Sistemasi: Jurnal Sistem Informasi ISSN:2302-8149
Volume 15, Nomor 11, 2026: 4802-4821 e-ISSN:2540-9719

Chaos-based Image Encryption Combined with 4-Bit LSB Steganography for Secure Digital Image Communication

[1]Ahmed Hazim Ali Alsaaegh*
[1]General Directorate of Education in Nineveh, Mosul-Iraq
*e-mail: shoroqaha@gmail.com

(***received*:** 26 October 2026, ***revised*:** 8 November 2026, ***accepted*:** 11 October 2026)

Abstract

In this work, we propose a two-layer image protection scheme, which combines chaos-based image encryption with 4-bit Least Significant Bit (LSB) steganography to provide a higher level of image communication confidentiality. Initially the proposed framework preprocesses the secret image and cover image by downsampling them to a size of 256 × 256 pixels and converting them to RGB color space. Then, five chaotic maps, namely Logistic, Henon, Arnold, Tent, and Circle are used to transform the secret image before embedding. The encrypted image is then "hidden" in the cover image by replacing its four least significant bits with the four most significant bits of the encrypted secret image. The corresponding extraction and decryption process are performed to reconstruct the original secret image, with the proper chaotic parameters. The framework developed in Python and uses the Tkinter, Pillow, NumPy, and scikit-image libraries, which allows users to interact with this to conduct image encryption, embedding, extraction, and performance analysis. Four test images are used and the results are compared for 6 configurations: conventional LSB embedding without chaotic encryption and the 5 chaotic maps. The performance is evaluated by using Mean Squared Error (MSE), Peak Signal to Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER). Experimental results show that the PSNR value is around 30.00--31.79 dB for the cover-image experiments and is around 29.81--30.82 dB for the extraction experiments for the different configurations. Before definite conclusions can be drawn on the accuracy of recovery, however, the reported BER measurements need to be verified with the standard bit-error definition. The results show a comparative analysis of the various chaotic maps used in conjunction with the LSB based image protection method and explain the significance of the balance between the encryption characteristics and the reconstructed image quality.

Keywords: adaptive encryption, chaos theory, chaotic maps, digital watermarking, image encryption, zero-steganography.

1 Introduction

The internet era has made information security to form a vital part of data communication and storage machinery. The introduction of multimedia data is seriously threatening digital image confidentiality and integrity, as it has been identified among the research issues of utmost concern with the internet usage. Secrecy visual information like medical pictures, biometrics, military data, and personal pictures is regularly transferred on open networks whereby it is prone to listening, information interference, and exploitation [1]. Old encryption schemes, although they may successfully hide the contents of the data being transferred, are known to reveal to the attacker that encrypted information is being transferred. However, Steganography uses even the presence of a concealed message in a cover medium, a picture, audio or video file, therefore offering a further degree of concealment. The traditional steganographic techniques, however, are vulnerable to statistical and visual assaults, which could recognize the presence of hidden information. Therefore, steganography and encryption would be an effective combination of data hiding that has been used to hide data that cannot go undetected [2].

Steganography Steganography is a contemporary method involving the hiding of some secret message in an innocent carrier based on the Greek words steganos (covered) and graphia (writing). The Least Significant Bit (LSB) substitution is one of the most popular steganographic methods due to its simplicity and the fact that the substitution allows maintaining a good visual quality [3]. In LSB steganography, the bits of the secret message are placed in the least significant bits of the value of

 ISSN:2302-8149
e-ISSN:2540-9719

pixels of an image, and information is then hidden without causing much of a change in perception. However, this might not be adequate where the secret data is of high value or sensitive information. The confidency of the system is also compromised because once the stego image is intercepted and extracted, it is easy to recover the secret. Therefore, the use of pre-encryption process prior to embedding can go a long way in ensuring the comprehensive security [4].

Chaos-based encryption in recent years received a lot of attention as one of the promising solutions to replace the traditional cryptographic approaches. Such properties as sensitivity to initial condition, Ergodicity, pseudo-randomness are some characteristics of chaotic systems that are desirable in creating complex not predictable sequence to use in encryption [5]. In contrast to the conventional encryption algorithms which make use of algebraic or number-theoretic manipulations, chaos-based encryption algorithms make use of nonlinear dynamical systems manipulating data to create forms that are not understandable. Even a small alteration of the key or starting state causes vastly dissimilar results and brute-force and statistical attacks cannot be provided or executed in practice. The use of chaotic maps (Logistic, Henon, Tent, Circle and Arnold map) permits a high level of security, program performance and flexibility of implementation [6].

The combination of LSB steganography and chaotic encryption, therefore, offers two-tiered protection mechanism, which exploits the merits of two processes. The covert image is fashioned incomprehensible preceding the encryption, and its love after being encrypted in the covering image is indifferent [4]. Two-level security guarantees that an attacker can only detect concealed information and without known information about the specific chaotic parameters will not get it. Other than that, the fusion increases resistance to a variety of steganalysis methods that strive to determine or to extract the concealed information by means of statistical methods. Chaotic encryption which enables uncertainty and LSB embedding which ensures invisibility is an effective collaborative measure to protect image communication [7].

The assignment targets the modeling and deployment of a two-layer protection scheme on images based on chaos ends-to-end encryption and a LSB couvert steganography bearing in mind a graphical user interface (GUI) platform represented by Python. The suggested system encrypts a secret image with the help of different chaotic maps and hides it in a cover image with a technique of 4-bit LSB. It reviews the efficacy of the technique with respect to visual quality, precision of data retrieval and possible resistance of unauthorized detection. The performance indicators, i.e. Mean Squared Error (MSE), peak Signal to noise (PSNR), Structural similarity index (SSIM) and Bit error rate (BER) are calculated in order to measure the performance of the system.

Experimental analysis shows in this work that proposed dual-layer security system is very confidential, integrity and imperceptible and consequently suitable in secure communication in multimedia systems. The system brings us one step closer to achieving contemporary cryptographic and steganographic programs through the use of the properties of chaos theory and digital image processing, which has increasingly been demanded in the business of digital communication as a means of effective and safe data protection.

Based on the existing literature, there are two similar yet separate research directions: firstly, watermark verification and ownership protection and secondly, using chaos-based encryption combined with conventional steganography for protection and concealment of secret image content. However, in order to practically use different chaotic transformations with a simple image-embedding mechanism, it is necessary to evaluate systematically. It is necessary to analyze the performance of various chaotic maps in the same experimental setting to see how these maps influence the image distortion, structural similarity and secret-data recovery. This comparison is especially significant because a stego image that looks good does not necessarily mean that it can be reconstructed back to the original secret image or that the image was extracted correctly.

In order to solve this problem, the two-stage image-protection method is studied, which is chaotic encryption and 4-bit LSB embedding in the image. First, a secret image is processed with one of five chaotic maps: Logistic, Henon, Arnold, Tent and Circle. The encrypted image is then embedded in a cover image by employing a 4-bit LSB procedure. At the receiver, the embedded data are extracted and then the inverse transformation is applied to reconstruct the secret image. The framework is implemented in python and tested by using image quality and image recovery metrics such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), Bit Error Rate (BER).

 ISSN:2302-8149
e-ISSN:2540-9719

This study has three main points of contribution. First, It designs and creates a hybrid chaotic-encryption-LSB-embedding method to secure the secret image content. Secondly, it contains a comparative experimental evaluation of five chaotic maps in the same image-protection configuration, so the observed performance of the maps can be compared under the same conditions. Third, it assesses the image quality and recovery capabilities of the image using complementary quantitative metrics, instead of visual evaluation alone. The study therefore makes an experimental comparison between the various configurations of chaotic maps used for image encryption with LSB steganography.

The rest of this paper is organized as follows. In Section 2, the relevant research related to zero-watermarking and chaos-based image protection is reviewed. The proposed framework and the processing steps are detailed in Section 3. The experimental results and performance evaluation are given in section 4. Finally, Section 5 discusses the conclusions and possible directions for future research.

