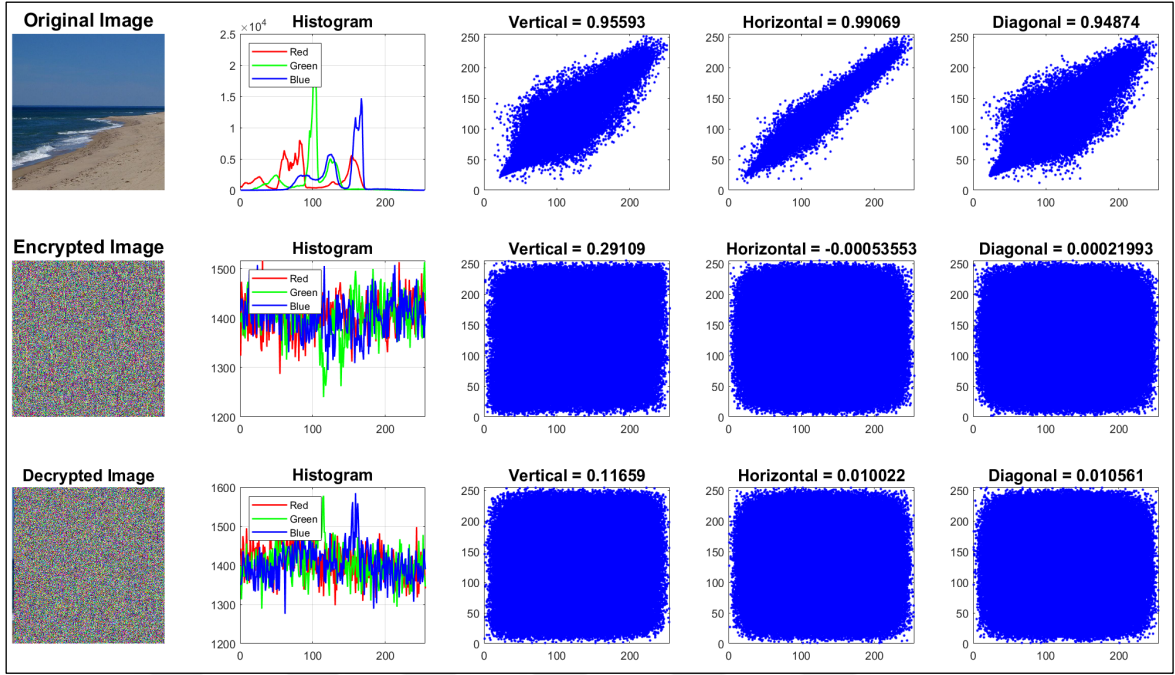


Figure 4.5: Decrypted Image 8 by Changing the Z (1) by 10^{-15} .

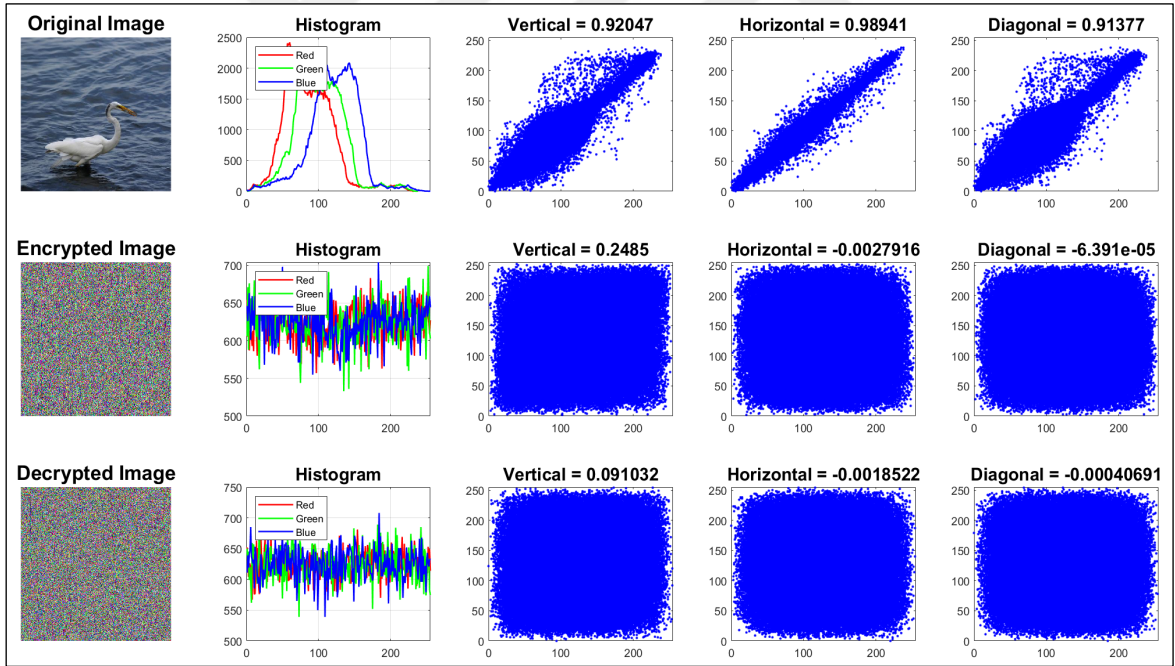


Figure 4.6: Decrypted Image 8 by Changing the Parameter (b) by 10^{-15} .

4.3.3.2 Keyspace based on lorenz system

To calculate the key space based on the Lorenz system, there are six dimensions (3 Initial conditions and three parameters)

The key space in one dimension,

$$K = \frac{1}{S} * R \quad (4.1)$$

where K is a key for each dimension, $S = 10^{-15}$ is the sensitivity in each dimension, and R is the range of functions for each dimension of any key, which is the distance between the maximum and minimum value of the Lorenz system.

$$\text{Number of keys} = \frac{1}{\text{Sensitivity}} * \text{Range} \quad (4.2)$$

$$K = 10^{15} * R \quad (4.3)$$

The keyspace for the Lorenz system (6 dimensions)

$$K_6 = \prod_{i=1}^6 K_i = \prod_{i=1}^6 [(10^{15}) * R_i] \quad (4.4)$$

Then

$$K_d = (10^{15})^6 \prod_{i=1}^d [R_i] \quad (4.5)$$

The keyspace in XOR operation is based on the Lorenz System,

$$K_6 = (10^{15})^6 [R_x * R_y * R_z * R_\sigma * R_r * R_b] \quad (4.6)$$

where $R_x = 40, R_y = 40$ and $R_z = 20$. Then:

$$K_6 = (10^{15})^6 (40) * (40) * (20) * R_\sigma * R_r * R_b \quad (4.7)$$

$$K_6 = 10^{90} * 32000 * R_\sigma * R_r * R_b \quad (4.8)$$

$(32 * R_\sigma * R_r * R_b)$ can be neglected because it represents minimal values compared with the 10^{93} . The key space based on the Lorenz model is at least equal:

$$K_6(\text{Lorenz}) \geq 10^{93} \approx (2^{309}) \quad (4.9)$$

4.3.4 Advantages of the CBVE Method-Based Image Encryption

The CBVE method has garnered significant attention in image encryption due to its notable attributes, including robust security measures, scalability to handle large datasets, user-friendly implementation, and adaptable functionality.

The utilization of a Chaotic Random Integer Number (CRIN) is based on generating a random integer derived from the Lorenz chaotic system. The Lorenz system is a set of three differential equations known for its ability to produce chaotic dynamics. The sensitivity of this system to initial conditions renders it a suitable mechanism for generating random numbers.

The CBVE method can encrypt images of varying dimensions using the CRIN, which relies on a random number generator. The implementation and utilization of this system are relatively straightforward. Furthermore, the CBVE method can encrypt images of diverse formats.

However, the CBVE method is considered a relatively recent approach in image encryption and has not been extensively researched compared to other existing methods. Consequently, this limited body of knowledge poses a challenge for potential attackers in devising effective strategies to compromise the security of the CBVE system. Notwithstanding these benefits, the CBVE technique continues to hold promise as a viable approach for image encryption.

4.4 RESULTS OF LSB STEGANOGRAPHY BASED ON HENON MAP

In the third chapter, it was clarified that the process of hidden confidential data is adopted as a second security level after encryption. Here in this part, the most prominent results of this level will be shown, represented by hiding the encrypted bits of the color image within the cover image.

4.4.1 Embedded and Reconstructed Images Results

For the masking process to work correctly, the size of the cover image must be many times or larger than the image to be hidden (because masking is done only in the first bit of each pixel). The initial values and the parameters of the Henon map are:

$X(1) = 1$	$Y(1) = -0.7$	$r\text{-parameter} = 1.4$	$b\text{-parameter} = 0.3$
------------	---------------	----------------------------	----------------------------

We will show some examples as follows:

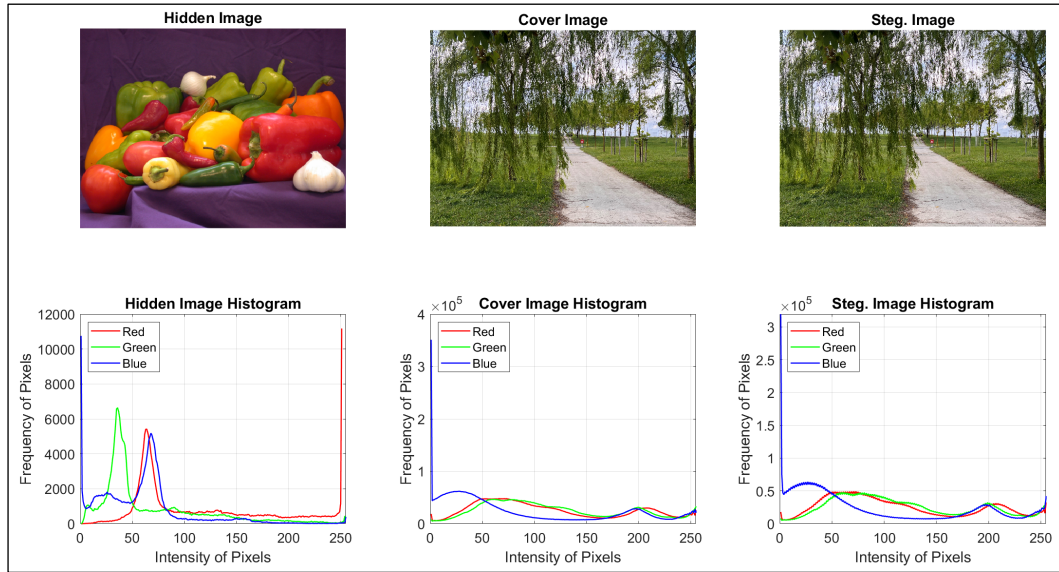


Figure 4.7: The Results of LSB Steganography Based on Henon for Embedded Image 1 inside Image 3.



Figure 4.8: Recovered the Hidden Image 1 from the Stego Image Using the Same Initial Values and Parameters of Henon Map.

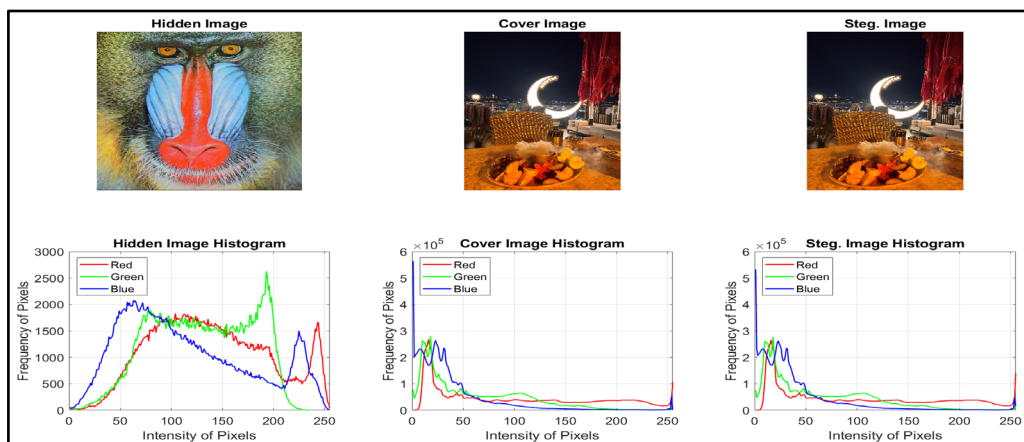


Figure 4.9: The Results of LSB Steganography Based on Henon for Embedded Image 2 Inside Image 5.



Figure 4.10: Recovered the Hidden Image 2 from the Stego Image Using the Same Initial Values and Parameters of Henon Map.

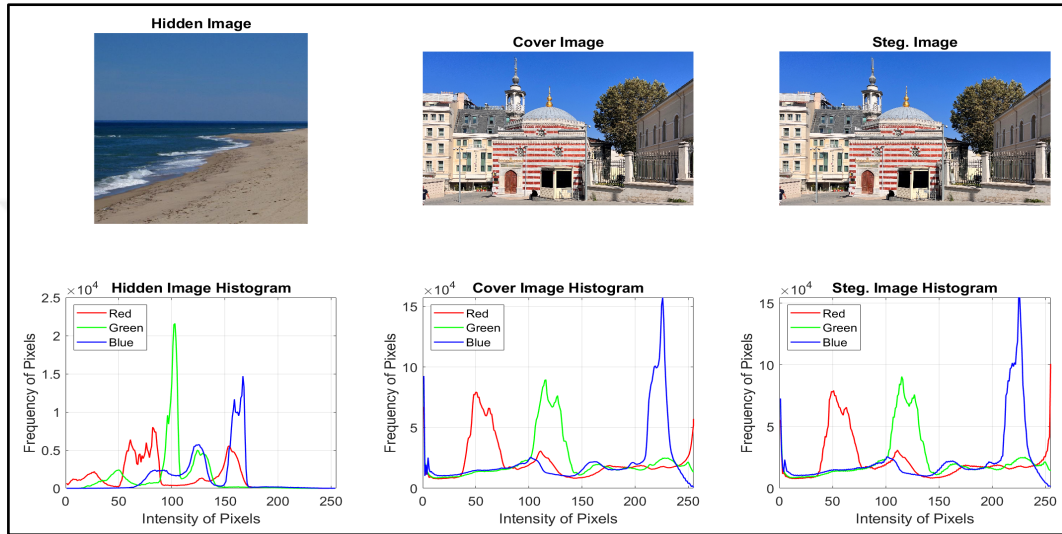


Figure 4.11: The Results of LSB Steganography Based on Henon for Embedded Image 8 inside Image 11.



Figure 4.12: Recovered the Hidden Image 8 from the Stego Image Using the Same Initial Values and Parameters of the Henon Map.