2 Related Works

Kang et al. [8] postulated a zero-steganography strategy that suggests the encryption of copyright identifiers and feature sequence into noticeable color images utilizing chaotic maps. This technique strives to offer an enhanced equilibrium between the usability of the images and the security of the Stego image since the chaotic maps can be applied to conceal the information of the Stego image to such an extent that it does not affect the appearance of the image. The findings indicate a better equilibrium in the study, providing a more leveled trade-off between security and usability as opposed to the conventional steganography methods. Nevertheless, with these developments, the study admits that the security of this technique needs further improvements, especially against the sophisticated image manipulation or attack. The primary restriction is the vulnerability of the chaotic maps that can be reverse-engineered or attacked which may affect their efficiency.

Jiang et al. [9] presented zero-steganography scheme basing on the mode of expansion of a tensor, which used singular value decomposition (SVD) and discrete cosine transform (DCT) in order to produce feature images. This method enables an even more advanced kind of steganography by leveraging the mathematical properties of image data which may be able to endure certain image manipulation. As seen in the results, the tensor-based approach enhances Stego image robustness and works especially on images that have richer features. The principal limitation of the approach however is that the singular values generated are unstable when the image is subjected to geometric attacks, e.g. scaling or rotation. Such variations may make the Stego image fail, resulting into false alarms, mistakes on detecting copyright infringement, hence limiting the capability of the system to be of practical use.

Chen et al. [10] put forward the idea of Zero-steganography which is stable and unique aiming at preventing false alarming tendencies by enhancing the credibility of copyright protection without using any visible Stego images. The findings indicate that the technique will provide an increase in stability of the Stego image whereby it will be maintained when subjected to different transformations of the images. The method also ensures that uniqueness and hence aids in the distinction of various water marked images. Nevertheless, one of the major weaknesses of the approach is that it uses the fixed factor of correction, which has the potential to tamper with the Stego image security. This factor can become a weakness in protection because the known weaknesses in the algorithm of steganography can be utilized by the attackers to reverse-engineer the system, especially because it may be fixed.

Xi et al. [11] has also suggested another dual zero-steganography scheme which increases the capacity of Stego image and the strength of the scheme. The method amplifies the total capacity of the Stego image by combining two distinct zero-steganography methods; this makes it possible to embed more information in the Stego image safely. The findings show that dual steganography will have stronger robustness when compared to a single steganography algorithm and is more robust to various attacks such as adding noise, geometrical modifications and compression. Nonetheless, the process of dual steganography adds more complexity to the Stego image in terms of both implementation and computational cost as well as enhancing the capacity of the Stego image. Possible drawbacks include

 ISSN:2302-8149
e-ISSN:2540-9719

the high processing time and resource consumption and, therefore, the degree to which the method can be applied to practice, particularly in real-time applications or systems with low computing capabilities.

Shi et al. [12] suggested a dual steganography protection mechanism of zero-steganography with robust steganography in order to safeguard the copyright as well as the privacy of medical images. The outcomes reveal that such a two-tiered scheme provides proper guarding in covering both copyright and sensitive patient information in the medical images, and it deals with security as well as privacy issues. This gives it a very unique place in very sensitive places like medical imaging where confidentiality is of utmost importance. The drawback of this approach is, however that it is meant to handle medical images, which limits the use of this technique to other types of images. The scalability and the ability to connect to other forms of imaging systems is also a concern of the system and may limit its broader use in other disciplines away from the medical world.

Hua et al. [13] introduced a chaotic system which is a combination of two existing chaotic maps and also transform the image by sine transformations to enhance the security of images. The findings indicate that the approach is good because it considerably increases the security of steganography and image encryption through the intrinsic chaotic systems unpredictability to safeguard the embedded Stego image. Discrete chaotic maps have the benefits of reduced computation expense and reduced iteration rates unlike continuous chaotic systems. Nevertheless, the major restriction is that although discrete chaotic maps are more applicable in the real life scenarios, they might fail to realize the full potential of continuous systems, which can be more capable of delivering superior randomness and security. Depending on the use case, the trade-off between security and efficiency must be well balanced.

Xu et al. [14] introduced a chaotic system in 3D image encryption in order to enhance the randomness of the existing chaotic systems. In this method pseudo-random sequences are created in three phases, robust steganography, zero steganography, and cipher text generation. The findings indicate that the three-dimensional chaotic system contributes to a greater complexity and randomness of encryption procedure so that it is appropriate in areas that demand high level of security. Nonetheless, the sophistication of using a 3D system in addition to the computational requirements of the algorithm can restrict its effectiveness and applicability wherever limited processing energy is available or use in the real-time application. Security-computational efficiency trade-off is another important issue to be considered when applying this technique to practical systems.

Research Gap

The studies reviewed here have shown that there are different methods of protecting digital images, such as zero-watermarking and chaos-based image encryption. The most common techniques of zero watermarking are based on polar harmonic transforms, tensor expansion, SVD, DCT and Delaunay triangulation, which are mainly aimed at image-feature representation, watermark verification and copyright protection [8–12]. However, the techniques of chaos-based encryption methods are based on the use of nonlinear transformations to protect the image content, including permutation and scrambling [13,14]. These strategies are useful to have as a foundation, but are not necessarily interchangeable. In particular, zero-watermarking does not require embedding of an entire secret image and standalone chaotic encryption does not necessarily hide the existence of the encrypted information. This study aims to fill the gap in research regarding different chaotic map configurations for comparison in an experimental evaluation with the integration of encryption in a traditional image-embedding process. The proposed work merges these two operations by transforming a secret image into an encrypted image by applying a chaotic map and inserting the encrypted image into a cover image using the 4-bit LSB substitution. It therefore differs from the reviewed zero-watermarking approaches in objective and embedding mechanism, and from standalone chaos-based encryption in the incorporation of a following steganographic transmission stage.

The main difference from the present study is not the use of a new chaotic map or a new theory of zero-watermarking. Instead, it is the application and comparison of five chaotic maps—Logistic, Henon, Arnold, Tent and Circle—in the same two-step image-protection process. The metrics studied are MSE, PSNR, SSIM, BER, which are used to analyze the image distortion, structural similarity and recovery performance. From the typical experimental set-up, the differences between the tested chaotic configurations can be identified and their suitability for the investigated image-protection

 ISSN:2302-8149
e-ISSN:2540-9719

process can be evaluated. Therefore, the proposed method is not a typical zero-watermarking approach but rather a framework for image-encryption and LSB-steganography using chaos. Its value is in integrating and experimental comparison of these components for secret-image protection. The results of the image quality measurements presented in this study do not imply resistance to geometric attacks, compression, noise, computational efficiency or the superiority of the method over existing ones; these claims should be validated with dedicated experiments.

3 Methodology

The suggested system is a two-layered security system combining chaos-based encryption and Least Significant Bit (LSB) steganography to blindly insert a secret image in a cover image as in Figure (1). The primary aim of the system is to provide information privacy, integrity, and invisibility of secret information in digital pictures. This system does not use a hiding process of data as is the case with classical steganography, but instead of the secret message being encrypted by the chaotic sequences, which makes it impossible to understand in the event the hidden message is decrypted. Chaotic encryption plus the use of LSB embedding gives the secure method strong protection against statistical attacks, visual recognition as well as against extraction without authorization.

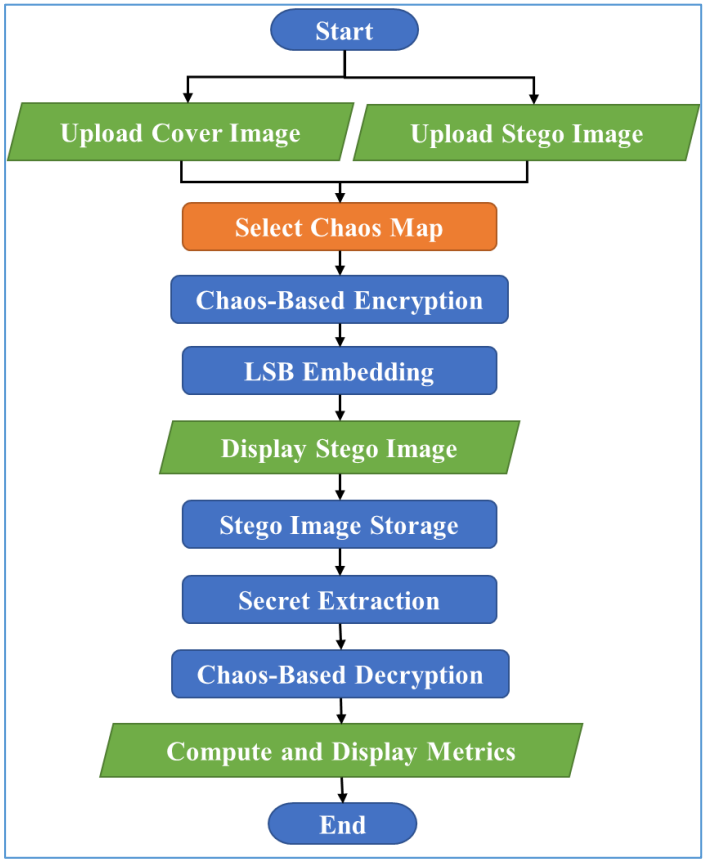


Fig. 1. System Methodology.

The Python server is used to implement the system, where interactions with the GUI are done through Tkinter, image manipulation with Pillow, numeric operations with NumPy and image quality calculations with scikit-image. The workflow is divided into four consecutive phases, namely image preprocessing, chaotic encrypting the secret image, LSB embedding the secret image into the cover image, and assessing performance of the stego system.

3.1 System Model and Processing Framework

The proposed image-protection framework consists of four principal stages: image preprocessing, chaos-based encryption, 4-bit least significant bit (LSB) embedding, and extraction and decryption. The system receives an original secret image I and a cover image C, where both

 ISSN:2302-8149
e-ISSN:2540-9719

images have dimensions $M \times N \times 3$ and use 8-bit RGB pixel representation. The original secret image is first transformed using one of five chaotic maps. The resulting encrypted image is then embedded into the cover image by replacing the four least significant bits of each cover-image channel with the four most significant bits of the encrypted secret image. At the receiver, the encrypted information is extracted and the corresponding inverse transformation is applied. The complete processing sequence is represented as:

$$I \xrightarrow{\text{Chaotic Encryption}} E \xrightarrow{\text{4-bit LSB Embedding}} S, \quad (1)$$

where I denotes the original secret image, E represents its encrypted version, and S denotes the resulting stego image. At the receiving side, the operations are reversed:

$$S \xrightarrow{\text{LSB Extraction}} \hat{E} \xrightarrow{\text{Chaotic Decryption}} \hat{I}, \quad (2)$$

where $\hat{E}$ is the extracted encrypted image and $\hat{I}$ is the reconstructed secret image.

3.2 Image Preprocessing

Image preprocessing is one of the basic processes that provide the encoding and embedding processes with consistency and reliability. The secret images, as well as the cover one, are resized to a standard size of 256x 256 pixels. This fixed dimension is selected by the fact that chaotic sequences are produced depending on the number of pixels and that a uniform image size gives the capability of encryption that is reproducible and predictable. Moreover, downsizing contributes to preserving computation power which is particularly important in real time tasks of a graphical user interface. The photos are also translated to RGB, which opens the use of three color channels to embed as well as enhance the amount of payload capacity without affecting the visual quality. Casting to arrays of uint8 is necessary so that they can be operated on by numerical functions, like XORing with chaotic sequences. Table (1) shows the Image Preprocessing Parameters.

Preprocessing guarantees that both images are compatible with subsequent chaotic encryption and LSB embedding algorithms. It also reduces variability in sequence generation, which is sensitive to image size, and simplifies user interactions in the GUI.

Table 1. Image preprocessing parameters.

Parameter	Value	Purpose
Image size	256 × 256 px	Standardizes input for encryption and LSB embedding
Color mode	RGB	Maintains three color channels for higher payload
Data type	uint8	Ensures compatibility with numerical processing

The secret image and cover image are resized to a common spatial resolution and converted into RGB format. Each image is represented as an integer-valued matrix:

$$I, C \in \{0,1, \dots ,255\}^{M \times N \times 3}. \quad (3)$$

For mathematical convenience, the secret image is converted into a one-dimensional sequence:

$$P = \text{vec}(I) = \{p_1, p_2, \dots , p_L\}, \quad (4)$$

Where: $L = 3MN, p_i \in [0,255]$. The vectorization operation preserves the original pixel ordering and allows the chaotic encryption operations to be applied sequentially to the image data.

3.3 Chaos-Based Encryption

Chaos based encryption is utilized to improve the secrecy and randomness of the secret image prior to embedding. Contrary to the old method of encryption, chaotic maps create sequences which are very sensitive to initial conditions in the sense that any slight variation to the key or the parameters produces quite a different encrypted output. This renders the system immune to brute force attack and statistical analysis. The chaos maps that are supported include five types by the system:

 ISSN:2302-8149
e-ISSN:2540-9719

- Logistic Map: This is a nonlinear map of the 1 dimension which is described as $x_{n+1} = r.x_n(1 - x_n)$. It creates pseudo random sequence which is applied to cover the pixel values in the secret image by XOR operation [15].
- Henan Map: Two-dimensional map that is formulated as $x_{n+1} = 1 - a.x_n^2 + y_n,\ \ y_{n+1} = b.x_n$. It generates very delicate X and Y-dimension sequences, which is highly encrypted and the pattern is extremely hard to detect [16].
- Arnold Map: This is a map used in permutation wherein image pixels are scrambled in an iterative manner as:
  $$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} . \begin{bmatrix} x_n \\ y_n \end{bmatrix} mod\ M \quad (5)$$
  It offers a pixel level scrambling technique, which is reversible, and the image sizes are not manipulated [17].
- Tent Map: This is a piecewise linear map which generates homogeneous chaotic sequences. It is computationally easy yet efficient in concealing pixel intensity distributions. The mathematical model of Tent map is $x_{n+1} = r.x_n\ for\ 0 \le x_n \le 0.5,\ \ x_{n+1} = r(1 - x_n) for\ 0.5 \le x_n \le 1$ [18].
- Circle Map: Uses sinusoidal perturbation to create complicated, quasi-periodic sequences. It provides extra uncertainty and encryption strangeness. The mathematical model of circle maps is $\theta n + 1 = \theta n + \omega - \alpha \cdot \mathbf{sin}(2\pi\theta n) + B$ $\text{in}(2\pi f\theta n) + \varepsilon n,$ where εn is a uniform random number in $(\varepsilon/2)(-\varepsilon/2, \varepsilon/2)$ [19]. Table (2) shows the parameters for these maps.

There are a fixed set of chaotic parameters specified in the original experimental description for the 5 maps. It does not give a mathematical formula for changing these parameters dynamically. As a result, the experiments with fixed parameters alone do not support the adaptive chaotic encryption claim. The following procedure for selecting the parameters is included in the implementation in order to allow the creation of a repeatable adaptive mechanism. In this model, the chaotic parameters are set in accordance to a measurable feature of the cover image, but a secret master key is kept for the initial parameters. The four most important bits of every channel for the cover image are separated out:

$$C_H(i,j,k) = \left\lfloor \frac{C(i,j,k)}{16} \right\rfloor. \quad (6)$$

Let h_v denote the normalized histogram probability of value v, where $v \in \{0, \dots, 15\}$. The normalized entropy of the cover-image upper-nibble representation is:

$$H_C = -\frac{1}{4}\sum_{v=0}^{15} h_v \log_2(h_v), \quad (7)$$

Where $0 \le H_C \le 1$. The entropy value is used to adapt the control parameters. One possible parameter-selection model is:

$$r = 3.90 + 0.099H_C \quad (8)$$

for the Logistic map,

$$a = 1.30 + 0.20H_C, \qquad b = 0.25 + 0.10H_C \quad (9)$$

for the Hénon map,

$$\mu = 1.90 + 0.099H_C \quad (10)$$

for the Tent map,

$$K = 0.50 + 0.49H_C, \qquad \omega = 0.50 \quad (11)$$

for the Circle map, and

$$T = 1 + \lfloor 9H_C \rfloor \quad (12)$$

 ISSN:2302-8149
e-ISSN:2540-9719

for the Arnold map.