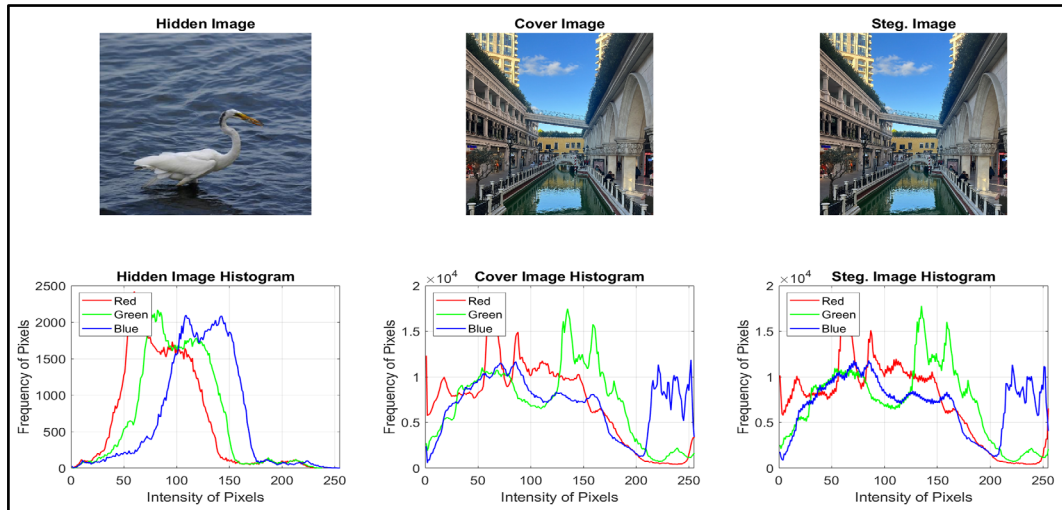


Figure 4.13: The Results of LSB Steganography Based on Henon for Embedded Image 9 Inside Image 10.



Figure 4.14: Recovered the Hidden Image 9 from the Stego Image Using the Same Initial Values and Parameters of Henon Map.

Table 4.7: The Steganography and De-Steganography Results.

Cover	Hidden	Results	MSE	PSNR _{dB}	Correlation	SSIM	Delay (Sec)
Image 3	Image 1	Steg.	0.121	57.308	0.996	0.9999	0.867
		De-Steg.	0	Inf	1	1	1.183
Image 5	Image 2	Steg.	0.087	58.712	0.9999	0.9599	1.647
		De-Steg.	0	Inf	1	1	2.133
Image 11	Image 8	Steg.	0.249	54.162	0.9999	0.9437	0.787
		De-Steg.	0	Inf	1	1	1.466
Image 10	Image 9	Steg.	0.351	52.684	0.99999	0.9075	0.255
		De-Steg.	0	Inf	1	1	0.569

From Figure 4.7 to Figure 4.14 and Table 4.7 shows the extent of the change in the cover image after hiding the data. Changes in the cover are imperceptible and invisible to the

human eye. It also shows that the difference in the histogram between the original image and the stego-image is indistinguishable. This indicates that the proposed system is effective and does not arouse the suspicion of hackers that there is data hidden in the available cover image.

Also, the value of the MSE is equal to 0.35 or less, the value of PSNR is more than 52 dB, and the amount of correlation between the original image and the image in which the data hid it is very close to 1 (0.9999), and this shows that the correlation between the two images is too significant to distinguish between them.

4.4.2 The Brute-Force Attack for LSB Steganography Using Henon Chaotic Map

A brute force attack is a cryptanalytic attack that attempts to recover the secret message in a steganographic image by trying all possible combinations of secret message bits. Brute force attacks are effective against LSB steganography because the secret message bits are hidden in the least significant bits of the cover image, which are the easiest to modify.

The effectiveness of a brute force attack against LSB steganography using the Henon chaotic map depends on the size of the secret message and the length of the Henon chaotic sequence. The larger the secret message and the longer the Henon chaotic sequence, the more difficult it is to perform a successful brute-force attack.

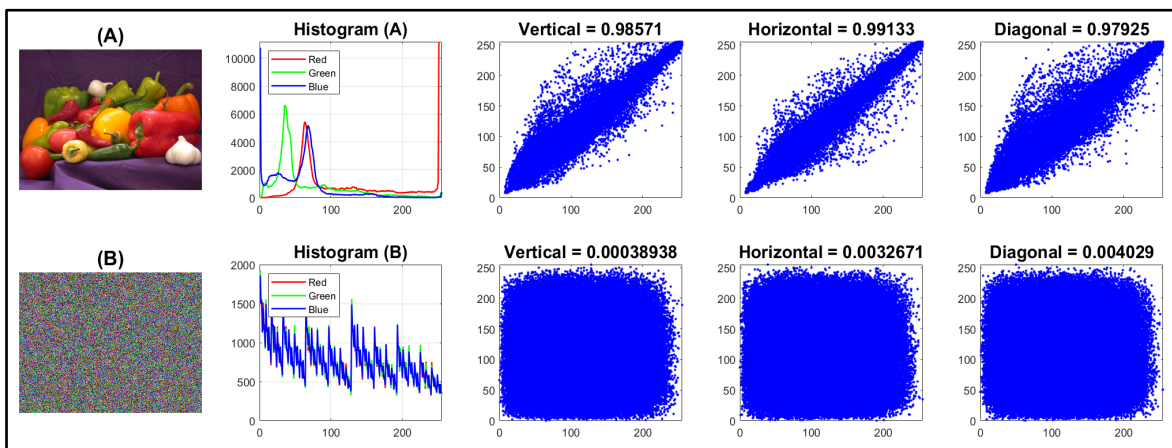


Figure 4.15: Recovered the Secret Image from the Stego Image at $\Delta x=2e-16$. (A) Original Secret Image 1 and (B) Recovered Secret Image.

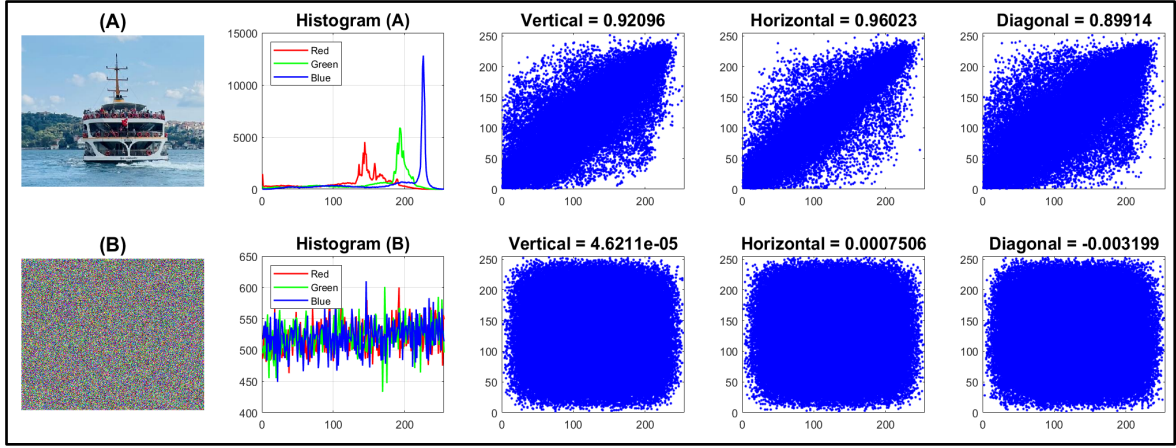


Figure 4.16: Recovered the Secret Image from the Stego Image at $\Delta y=2e-16$. (A) Original Secret Image 4 and (B) Recovered Secret Image.