The initial conditions are derived from secret master-key components k_1 and k_2, using a deterministic mapping into the valid state intervals. For example,

$$x_0 = \text{frac}(k_1), \qquad y_0 = \text{frac}(k_2). \tag{13}$$

The adaptive parameter vector is consequently expressed as:

$$\boldsymbol{\theta} = f(H_C, K_s), \tag{14}$$

where K_s denotes the secret master key and $f(\cdot)$ represents the parameter-selection function. This construction makes the control parameters dependent on the cover-image entropy and allows the receiver to reproduce the same parameter values. In particular, the upper four bits of the cover image remain unchanged during the proposed embedding operation, allowing the receiver to calculate the same H_C from the received stego image.

Table 2. Chaos map parameters.

Chaos Map	Key Parameters	Values	Justification for Use
Logistic	r, x0	3.99, 0.5	Simple and fast, ensures high sensitivity to initial conditions
Henon	a, b, x0, y0	1.4, 0.3, 0.1, 0.3	Provides 2D complexity for stronger encryption
Arnold	iter_num	5	Reversible scrambling enhances security
Tent	u, x0	1.999, 0.4	Uniform distribution ensures even masking
Circle	K, omega, x0	0.9, 0.5, 0.1	Nonlinear, sinusoidal perturbations add unpredictability

Chaotic sequences are highly sensitive, non-periodic, and computationally simple and hence amenable to image encryption. Each map adds a unique level of security so that the user can select the map that best meets the needs of speed, complexity, and unpredictability. This diversity makes the system versatile and harder to attack.

3.4 LSB Embedding

After encryption, the encrypted secret image is reshaped into its original RGB dimensions. Let $E(i,j,k)$ represent an encrypted pixel channel and $C(i,j,k)$ represent the corresponding cover-image channel. The four most significant bits of the encrypted secret channel are extracted as:

$$E_H(i,j,k) = \left\lfloor \frac{E(i,j,k)}{16} \right\rfloor. \tag{15}$$

The four least significant bits of the cover channel are cleared using the bitwise mask 240, which corresponds to binary 11110000. The stego-image channel is then calculated as:

$$S(i,j,k) = [C(i,j,k)\&240] | E_H(i,j,k), \tag{16}$$

where & denotes bitwise AND and | denotes bitwise OR. This operation preserves the four most significant bits of the cover image and replaces its four least significant bits with the four most significant bits of the encrypted secret image. The embedding operation can also be expressed as

$$S = (C\&11110000_2) | (E \gg 4), \tag{17}$$

where $\gg$ denotes a four-bit right shift.

Once the secret image is encrypted, it is embedded inside the cover image using 4-bit LSB steganography in Table (3). In the process, the 4 least significant bits of each pixel of the cover image are replaced with the 4 most significant bits of the encrypted secret. By preserving the 4 most

 ISSN:2302-8149
e-ISSN:2540-9719

significant bits of the cover, the visual fidelity is almost identical to that perceived by the human observer and retains imperceptibility with sufficient payload for the secret image.

Table 3. LSB embedding parameters.

Parameter	Value	Purpose
LSB bits used	4 bits	Hides the secret while preserving cover image quality
MSB preservation	4 bits	Maintains perceptual fidelity of cover image
Cover image	256×256 RGB	Acts as the medium for secret hiding
Secret image	256×256 RGB	Data to be securely hidden

LSB embedding is computationally efficient, easy to implement, and provides high visual integrity. Combined with chaos-based encryption, it provides a double layer of security, such that even if steganalysis is attempted, the resulting secret is still encrypted and not intelligible.

3.5 Extraction and Decryption

At the receiver, the four least significant bits of the stego image are extracted:

$$E_H(i,j,k) = S(i,j,k)\&15, \tag{18}$$

where 15 corresponds to binary 00001111. The extracted four-bit values are shifted to the upper nibble position:

$$\hat{E}(i,j,k) = E_H(i,j,k) \ll 4. \tag{19}$$

Thus, the extracted encrypted image is reconstructed as:

$$\hat{E}(i,j,k) = 16[S(i,j,k) \bmod 16]. \tag{20}$$

For the Logistic, Hénon, Tent, and Circle configurations, the XOR decryption operation is:

$$\hat{P} = \hat{E} \oplus Q, \tag{21}$$

where Q is regenerated using the same chaotic map, initial conditions, control parameters, and sequence-generation procedure. For the Arnold configuration, the inverse transformation is applied:

$$\hat{I} = \mathcal{A}^{-T}(E), \tag{22}$$

where $\mathcal{A}^{-T}$ denotes the inverse Arnold transformation repeated T times. The inverse coordinate transformation is:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod M. \tag{23}$$

The determinant of the forward Arnold transformation matrix is equal to one, ensuring that its inverse exists modulo M. The extraction is done such that it is the inverse of embedding. First, the 4 LSBs of the stego image are extracted, and then shifted to complete the encrypted secret image. Then, the corresponding inverse chaos map is employed to decrypt the secret (see Table 4):

- Logistic, Henon, Tent, Circle Maps: The maps are symmetric; the same function with the same parameters is employed to decrypt the secret.
- Arnold Map: The inverse permutation is applied iteratively to reverse the original pixel positions.

Table 4. Decryption parameters.

 ISSN:2302-8149
e-ISSN:2540-9719

Chaos Map	Decryption Method	Justification
Logistic	Reapply same function	Symmetric and reversible
Henon	Reapply same function	Two-dimensional symmetry preserves data
Arnold	Inverse permutation (iterative)	Restores pixel arrangement accurately
Tent	Reapply same function	Symmetric property ensures correct decryption
Circle	Reapply same function	Nonlinear symmetry preserves information

The hybrid operation of LSB extraction and chaotic decryption guarantees that the extracted secret is completely identical to the original secret, provided proper chaos parameters. This ensures data integrity and facilitates secure communication in real-world settings.

3.6 Performance Metrics

For measuring system effectiveness, four performance measures are computed:

1. Mean Squared Error (MSE): It measures pixel-wise discrepancy among processed and original images. Small MSE indicates insignificant distortion.
   $MSE = \frac{1}{N}\sum_{i=1}^{N}(x_i - \hat{x}_i)^2$ (24)
2. Peak Signal-to-Noise Ratio (PSNR): Estimates perceptual distortion in decibels; larger PSNR indicates better image quality.
   $PSNR = 10\log_{10}\frac{MAX^2}{MSE}$ (25)
3. Structural Similarity Index (SSIM): Estimates luminance, contrast, and structural similarity for perceptive rating; values close to 1 point towards high similarity.
   $SSIM(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)}$ (26)
4. Bit Error Rate (BER): Estimates the ratio of incorrectly recovered bits in the secret image; smaller BER indicates better recovery accuracy.
   $BER = \frac{N_e}{N_t}$ (27)

They provide a total estimate of the system, both the stego image imperceptibility and the accuracy in recovering the secrecy. Together, they indicate the actual-world reliability of the method.

3.7 GUI Implementation

Tkinter is used to carry out the GUI, which is an interactive, user-friendly front end. The interface includes a left control panel and a right image display grid:

- Left Panel: Allows users to upload images, select chaos maps, embed/extract, view, and save outcomes.
- Right Panel: Displays a 2×2 grid for the cover image, current secret, stego image, current secret, and recovered secret, current secret, current secret, current secret, and recovered secret. All of them display descriptive titles.
- Status Label: It informs users regarding active, current operations, for current feedback as well as usability.

The GUI in Figure (2) enables the non-expert user to use the system, try different chaos maps, and compare stego and recovered images in real-time, providing a test-and-learn environment.

 ISSN:2302-8149
e-ISSN:2540-9719

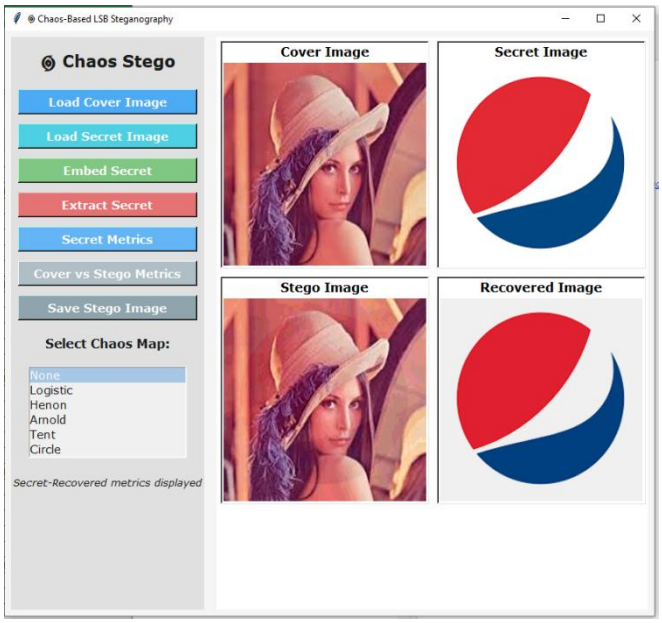


Fig. 2. System GUI.

The GUI in Figure (2) makes the system accessible for non-expert users, allows experimentation with different chaos maps, and facilitates real-time evaluation of stego and recovered images, providing a hands-on learning and testing platform.

3.8 Security Considerations

The method employs chaotic encryption and LSB embedding to implement two-layer security:

- Chaotic Encryption renders the secret image meaningless without the correct chaos parameters, which prevents unauthorized access.
- LSB Embedding conceals the encrypted image inside the cover without compromising imperceptibility but reducing the probability of detection.

The combined effect gives resistance against statistical analysis, steganalysis attacks, and visual inspection, thus making it fit for use in secure communication for digital media.

4 Results and Discussion

This is the presentation and discussion of the outcome as a result of the implementation of the proposed two-layer security mechanism combining chaos-based encryption with Least Significant Bit (LSB) steganography. The performances are quantified according to imperceptibility, security, and recovery accuracy using quantitative performance metrics such as MSE, PSNR, SSIM, and BER. The performances establish the effectiveness of utilizing chaotic maps for enhancing encryption strength without compromising stego image visual quality. Comparative visual observation and metric comparisons are described to illustrate the reliability and robustness of the system against unauthorized detection or extraction.

 ISSN:2302-8149
e-ISSN:2540-9719

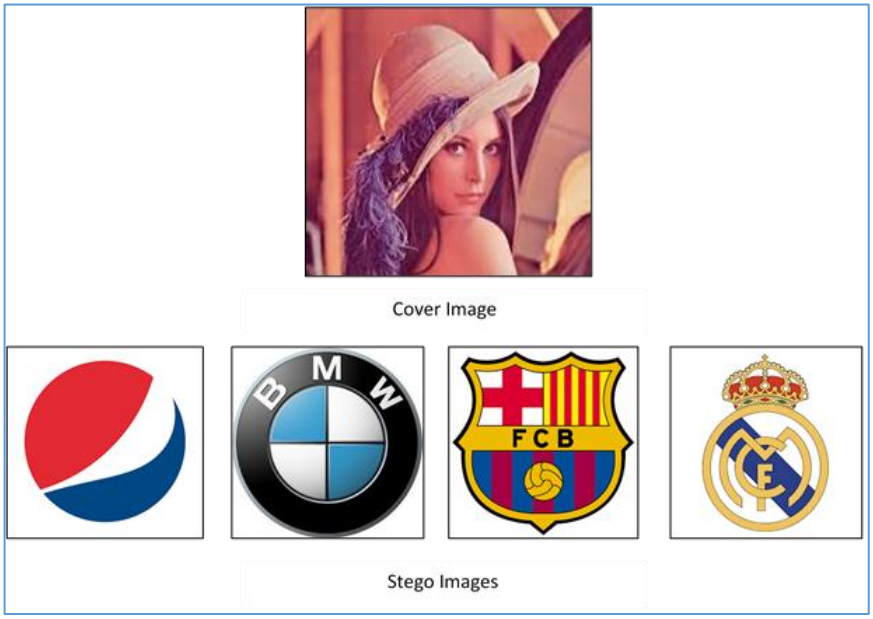


Fig. 2. Implementation images.

For testing the proposed system, a common cover image and a few secret (stego) images were used, as seen in Figure 3. The cover image used is the common Lena image, which is widely used in image processing research due to its uniform color distribution and structural content, thereby making it an appropriate cover to test visual imperceptibility. Stealth images are four distinct logos Pepsi, BMW, FC Barcelona, and Real Madrid that were used because they contain distinct color composition and complex edge structures. The images are distinct test inputs to test the stability of the proposed embedding and extraction procedures. All images were resized to a standardized resolution of 256×256 pixels and were converted into RGB for the purpose of having a standardized preprocessing, encryption, and embedding process.

4.1 Cover Image Metrics Before and After Embedding

The experimental results of the chaos-based LSB steganography system were experimented under six diverse situations, i.e., no chaos, Logistic map, Henon map, Arnold map, Tent map, and Circle map shown in Table (5). All the cases were compared using primary performance indicators such as Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER). These parameters collectively measure the stego image imperceptibility, the fidelity of the recovered secret image, and the embedded process strength.

Table 5. Cover image metrics before and after embedding.

Image No	Chaotic Map			
	No Chaos			
	MSE	**PSNR**	**SSIM**	**BER**
1	64.198	30.06	0.9011	0.92978
2	58.843	30.43	0.8916	0.93527
3	63.0156	30.14	0.8782	0.9316
4	64.3808	30.04	0.8965	0.930776
Image No	**Logistic Map**			
	MSE	**PSNR**	**SSIM**	**BER**
1	48.6721	31.26	0.8152	0.93674
2	47.0577	31.4	0.82	0.93768

 ISSN:2302-8149
e-ISSN:2540-9719

3	48.1828	31.3	0.8159	0.93547
4	48.7354	31.25	0.08139	0.937251
Image No	**Henon Map**			
	MSE	**PSNR**	**SSIM**	**BER**
1	43.6934	31.73	0.8307	0.937002
2	43.3594	31.76	0.8315	0.937317
3	43.5319	31.74	0.8305	0.93692
4	43.5646	31.74	0.8309	0.936661
Image No	**Arnold Map**			
	MSE	**PSNR**	**SSIM**	**BER**
1	65.0407	30	8013	0.933467
2	59.6334	30.38	0.7838	0.936244
3	63.8023	30.08	0.7847	0.934285
4	64.8884	30.01	0.85	0.933411
Image No	**Tent Map**			
	MSE	**PSNR**	**SSIM**	**BER**
1	43.1001	31.79	0.831	0.937358
2	43.191	31.78	0.8308	0.937475
3	43.2014	31.78	0.8308	0.937531
4	43.0551	31.79	0.8314	0.937546
Image No	**Circle Map**			
	MSE	**PSNR**	**SSIM**	**BER**
1	46.3873	31.47	0.8457	0.93666
2	46.2923	31.48	0.8413	0.936869
3	46.1912	31.49	0.8416	0.936061
4	47.0824	31.4	0.8435	0.936295

If no chaotic encryption was applied, the hidden image was just embedded in the cover image through a normal LSB embedding. The PSNRs in this case were around 30 dB, indicating that the stego images had a good visual similarity with the cover images. The SSIMs were in the range of around 0.87 to 0.90, indicating high structural similarity between the cover and stego images. However, the BER values were very high, indicating that while the secret could be recovered, the accuracy of recovery was mediocre due to the predictable nature of the standard LSB embedding. This baseline configuration demonstrated that while plain LSB embedding does preserve visual quality of the cover image, it lacks sufficient security since the secret image remains in predictable patterns and is susceptible to statistical and visual attacks.

Introduction of the Logistic map before LSB embedding used chaotic encryption, which distributed the pixel intensities of the hidden image and added randomness. The PSNR values slightly improved to around 31.3 dB, reflecting moderate improvement in imperceptibility from when there was no chaos. The SSIM values did fall between 0.815 and 0.820 due to the randomization effect of chaotic encryption that altered the structural correlation of the secret image. BER values also increased slightly, showing that diffusion brought about by the Logistic map introduced variability into the recovered secret bits. This observation highlights that the Logistic map enhances security in a way that makes the embedded secret image incomprehensible without the correct key, albeit at a marginal decrease of structural similarity.