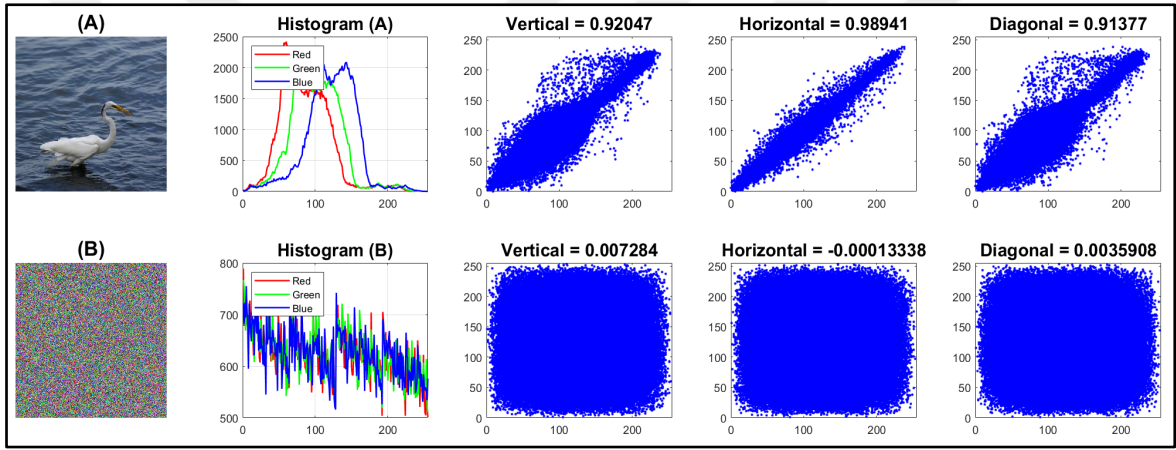


Figure 4.17: Recovered the Secret Image from the Stego Image at $\Delta r=2e-16$. (A) Original Secret Image 9 and (B) Recovered Secret Image.

From Figure 4.15 to Figure 4.17, it is shown that any small change in the parameters or starting points of the Henon system does not allow the hidden image to be retrieved, and the resulting image is completely encrypted.

The key space based on the Henon map at two parameters and two initial values is calculated as follows:

$$Key(Henon) = \left(\frac{1}{2 \times 10^{-16}} \right)^4 \quad (4.10)$$

$$Key(Henon) = (5 \times 10^{15})^4 = 625 \times 10^{60} \quad (4.11)$$

$$Key(Henon) \approx 10^{62} \approx 2^{206} \quad (4.12)$$

4.4.3 Saved Image Types for the Stego Images

Specific steganography algorithms determine the best-saved stego image type. However, certain broad principles exist. Lossless image formats are excellent for steganography—lossless image formats store without discarding information, unlike lossy formats. Lossless image formats reduce the danger of hidden message corruption. Some prominent lossless image formats are:

- a. PNG is a lossless image format supported by most online browsers and image editing applications. PNG pictures are tiny and suitable for stego images.
- b. BMP is a lossless image format supported by all major operating systems. While BMP pictures are more significant than PNG images, they are more compatible with legacy systems.
- c. TIFF is a popular lossless image format for professional photography and printing. TIFF pictures are large yet the most compatible and high-quality lossless image format.

Generally, high-bit depth image formats are preferable for steganography. High-bit depth image formats have more bits per pixel, giving the hidden message more room to hide. The popular high-bit depth RAW image format includes:

Keep in mind that some steganography algorithms are optimized for lossy image formats. The JPEG steganography technology hides hidden messages in JPEG pictures. Choosing a stored image type also depends on the private message's size. Consider a lossless image format with high bit depth for a significant personal statement. A lower-bit-depth lossy image format may work if the secret message is tiny.

Finally, stego image security is independent of stored image type. Steganography algorithm strength determines stego idea security.

4.5 THE SIMULATION RESULTS OVER ALL THE PROPOSED SYSTEM

The CBVE method and chaos-based steganography can provide a high level of security for data storage and communication, primarily when used in conjunction with other security measures.

4.5.1 The Security Results

The following simulation results show the performance of the proposed chaos-based visual cryptography and LSB steganography (CBVE-LSB) scheme:

Firstly, the color image is encrypted by the CBVE method and embedded the encrypted image inside the cover image by the Chaos-Based LSB-Steganography, and the saved image is uploaded to the cloud.

On the other side, downloaded the stego. Image from the cloud and recovered bits and reconstructed the encrypted image by the De-Steganography process using the same initial values and parameters of the Henon map. They were finally decrypted for the recovered encrypted image by the same initial values and parameters of the Lorenz system. The following images and tables show the original, cover, encrypted image, stego, recovered, and decrypted images. The Table shows the MSE, PSNR, Correlation, and SSIM values for four cases:

Case 1: Image 4 is the secret (A), and Image 11 is the cover (B)

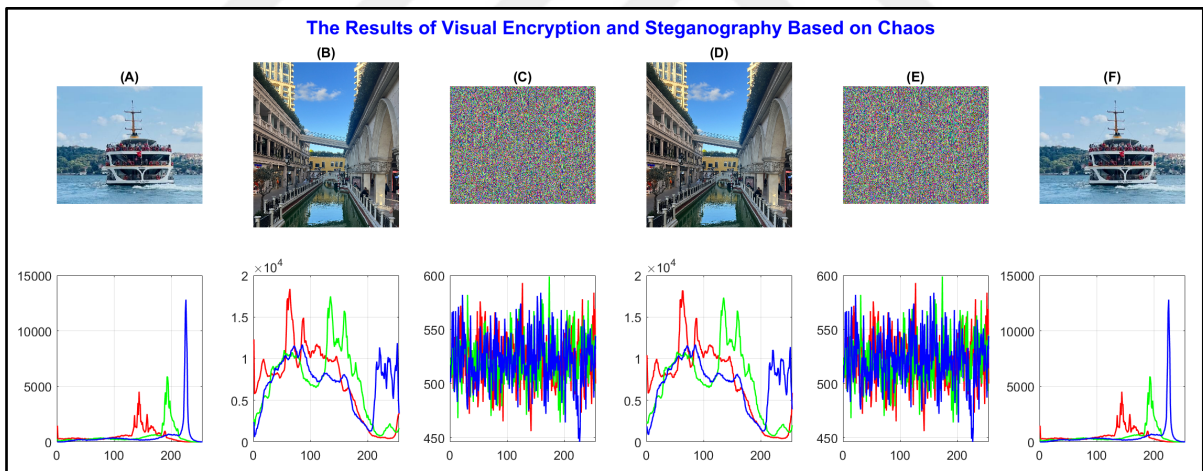


Figure 4.18: Images and Histogram Plots for A- Secret Image 4 B- Cover Image 11 C- Encrypted Image D- Steg Image E- Rec of Enc Image F- Dec of Rec Image.

Table 4.8: Simulation Results for the Images in Figure 4.18.

Image Results	MSE	PSNR _{dB}	Correlation	SSIM
Encryption (B)	10006	8.128	-0.0034	0.0019
Steganography (C)	0.29222	53.474	0.99996	0.9185
De-Steganography (D)	10006	8.128	-0.0034	0.0019
Decryption (F)	0	Inf	1	1

Case 2: Image 1 is the secret (A), and Image 6 is the cover (B).

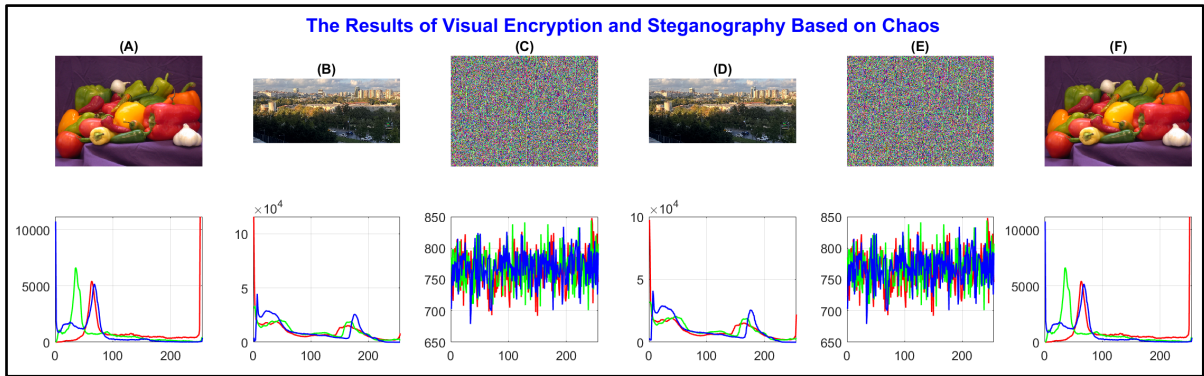


Figure 4.19: Images and Histogram Plots for A- Secret Image 1 B- Cover Image 6 C- Encrypted Image D- Steg Image E- Rec of Enc Image F- Dec of Rec Image.