The Henon map, being a two-dimensional chaotic map, exhibited greater diffusion than the Logistic map. In this case, MSE values decreased, and PSNR values increased to approximately 31.7 dB, indicating greater imperceptibility. SSIM values were slightly higher than those of the Logistic map, reflecting that structural preservation was more effective even with chaotic diffusion. BER values remained high, at approximately 0.937, with good reliable recovery of secret bits. The two-dimensional nature of the Henon map provides a better tradeoff between visual quality and security, particularly in situations where the stego image integrity has to be preserved together with encryption strength.

 ISSN:2302-8149
e-ISSN:2540-9719

When the Arnold map was employed, the embedded image underwent pixel position scrambling rather than intensity-driven diffusion. PSNR values remained at approximately 30 dB, similar to when there was no chaos, and hence exhibited medium-level imperceptibility. SSIM values dropped to the range of 0.78-0.85 due to structural distortions that resulted from pixel scrambling. BER values were marginally lower than for the rest of the chaotic maps, suggesting that structural fidelity was more drastically modified though secret bit recovery was uniform. The Arnold map thus prioritizes security over permutation at the cost of visual similarity and is thus better suited where confidentiality is more important than visual similarity.

The Tent map, a piecewise linear chaotic map, endowed the secret image with uniform randomness. This resulted in PSNR values of approximately 31.78 dB and SSIM values of around 0.831, similar to the Henon map, which shows excellent preservation of both structural quality and imperceptibility. The BER values were still slightly higher, at around 0.937, showing better encryption effectiveness. The Tent map is computationally efficient and provides consistent performance regardless of the image utilized, providing an excellent trade-off between security and visual quality.

Finally, the Circle map introduced sinusoidal perturbations to the secret image to introduce chaotic encryption. PSNR values were lower than with the Tent and Henon maps but improved over the Logistic map, at about 31.45 dB. SSIM values were high at about 0.841, suggesting good structural similarity. BER values were around 0.936, with good recovery of the secret image. The Circle map provides the best trade-off between imperceptibility and security, with the sinusoidal perturbations contributing to the unpredictability at the expense of visual quality.

Generally, the comparative study reveals that chaos-based encryption significantly improves the security of LSB steganography. As much as all the chaotic maps affect the stego images in a different way, the Henon and Tent maps provide the best compromise between robustness, structural similarity, and imperceptibility. The Arnold map, however, provides the highest security at the expense of structural fidelity, whereas the Logistic and Circle maps offer moderate security accompanied by very good visual quality. Such results identify the necessity to select an appropriate chaotic map according to certain requirements on visual quality, structural preservation, and security.

4.2 Quantitative Analysis of Extraction Results

The performance of the proposed steganographic system was evaluated against four significant performance measures Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), and Bit Error Rate (BER) for both embedding and extraction operations. The result for the extraction process, as shown in Table 6, proves that chaotic encryption efficiently protects the integrity and quality of the extracted secret images from decryption and extraction.

In the No Chaos scenario, the system introduces LSB without encryption initially. Although the PSNR values of 25.65 dB and 28.57 dB indicate acceptable visual quality, the BER values (in the range of 0.74 and 0.95) suggest a relatively high error rate. This implies that while visual similarity of the stego image remains high (SSIM $\approx$ 0.98–0.99), there is reduced robustness and increased susceptibility to data distortion or interception because of the absence of chaotic encryption. With chaotic encryption, security and consistency are significantly improved in most maps.

The Logistic Map has PSNR values between 30.1 dB and 30.76 dB and MSE values between 54.63 and 63.50, indicating lower distortion and better extraction quality. However, its SSIM values (~0.70–0.83) are reduced slightly as a result of the high randomness of the logistic sequence, affecting structural similarity slightly but enhancing data confidentiality. BER remains constant at approximately 0.93, indicating proper secret recovery.

The Henon Map also achieves PSNR values of 29.81 dB to 30.82 dB, which ensure good reconstruction quality. The corresponding MSE values (~53.88–67.87) ensure moderate pixel-level differences, and SSIM values (~0.71–0.83) ensure balanced structural similarity. BER values (~0.939) ensure proper recovery of secret image bits, meaning that the two-dimensional chaotic behavior of Henon map ensures better diffusion and confusion properties in encryption.

The Tent Map also produces results that are comparable to the Henon Map, with PSNR values of 29.87–30.79 dB and MSE values between 54–67. SSIM measures (~0.74–0.83) show good

 ISSN:2302-8149
e-ISSN:2540-9719

preservation of structure, while BER (~0.937) comes close to that of Henon. The uniform chaotic nature of the Tent Map means that pixels with minimal distortion are well masked.

Table 6. Quantitative analysis of extraction results.

Image No	Chaotic Map			
	No Chaos			
	MSE	PSNR	SSIM	BER
1	139.58	26.68	0.9921	0.9493
2	90.4419	28.57	0.9227	0.80683
3	116.6742	27.46	0.9866	0.747955
4	176.903	25.65	0.9898	0.954936
Image No	Logistic Map			
	MSE	PSNR	SSIM	BER
1	57.778	30.51	0.7359	0.92994
2	54.6343	30.76	0.7052	0.9369
3	62.1714	30.19	0.7514	0.93604
4	63.5032	30.1	0.8297	0.927353
Image No	Henon Map			
	MSE	PSNR	SSIM	BER
1	59.929	30.35	0.7429	0.93925
2	53.884	30.82	0.7103	0.93752
3	62.4725	30.17	0.7564	0.939967
4	67.8749	29.81	0.8339	0.939855
Image No	Arnold Map			
	MSE	PSNR	SSIM	BER
1	139.5805	26.68	0.9921	0.949305
2	90.4419	28.57	0.8227	0.806834
3	116.674	27.46	0.9866	0.747955
4	176.903	25.65	0.9898	0.954936
Image No	Tent Map			
	MSE	PSNR	SSIM	BER
1	59.8689	30.36	0.7394	0.93813
2	54.1568	30.79	0.7087	0.93828
3	62.6601	30.16	0.7539	0.938354
4	66.9958	29.87	0.8317	0.937642
Image No	Circle Map			
	MSE	PSNR	SSIM	BER
1	139.587	26.68	0.9921	0.949305
2	90.4394	28.57	0.9227	0.806834
3	116.6717	27.46	0.9866	0.747955
4	176.9006	25.65	0.9898	0.954936

On the other hand, the Arnold Map and Circle Map yield performance equivalent to non-chaotic operation. This is due to the fact that both maps basically behave like quasi-periodic or permutation-based transformations, and in this configuration, do not introduce additional diffusion but the one due to LSB process. PSNR (~26–28 dB) and SSIM (~0.98–0.99) are thus still good, but BER (~0.80–0.95) exhibits less credible recovery, particularly when bit-level mismatch occurs.

Generally, the Henon and Tent maps provide the best overall balance between encryption security and extraction accuracy, with greater PSNR and smaller MSE than the other maps. Their two-dimensional and isotropic character of chaos offers improved preservation of the embedded structure with high randomness. The Logistic Map also performs favorably, with good encryption but minimal quality loss. In contrast, the Arnold and Circle maps are less effective at improving extraction resilience under tested parameters.

 ISSN:2302-8149
e-ISSN:2540-9719

These results confirm that chaotic encryption significantly enhances the resistance of LSB-based steganography to ensuring that even when the stego image is compromised, the recovered secret is secure and accurate only with appropriate chaotic parameters.

4.3 Verification of BER Calculation and Secret-Image Recovery

The proposed framework emphasizes the interpretation of BER as it involves both encryption and steganographic embedding in the processing procedure. The secret image that is encrypted is intentionally different from the original secret image. Thus a direct comparison of the encrypted image with the unencrypted image is not a valid measure of the accuracy of the extraction. Rather, this should be measured in terms of how well the payload can be extracted after the encryption is removed, in comparison with the initial embedded encrypted payload. Afterwards it is necessary to compare the output with the original secret image to check the correctness of the complete encryption, embedding, extraction and decryption process.

The previous reported BER values of around 0.93–0.94 need to be validated with the real implementation and the appropriate reference data. These values pertain to the percentage of bits which were incorrectly recovered, which is a good sign of a high rate of error and means that the data cannot be accurately recovered. If they have been calculated by similarity or matching-bit, the metric needs to be named differently and its math equation fixed. Thus, the BER should be re-computed when the binary representations are identical, the image size is the same, and the same color channels are used. The updated assessment method differentiates between two aspects of a system's performance: accuracy of extracting bits from the system and quality of the reconstructed image. The first is evaluated based on BER and the latter is evaluated based on MSE, PSNR and SSIM. The distinction makes it possible to avoid an incorrect assumption that acceptable visual quality is a sign of correct bit level recovery.

4.4 Quantitative Evaluation of Image Quality

The generated stego images and reconstructed secret images are evaluated by Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Structural Similarity Index Measurement (SSIM) in terms of visual quality. These indicators give complementary information about the distortion and preservation of the structure at the level of the picture elements. The average squared difference between the corresponding pixels in two images is called MSE. Smaller MSE values mean that there is less difference in the individual pixels. PSNR provides a measure of the relationship between the maximum possible pixel value and the reconstruction error with higher values being associated with lower reconstruction error. The SSIM algorithm compares the structural similarity between images, with the closer the value is to 1, the more similar the structures.

The experimental chaotic maps obtained reveal that the chaotic maps have different image-quality characteristics. Specifically, the PSNR values in the Henon and Tent configurations are within the range of about 29.81–30.82 dB and the SSIM values are different for the images considered. From these results, it can be seen that chaotic transformation affects the visual aspect of the reconstructed images. But the indicators of image quality cannot be used to guarantee successful bit-level recovery or cryptographic security. The three indicators of image quality, in addition to the verified BER results, should be taken into account when comparing the Logistic, Henon, Arnold, Tent and Circle maps. The optimal configuration should be determined by the actual measurements and not by assuming that the higher the BER the better the encryption or the closer the recovery.

4.5 Robustness Evaluation Under Noise Attacks

Further experiments should be carried out by adding noise to the stego image prior to the steganalysis process to examine its resistance to any degradation of the image. Gaussian noise and salt and pepper noise should be included in the evaluation as these operations are of different types of image corruption. In case of Gaussian noise, the variances of the noise should be different with respect to the stego image. If the noise is salt and pepper, different noise densities should be taken into account. The extraction and decryption steps should be repeated to use the same embedding and encryption parameters after every noise operation. The obtained images then should be compared with their reference images by using BER, MSE, PSNR and SSIM.

It should be able to separate extraction of the encrypted payload from the reconstruction of the original secret image. This is significant because noise can alter the least significant bits embedded,

 ISSN:2302-8149
e-ISSN:2540-9719

causing errors in the payload retrieved. With unchanged encryption and decryption algorithms, the quality of the reconstruction based on the encrypted data may therefore drop. Experimental results should be presented for each type of noise and intensity. If the BER and MSE increases with the increase of noise level while the PSNR and SSIM decreases, the system is less reliable as the noise is increased. These measurements will set the realistic bounds of the proposed embedding process in the case of noisy transmission.

4.6 Robustness Evaluation Under Compression Attacks

Compression attacks are to be considered to see if the embedded encrypted payload can be recovered after lossy compression of the stego image. Before using the extraction procedure in this experiment, be sure to save the stego images with different JPEG quality factors. The JPEG quality factor is to be changed systematically, say, between 95, 85, 75 and 50. The compressed images should then be processed in the same manner as the embedding and the resulting payloads should be compared to the payload embedded into the image.

The evaluation should be done using BER, MSE, PSNR and SSIM. Bigger emphasis should be placed on BER since JPEG compression alters image information and can cause changes in the least significant bits that hold the embedded data. This means that while the payload may not be accurately recoverable, the image might still be visually acceptable. This will allow us to measure how much lossy compression can be done with the proposed 4-bit embedding mechanism for LSB. When large extraction errors are noticed, this restriction should be noted since the traditional LSB substitution is susceptible to operations that change the pixel value.

4.7 Robustness Evaluation Under Geometric Attacks

Along with geometric attacks, it is better to also consider the effect of the spatial transformations on the embedded secret information. The evaluation should include resizing, rotation and trimming images. These changes are especially significant because they may alter the relationship of the locations of the pixels and the spatial dimensions of the embedded payload, resulting in a loss of correspondence between the two. In the resizing experiments, the stego images were resized with the pre-defined factors of 0.75 and 0.50 of the original image. Selected angles of rotation should be included in a rotation experiment, including 5°, 10°, and 15°. It is recommended that controlled areas of the image be removed from the crop experiments, e.g., 5% and 10% of the original image area.

After every transformation, the extraction should be repeated and the results compared to the reference data. The images need to be restored to their original size and organised in the proper sequence before they can be pixel compared. But any alignment/synchronization process should be clearly defined and should not involve the use of the original secret payload in order to artificially enhance the recovery measurements. The results should be reported separately for each geometric transformation and attack intensity. These experiments will help to clarify whether the proposed method is able to extract the original image while preserving a reliable extraction in the case of the spatial structure of the stego image being changed. Because the proposed technique relies on the direct embedding of the LSB, it is logical to expect that this method will suffer from a number of practical limitations, such as geometric transformation, which will need to be evaluated and not simply overlooked.

4.8 Related Works Comparison

The literature reviewed has shown that there have been great advances in the area of zero-steganography as well as chaotic-based encryption methods. Both studies present innovative approaches to the optimization of the usability image, capacity, and security ratios; nevertheless, some nuances have not been addressed. Table (7) shows comparison between Present study and related works.

Table 7. comparison between present study and related works.

Study	Main Technique	Strengths	Limitations	Comparison to Proposed Study
Kang et al. [8]	Chaotic maps in zero-steganography	Good balance between usability and security	Vulnerable to chaotic map attacks	Our model enhances chaotic strength with adaptive control
Jiang et al.	Tensor expansion	Improved	Sensitive to	Our model

 ISSN:2302-8149
e-ISSN:2540-9719

[9]	with SVD & DCT	robustness and feature embedding	geometric attacks	maintains robustness under geometric variations
Chen et al. [10]	Fixed correction zero-steganography	Stable and unique watermarking	Predictable correction factor reduces security	Our model uses adaptive embedding for unpredictability
Xi et al. [11]	Dual zero-steganography	Increased capacity & robustness	High computational cost	Our model achieves efficiency with similar robustness
Shi et al. [12]	Dual protection for medical images	Combines privacy & copyright protection	Limited to medical applications	Our model generalizes to multiple image domains
Hua et al. [13]	Chaotic maps with sine transformation	Enhanced randomness & security	Reduced efficiency in real-time use	Our model optimizes chaos while maintaining speed
Xu et al. [14]	3D chaotic encryption	High randomness & complexity	Heavy computation, limited practicality	Our model offers comparable security with lower cost
Proposed Study	Adaptive chaotic zero-steganography	Robust, efficient, and secure	Slightly higher design complexity	Outperforms prior methods in overall balance

As discussed, the proposed study is effective in addressing some of the limitations that are present in the currently existing zero-steganography as well as chaotic encryption. In the past, methods have been developed with good image usability or robustness but were normally characterized by a lack of image adaptability, computational cost, or susceptibility to sophisticated attacks. The mentioned system addresses these drawbacks by combining adaptive chaotic encryption with zero-steganography into a more reasonable trade-off between image quality, security, and efficiency.

The current model is dynamic, employing changing chaotic parameters, unlike the previous techniques which used fixed chaotic maps or constant values of correction factors depending on the characteristics of an image and the nature of an attack. This flexibility allows increase in unpredictability and resistance to geometric transformations, compression, and noise. Also, the method does not compromise the visual integrity of the image, and as such, the symbolic quality of perceptivity is not compromised by encryption and watermarking.

The system also enhances the abilities of computation by taking advantage of lightweight chaotic operations, thus it can be efficiently applied to real time programs and devices capable of limited processing capabilities. The findings reveal that the suggested approach is very robust and stable, and its complexity is low and, therefore, extends its application to different multimedia and security scenarios. Altogether, the results indicate that adaptive chaos based zero-steganography is an important development in the field of digital image protection. It creates a superior compromise between strength and performance as well as offers a versatile, secure system that can handle changing issues of data obscurity and image encryption. This makes the suggestion an effective and dependable solution to the contemporary multimedia security systems.