Table 4.9: Simulation Results for the Images in Figure 4.19.

Image Results	MSE	PSNR _{dB}	Correlation	SSIM
Encryption (B)	11351	7.5803	-0.0048	0.0006
Steganography (C)	0.3059	53.274	0.99997	0.9565
De-Steganography (D)	11351	7.5803	-0.0048	0.0006
Decryption (F)	0	Inf	1	1

Case 3: Image 9 is the Secret (A), and Image 3 is the Cover (B).

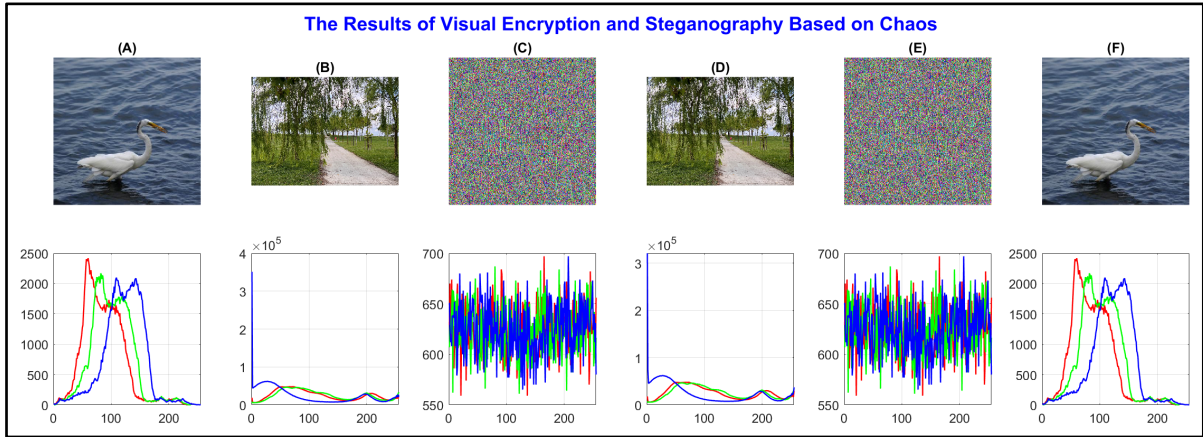


Figure 4.20: Images and Histogram Plots for A- Secret Image 9 B- Cover Image 3 C- Encrypted Image D- Steg Image E- Rec of Enc Image F- Dec of Rec Image.

Table 4.10: Simulation Results for the Images in Figure 4.20.

Image Results	MSE	PSNR _{dB}	Correlation	SSIM
Encryption (B)	7492	9.3845	-0.0033	-6.31e-5
Steganography (C)	0.9832	58.204	0.99996	0.9965
De-Steganography (D)	7492	9.3845	-0.0033	-6.31e-5
Decryption (F)	0	Inf	1	1

The PSNR and MSE values for the encrypted image indicate that the CBVE method introduces a high MSE distortion to the original image and low correlation, SSIM, and low PSNR.

The MSE and PSNR values for the stego image indicate that embedding the encrypted image in the cover image does not significantly distort the original image. This is important because it means that the stego image can be transmitted or stored without any noticeable loss in quality.

The results suggest that the CBVE-based color image encryption and embedding in a cover image is a promising technique for securing color images. It achieves a good level of security and quality, making it suitable for use in a variety of applications.

4.5.2 Brute-Force Attacks Over all the Proposed System

The following results by changing any parameters or initial values and recovering and decrypting the secret image as shown in the following figures:

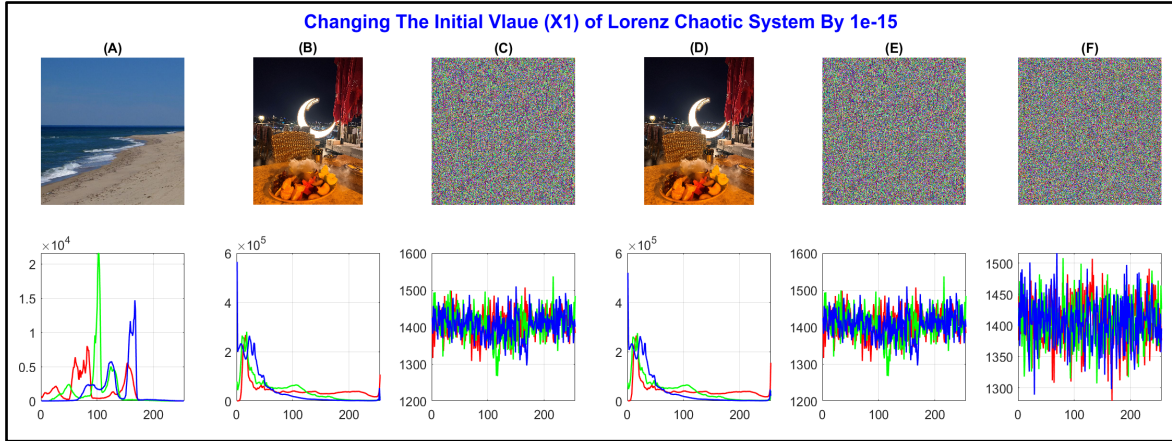


Figure 4.21: Recovered the Secret Image After Changed X (1) of Lorenz System by 1e-15.

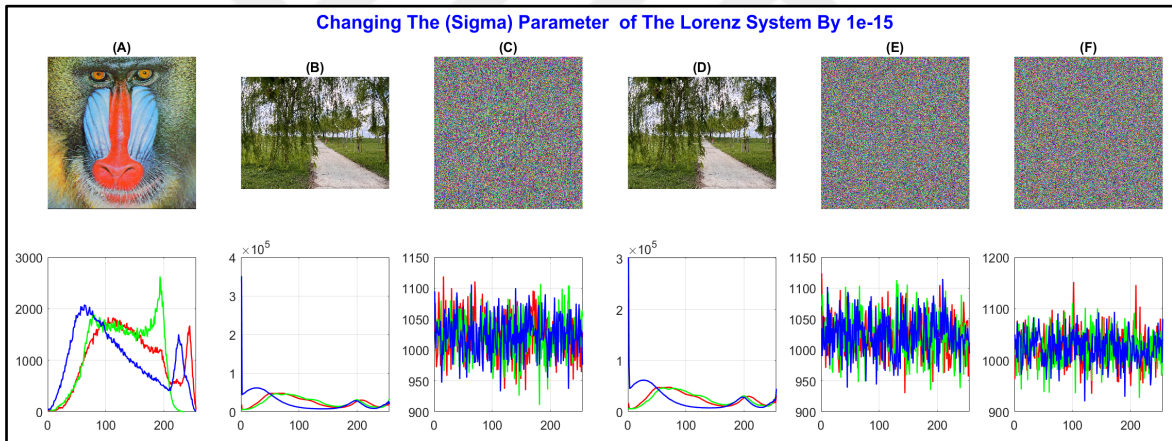


Figure 4-22: Recovered the Secret Image After Changed Sigma of Lorenz System by 1e-15.

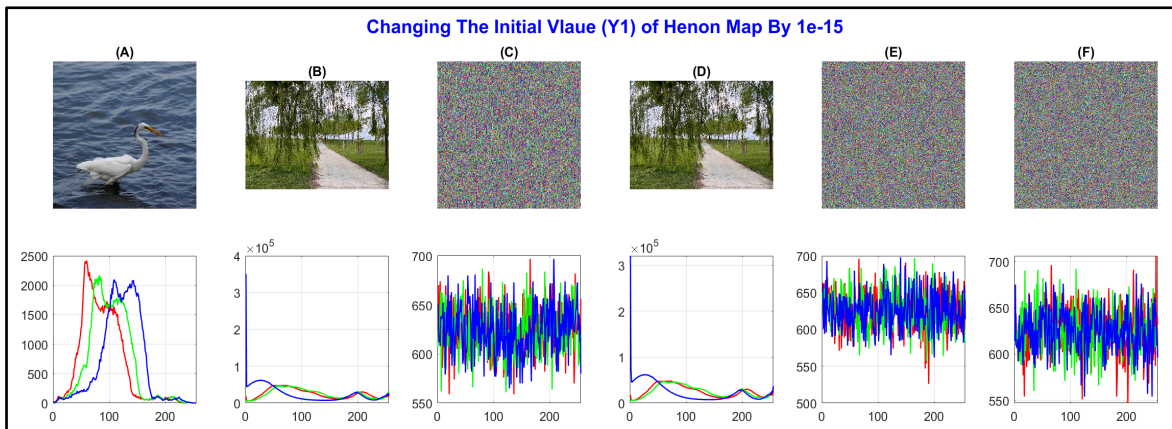


Figure 4.23: Recovered the Secret Image After Changed Y (1) of the Henon Map by 1e-15.

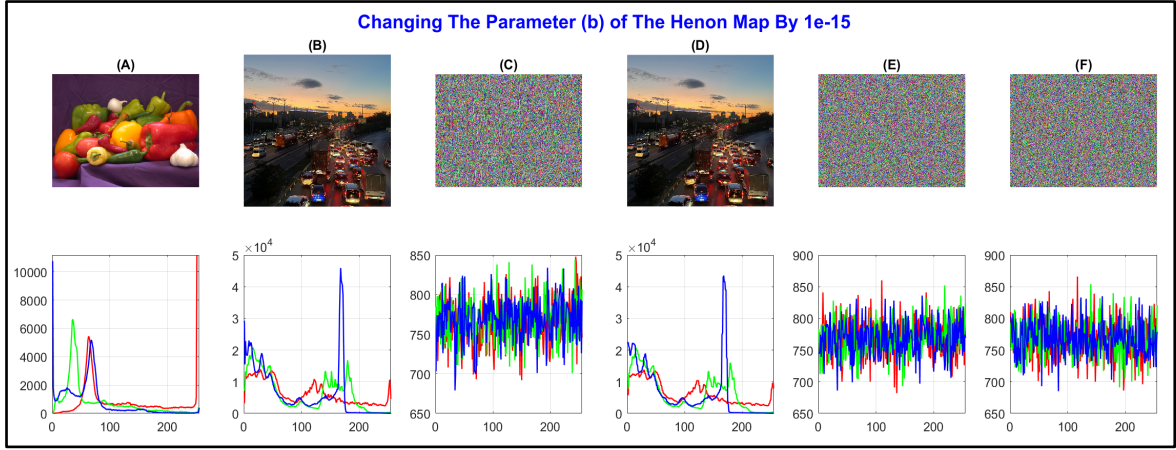


Figure 4.24: Recovered the Secret Image After Changed (B) Parameter of the Henon Chaotic Map by 1e-15.

From the above figures, it is clear that any slight change in any parameters or initial values of the Lorenz system used in encryption and the parameters and initial values of the Henon system don't allow for the recovery of the secret image.

The keyspace for all the proposed systems represents the multiplication of the keyspace of the Lorenz system and the Henon map.

$$Key\ Space(All) = (N.of\ Keys_{Lorenz}) * (N.of\ Keys_{Henon}) \quad (4.13)$$

$$Key\ Space(All) = 2^{309} * 2^{206} = 2^{515} \quad (4.14)$$

4.5.3 Comparing the Proposed System to Previous Research

Here, we will examine simulation results from the proposed system that uses two chaos-based encryption levels to encrypt images. As shown in Table 4. and Table 4.11, we will compare them to prior research between the key and the original image to produce the encrypted image.

Table 4.9: The Simulation Results for Other Research.

Ref.	Image	MSE	PSNR (dB)	Corr	Entropy	Delay (Sec)
Ref. [52]	Image 1	10033	8.1624	0.00175	7.9968	2.637
Ref. [53]	Image 1	-	-	0.0035	7.9959	-
Ref. [25]	Image 2	-	8.9311	0.5879	7.9973	-
	Image 1	-	8.6262	0.4917	7.9997	-
Ref. [54]	Image 1	-	-	0.0017	7.9976	-
Ref. [55]	Image 1	9445	8.38	-	7.9991	-
	Image 2	8413	8.88	-	7.9994	-

From the simulation results in Table 4., it is clear that the results of the proposed system are equal to or better than those of previous studies. Also, the encryption time in the fun system is much better than that in Ref [52]. Table 4.11 shows the number of keys in previous articles and their comparison with the number of keys in the proposed system.

Table 4.11: The Keyspace in the Proposed System is Compressed with the Other Articles.

References	Key Space
Ref. [5]	2^{266}
Ref. [10]	2^{319}
Ref. [52]	2^{478}
Ref. [25]	$10^{144} = 2^{479}$
Ref. [56]	Case1= 2^{128} and Case2= 2^{192}
Ref. [57]	2^{208}
All Proposed System	2^{515}

5. CONCLUSIONS AND FUTURE WORK

5.1 CONCLUSIONS

The proposed system is a significant contribution to the field of information security. The main conclusions for the proposed method as the following:

- a. The proposed system combines two chaotic systems, the Lorenz system and the Henon map, to achieve high security, scalability, efficiency, and adaptability for color image encryption and steganography.
- b. The proposed system achieves high image quality, with minimal distortion introduced to the stego image.
- c. The proposed system is more secure than existing color image encryption and steganography methods that use only a single chaotic system due to the combined use of the Lorenz system and the Henon map.
- d. The proposed system is more resistant to brute-force attacks than existing methods due to using random locations generated by the Henon map.
- e. The proposed system is more efficient than existing methods that use multiple chaotic systems, as it only requires two chaotic systems to achieve high security.
- f. The proposed system is more adaptable to different image formats and sizes than existing methods, making it more versatile and practical.
- g. The proposed system is compatible with existing cloud storage platforms, making it easy to implement and use in real-world applications because the time delay is low.
- h. The proposed system can significantly improve the security of color image encryption and steganography.
- i. The proposed image encryption scheme is fast, evident from the delay's low values, and can be used to encrypt large images.

- j. The greater the number of parameters and the initial values, the greater the number of keys (keyspace). Therefore, the Lorenz system uses six dimensions for the number of keys (three parameters and three initial values), while four dimensions (two initial values and two parameters) in the Henon Map.

5.2 FUTURE WORKS

- a. Extend the proposed system to support other media types, such as video and audio. And investigate the use of other chaotic systems for color image encryption and steganography.
- b. Develop new and improved methods for generating random locations based on the Henon map or other chaotic systems.
- c. Develop new methods for detecting and preventing steganalysis attacks on the proposed system.
- d. Implement the proposed system in hardware such as FPGA or FPAA to improve performance and efficiency.
- e. Develop a user-friendly interface for the proposed system to make it easier. And evaluate the performance of the proposed approach in real-world applications.
- f. Develop new applications for the proposed system, such as secure data transmission over public networks and secure cloud storage.

REFERENCES

- [1] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Noise Reduction of Chaotic Masking System using Repetition Method," 2016. [Online]. Available: <https://www.researchgate.net/publication/291356303>
- [2] H. N. Abdullah, S. S. Hreshee, and A. K. Jawad, "Design of Efficient noise reduction scheme for secure speech masked by chaotic signals," *J. Am. Sci.*, vol. 11, no. 7, pp. 49–55, 2015.
- [3] M. Moghtadaei and M. R. Hashemi Golpayegani, "Complex dynamic behaviors of the complex Lorenz system," *Sci. Iran.*, vol. 19, no. 3, pp. 733–738, 2012, doi: 10.1016/j.scient.2010.11.001.
- [4] S. S. Hreshee, H. N. Abdullah, and A. K. Jawad, "A high security communication system based on chaotic scrambling and chaotic masking," *Int. J. Commun. Antenna Propag.*, vol. 8, no. 3, pp. 257–264, 2018, doi: 10.15866/irecap.v8i3.13541.
- [5] A. K. Jawad, H. N. Abdullah, and S. S. Hreshee, "Secure speech communication system based on scrambling and masking by chaotic maps," in *IEEE, International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, 2018, pp. 7–12. doi: 10.1109/ICASEA.2018.8370947.
- [6] A. Mahdi and S. S. Hreshee, "Design and implementation of voice encryption system using XOR based on Hénon map," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, IEEE, 2016, pp. 1–5.
- [7] O. M. Al-Hazaimah, "A new speech encryption algorithm based on dual shuffling Hénon chaotic map," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 3, pp. 2203–2210, 2021, doi: 10.11591/ijece.v11i3.pp2203-2210.
- [8] A. Kiani-B, K. Fallahi, N. Pariz, and H. Leung, "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter," *ELSEVIER, Commun. Nonlinear Sci. Numer. Simul.*, vol. 14, no. 3, pp. 863–879, 2009, doi: 10.1016/j.cnsns.2007.11.011.

- [9] A. Mahdi, A. K. Jawad, S. S. Hreshee, A. Mahdi, and A. K. Jawad, "Digital Chaotic Scrambling of Voice Based on Duffing Map," *Commun. Eng. J.*, vol. 1, no. 2, pp. 16–21, 2016, doi: 10.11648/j.cej.20160102.11.
- [10] E. A. R. Hussein, M. K. Khashan, and A. K. Jawad, "A high security and noise immunity of speech based on double chaotic masking," *Int. J. Electr. Comput. Eng.*, vol. 10, no. 4, 2020, doi: 10.11591/ijece.v10i4.pp4270-4278.
- [11] S. B. Sadkhab, A. M. Raheema, and S. M. A. Sattar, "Design and Implementation Voice Scrambling Model Based on Hybrid Chaotic Signals," *IEEE, 1st Int. Sci. Conf. Comput. Appl. Sci. CAS 2019*, pp. 193–198, 2019, doi: 10.1109/CAS47993.2019.9075626.
- [12] Q. Lu, C. Zhu, and G. Wang, "A novel S-box design algorithm based on a new compound chaotic system," *Entropy*, vol. 21, no. 10, p. 1004, 2019.
- [13] Ameer K. Jawad, Wa'il a. H. Hadi, and Hyayder F. Y. Hussein, "Enhancement of Image Transmission Using Chaotic Interleaver over Wireless Sensor Network," 2016. [Online]. Available: www.ijntr.org
- [14] X. Li, H. Yu, H. Zhang, X. Jin, H. Sun, and J. Liu, "Video encryption based on hyperchaotic system," *Multimed. Tools Appl.*, vol. 79, no. 33–34, pp. 23995–24011, 2020, doi: 10.1007/s11042-020-09200-1.
- [15] A. A. Zaher, "An improved chaos-based secure communication technique using a novel encryption function with an embedded cipher key," *ELSEVIER, Chaos, Solitons and Fractals*, vol. 42, no. 5, pp. 2804–2814, 2009, doi: 10.1016/j.chaos.2009.04.032.
- [16] A. A. Zaher and A. Abu-Rezq, "On the design of chaos-based secure communication systems," *ELSEVIER, Commun. Nonlinear Sci. Numer. Simul.*, vol. 16, no. 9, pp. 3721–3737, 2011, doi: 10.1016/j.cnsns.2010.12.032.
- [17] K. H. Sun, X. Liu, and C. X. Zhu, "The 0-1 test algorithm for chaos and its applications," *Chinese Phys. B*, vol. 19, no. 11, pp. 1–7, 2010, doi: 10.1088/1674-1056/19/11/110510.
- [18] C. T. M. Clack, "Dynamics of the Lorenz Equations," p. 32, 2006.

- [19] W. K. Lee, R. C. W. Phan, W. S. Yap, and B. M. Goi, “a novel parallel chaos-based image encryption scheme,” *Springer, Nonlinear Dyn.*, vol. 92, no. 2, pp. 575–593, 2018, doi: 10.1007/s11071-018-4076-6.
- [20] M. Ashtiyani, P. Birgani, and S. Madahi, “Speech Signal Encryption Using Chaotic Symmetric Cryptography,” *Basic Appl. Sci. Res.*, vol. 2, no. 2, pp. 1678–1684, 2012, [Online]. Available: [http://www.textroad.com/pdf/JBASR/J. Basic. Appl. Sci. Res., 2\(2\)1678-1684, 2012.pdf](http://www.textroad.com/pdf/JBASR/J. Basic. Appl. Sci. Res., 2(2)1678-1684, 2012.pdf)
- [21] W. Al Nassan, T. Bonny, and A. Baba, “A New Chaos-Based Cryptoystem for Voice Encryption,” *IEEE Xplore, Int. Conf. Signal Process. Inf. Secur. ICSPIS 2020*, vol. 3, pp. 1–4, 2020, doi: 10.1109/ICSPIS51252.2020.9340132.
- [22] M. Ahmad, “Chaos Based Mixed Keystream Generation for Voice Data Encryption,” *Int. J. Cryptogr. Inf. Secur.*, vol. 2, no. 1, pp. 39–48, 2012, doi: 10.5121/ijcis.2012.2104.
- [23] M. Lawnik, L. Moysis, and C. Volos, “Chaos-Based Cryptography: Text Encryption Using Image Algorithms,” *Electron.*, vol. 11, no. 19, pp. 1–13, 2022, doi: 10.3390/electronics11193156.
- [24] A. J. Mansoor, H. N. Abdullah, M. F. Al-Gailani, and H. T. Ziboon, “Chaotic encryption system based on pixel value and position transformation for color images,” *18th IEEE Int. Multi-Conference Syst. Signals Devices, SSD 2021*, no. March, pp. 433–439, 2021, doi: 10.1109/SSD52085.2021.9429368.
- [25] H. H. Alsaabri and S. S. Hreshee, “Robust Image Encryption Based on Double Hyper Chaotic Rabinovich System,” *7th Int. Conf. Contemp. Inf. Technol. Math. ICCITM 2021*, pp. 146–152, 2021, doi: 10.1109/ICCITM53167.2021.9677722.
- [26] W. A. Al-Musawi, M. A. A. Al-Ibadi, and W. A. Wali, “Artificial intelligence techniques for encrypt images based on the chaotic system implemented on field-programmable gate array,” *IAES Int. J. Artif. Intell.*, vol. 12, no. 1, pp. 347–356, 2023, doi: 10.11591/ijai.v12.i1.pp347-356.

- [27] A. H. ElSafty, M. F. Tolba, L. A. Said, A. H. Madian, and A. G. Radwan, "Hardware realization of a secure and enhanced s-box based speech encryption engine," *Analog Integr. Circuits Signal Process.*, vol. 106, no. 2, pp. 385–397, Feb. 2021, doi: 10.1007/S10470-020-01614-Z.
- [28] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study," *J. Comput. Commun.*, vol. 7, no. 3, pp. 8–18, 2019.
- [29] M. Dua, D. Makhija, P. Y. L. Manasa, and P. Mishra, "3D chaotic map-cosine transformation based approach to video encryption and decryption," *Open Comput. Sci.*, vol. 12, no. 1, pp. 37–56, 2022, doi: 10.1515/comp-2020-0225.
- [30] I. Bakurov, M. Buzzelli, R. Schettini, M. Castelli, and L. Vanneschi, "Structural similarity index (SSIM) revisited: A data-driven approach," *Expert Syst. Appl.*, vol. 189, p. 116087, 2022.
- [31] H. N. Abdullah and H. A. Abdullah, "Colour image encryption using Nahrain chaotic map," *Int. J. Wirel. Mob. Comput.*, vol. 17, no. 2, p. 212, 2019, doi: 10.1504/ijwmc.2019.10022945.
- [32] H. Mazin, M. Alibraheemi, Q. Al-gayem, and E. A. Hussein, "Design and FPGA Implementation of High-Speed Cryptographic System for Wireless Communications Based on Multi-Dimensional Hyperchaotic Generator," vol. 20, no. 7, pp. 559–573, 2022, doi: 10.14704/nq.2022.20.7.NQ33073.
- [33] B. Abd-El-Atty, "Efficient S-box construction based on quantum-inspired quantum walks with PSO algorithm and its application to image cryptosystem," *Complex Intell. Syst.*, no. February, 2023, doi: 10.1007/s40747-023-00988-7.
- [34] A. A. Rashid and K. A. Hussein, "Image encryption algorithm based on the density and 6D logistic map," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1903–1913, 2023, doi: 10.11591/ijece.v13i2.pp1903-1913.
- [35] X. Wu, Y. Li, and J. Kurths, "A new color image encryption scheme using CML and a fractional-order chaotic system," *PLoS One*, vol. 10, no. 3, p. e0119660, 2015.

- [36] B. Stoyanov and K. Kordov, "Image encryption using Chebyshev map and rotation equation," *Entropy*, vol. 17, no. 4, pp. 2117–2139, 2015.
- [37] S. Salunke, A. K. Shrivastava, M. F. Hashmi, B. Ahuja, and N. D. Bokde, "Quad Key-Secured 3D Gauss Encryption Compression System with Lyapunov Exponent Validation for Digital Images," *Appl. Sci.*, vol. 13, no. 3, pp. 1–23, 2023, doi: 10.3390/app13031616.
- [38] R. J. Rasras, M. R. A. Sara, and Z. Alqadi, "Efficient Method to Message-Image Cryptography Using Reordered Image-Key," *Trait. du Signal*, vol. 40, no. 1, pp. 235–240, 2023, doi: 10.18280/ts.400122.
- [39] H. Wen and Y. Lin, "Cryptanalyzing an image cipher using multiple chaos and DNA operations," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, pp. 1–9, 2023, doi: 10.1016/j.jksuci.2023.101612.
- [40] H. R. Shakir, S. A. Mehdi, and A. A. Hattab, "A new four-dimensional hyper-chaotic system for image encryption," *Int. J. Electr. Comput. Eng.*, vol. 13, no. 2, pp. 1744–1756, 2023, doi: 10.11591/ijece.v13i2.pp1744-1756.
- [41] V. Patidar and G. Kaur, "A novel conservative chaos driven dynamic DNA coding for image encryption," *Front. Appl. Math. Stat.*, vol. 8, pp. 01–21, 2023, doi: 10.3389/fams.2022.1100839.
- [42] M. Majid Msallam and Fayez Aldoghan, "Multistage Encryption for Text Using Steganography and Cryptography," *J. Tech.*, vol. 5, no. 1, pp. 38–43, 2023, doi: 10.51173/jt.v5i1.1087.
- [43] X. Zhang and J. Tian, "Multiple-image encryption algorithm based on genetic central dogma," *Phys. Scr.*, vol. 97, no. July, pp. 1–23, 2022, doi: 10.1088/1402-4896/ac66a1.
- [44] B. Zhang and L. Liu, "Chaos-Based Image Encryption: Review, Application, and Challenges," *Mathematics*, vol. 11, no. 2585, pp. 1–39, 2023, doi: 10.3390/math11112585.

- [45] H. Tian, Z. Wang, P. Zhang, M. Chen, and Y. Wang, "Dynamic Analysis and Robust Control of a Chaotic System with Hidden Attractor," *Hindawi, Complex.*, vol. 2021, pp. 1–11, 2021, doi: 10.1155/2021/8865522.
- [46] D. E. Mfungo, X. Fu, Y. Xian, and X. Wang, "A Novel Image Encryption Scheme Using Chaotic Maps and Fuzzy Numbers for Secure Transmission of Information," *Appl. Sci.*, vol. 13, no. 12, pp. 1–25, 2023, doi: 10.3390/app13127113.
- [47] H. Mahalingam, T. Veeramalai, A. R. Menon, S. Subashanthini, and R. Amirtharajan, "Dual-Domain Image Encryption in Unsecure Medium—A Secure Communication Perspective," *Mathematics*, vol. 11, no. 2, pp. 1–25, 2023, doi: 10.3390/math11020457.
- [48] A. P. Kari and T. Ghomian, "An efficient image cryptosystem based on the residue number system and hybrid chaotic maps," *Res. Sq.*, pp. 0–22, 2023, doi: <https://doi.org/10.21203/rs.3.rs-3119915/v1> License:
- [49] N. Elkhailil, Y. C. Weddy, and R. Ejbalil, "Image encryption using the new two-dimensional Beta chaotic map," *Springer, Multimed. Tools Appl.*, p. 013014, 2023, doi: doi.org/10.1007/s11042-023-15105-6.
- [50] A. Dawood, Q. Thabit, and T. Fahad, "A Comprehensive Review of Color Image Encryption Technology," *Basrah J. Eng. Sci.*, vol. 23, no. 1, pp. 56–63, 2023, doi: 10.33971/bjes.23.1.8.
- [51] S. T. Allawi and N. A. A. Mustafa, "Image encryption based on combined between linear feedback shift registers and 3D chaotic maps," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 30, no. 3, pp. 1669–1677, 2023, doi: 10.11591/ijeecs.v30.i3.pp1669-1677.
- [52] W. Alexan, M. Elkandoz, M. Mashaly, E. Azab, and A. Aboshousha, "Color Image Encryption Through Chaos and KAA Map," *IEEE Access*, vol. PP, p. 1, 2023, doi: 10.1109/ACCESS.2023.3242311.
- [53] X. Wang and Y. Su, "Color image encryption based on chaotic compressed sensing and two-dimensional fractional Fourier transform," *Sci. Rep.*, vol. 10, no. 1, 2020, doi: 10.1038/s41598-020-75562-z.

- [54] M. Long and L. Tan, "A chaos-based data encryption algorithm for image/video," *2010 Int. Conf. Multimed. Inf. Technol. MMIT 2010*, vol. 1, no. 5, pp. 172–175, 2010, doi: 10.1109/MMIT.2010.27.
- [55] I. Yasser, M. A. Mohamed, A. S. Samra, and F. Khalifa, "A chaotic-based encryption/decryption framework for secure multimedia communications," *Entropy*, vol. 22, no. 11, pp. 1–23, 2020, doi: 10.3390/e22111253.
- [56] L. A. Hamood and M. K. Ibrahim, "Video Encryption Based on Chaotic System and Stream Cipher," *Iraqi J. Inf. Commun. Technol.*, vol. 1, no. 2, pp. 33–40, 2018, doi: 10.31987/ijict.1.2.19.
- [57] M. A. Fetteha, W. S. Sayed, L. A. Said, and A. G. Radwan, "Chaos-Based Image Encryption Using DNA Manipulation and a Modified Arnold Transform," (*including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics*), vol. 13761 LNAI, no. December, pp. 3–15, 2023, doi: 10.1007/978-3-031-21595-7_1.