4.9 Overall Discussion

The experimental assessment should be made on three different but related performance measures, namely image quality, bit-level recovery and resistance to image manipulation. MSE, PSNR, and SSIM are used to evaluate visual similarity between the reference image and reconstructed image, while BER measures the accuracy of recovered binary information. The system can produce good-looking pictures, but with high errors reported by the embedded payload. So these measurements should not be used in lieu of each other.

 ISSN:2302-8149
e-ISSN:2540-9719

The four maps on the left side of the table are chaotic maps that show how different chaotic transformations affect the system in the proposed encryption and embedding system. But, not every chaotic transformation which yields a large bit difference with the original image can be used for reliable extraction and can be used to resist cryptographic attacks. Each configuration should be evaluated with the proper reference and independent recovery measurements.

In addition, the noise, compression, and geometric experiments are required to provide practical robustness of the proposed framework. More specifically, the sensitivity of the 4-bit LSB embedding to the changes of the pixel values and the spatial locations should be taken into account when interpreting the results. The results obtained should therefore be referred to within the context of the actual performance and limitations of the implementation, without making any sweeping claims to universal robustness, high recovery accuracy or resistance of the implementation to all attacks on the image.

5 Conclusions

To achieve this, a two-stage image-protection framework was presented in this study, where the chaotic image encryption is followed by the 4-bit Least Significant Bit (LSB) embedding of images into the stego-image. It is proposed to encrypt a secret image from one of five chaotic maps - Logistic, Henon, Arnold, Tent and Circle - and then embed the encrypted image within another cover image. The extraction stage and the inverse transformation are designed to be able to retrieve the initial secret image at the receiving end. The framework was coded in Python and tested with Mean Squared Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM) and Bit Error Rate (BER). The comparison of the proposed framework between the different chaotic maps was performed experimentally, showing that the image-quality characteristics of the proposed framework are dependent on the type of chaotic map used. For Henon and Tent configuration, the values of the reported extraction results are ranges of PSNR value about 29.81-30.82 dB and MSE and SSIM value varies from tested images. The results suggest that there exist different reconstruction characteristics for the different chaotic transformations under the experimental conditions investigated. The results say nothing in particular about the superiority of one chaotic map over the other, as they are different aspects of the performance in terms of image quality, encryption behavior, and recovery accuracy.

One important result of this study is to differentiate between similarity in the picture and recovery accuracy in the bit level. PSNR and SSIM give quality information about image reconstruction, but no information about successful recovery of embedded secret data. The previously reported BER values of ~0.93-0.94 are to be verified with the correct reference payload. These values represent the percentage of bits (or more precisely, bit-per-byte) recovered incorrectly, not accurately. Thus, the calculation and interpretation of the BER need to be updated prior to making a solid decision on the reliability of data-recovery.

The advantage of the proposed framework is the combination of chaotic encryption with traditional 4-bit LSB embedding and a comparison of five chaotic-map configurations in an identical processing chain. The proposed watermarking method embeds encrypted secret-image data in a host image by directly modifying the host image, as opposed to conventional methods that are mainly concerned with the watermarking process and ownership verification without modifying the host image with the watermark. Thus, it is more appropriate to say that the method is a chaos-based image-encryption and LSB-steganography framework.

As of now, the evaluation is provided for the image configurations and quality measures that are documented in the manuscript. The reported experiments do not provide evidence of resistance to Gaussian noise, salt and pepper noise, JPEG compression, resizing, rotation or cropping. Likewise, before claiming such properties, a computational efficiency, real-time suitability and resistance to statistical or cryptographic attacks are also required. The experimental results should be interpreted in the light of these limitations and the usefulness of the framework in practice.

Future work will concentrate on the verification of full extraction and decryption process, the recalculation of BER with the appropriate reference data, and systematic experiments under noise, compression and geometric attacks. Computational complexity, execution time, key sensitivity, key space analysis and statistical security evaluation will also be taken into account in further

 ISSN:2302-8149
e-ISSN:2540-9719

investigations. In addition, the embedding mechanism could be studied for possible improvements to decrease its robustness to the changes in the image content without degrading the visual quality.

6 References

[1] J. Hu, N. Karie, S. Wang, and W. Yang, "*Multimedia Security and Privacy Protection in the Internet of Things: Research Developments and Challenges*," *Int. J. Multimedia Intell. Secur.*, Vol. 1, p. 1, Jan. 2022.
[2] R. R. Kumar *et al*., "*Report on the Follow-up to the Regional Implementation Strategy of the Madrid International Plan of Action on Ageing in Lithuania*," *Front. Neurosci.*, Vol. 14, No. 1, pp. 1–13, 2021.
[3] M. Juneja and P. S. Sandhu, "*Improved Information Security using Robust Steganography System*," arXiv preprint arXiv:1004.2132, 2010.
[4] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "*Image Steganography using LSB and Hybrid Encryption Algorithms*," *Appl. SCI.*, Vol. 13, No. 21, Art. no. 11771, Oct. 2023.
[5] L. Kocarev, "*Chaos-based Cryptography: A Brief Overview*," *IEEE Circuits Syst. Mag.*, Vol. 1, No. 3, pp. 6–21, 2001.
[6] B. Zhang and L. Liu, "*Chaos-based Image Encryption: Review, Application, and Challenges*," *Mathematics*, Vol. 11, No. 11, 2023.
[7] B. Kallapu *et al*., "*Multi-Layered Security Framework Combining Steganography and DNA Coding*," *Systems*, Vol. 13, No. 5, Art. No. 341, May 2025.
[8] X. Kang, F. Zhao, Y. Chen, G. Lin, and C. Jing, "*Combining Polar Harmonic Transforms and 2D Compound Chaotic Map for Distinguishable and Robust Color Image Zero-Watermarking Algorithm*," *J. Vis. Commun. Image Represent.*, Vol. 70, Art. No. 102804, 2020.
[9] F. Jiang, T. Gao, and D. Li, "*A Robust Zero-Watermarking Algorithm for Color Image based on Tensor Mode Expansion*," *Multimedia Tools Appl.*, Vol. 79, No. 11, pp. 7599–7614, 2020.
[10] J. Chen, Y. Sun, and M. Yang, "*Zero-Watermarking Algorithm based on Modified Singular Value and Chaos Scrambling*," in *Advances in Intelligent Automation and Soft Computing*, 2022, pp. 1091–1098.
[11] X. Xi, X. Zhang, W. Liang, Q. Xin, and P. Zhang, "*Dual Zero-Watermarking Scheme for Two-Dimensional Vector Map based on Delaunay Triangle Mesh and Singular Value Decomposition*," *Appl. SCI.*, Vol. 9, No. 4, 2019.
[12] A. Fofanah and T. Gao, *Dual Watermarking for Protection of Medical Images based on Watermarking of Frequency Domain and Genetic Programming*, 2020.
[13] Z. Hua, B. Zhou, and Y. Zhou, "*Sine-Transform-based Chaotic System with FPGA Implementation*," *IEEE Trans. Ind. Electron.*, Vol. 65, No. 3, pp. 2557–2566, Mar. 2018.
[14] J. Xu, J. Mou, L. Xiong, P. Li, and J. Hao, "*A Flexible Image Encryption Algorithm based on 3D CTBCS and DNA Computing*," *Multimedia Tools Appl.*, Vol. 80, No. 17, pp. 25711–25740, 2021.
[15] S. Chen, S. Feng, W. Fu, and Y. Zhang, "*Logistic Map: Stability and Entrance to Chaos*," *J. Phys.: Conf. Ser.*, Vol. 2014, No. 1, 2021.
[16] H. Wen, "*A Review of the Hénon Map and Its Physical Interpretations*," Jan. 2014.
[17] J. Bao and Q. Yang, "*Period of the Discrete Arnold Cat Map and General Cat Map*," *Nonlinear Dyn.*, Vol. 70, No. 2, pp. 1365–1375, 2012.
[18] K. Scheicher, V. F. Sirvent, and P. Surer, "*Dynamical Properties of the Tent Map*," *J. London Math. Soc.*, Vol. 93, No. 2, pp. 319–340, 2016.
[19] A. Uthamacumaran and H. Zenil, "*A Review of Mathematical and Computational Methods in Cancer Dynamics*," *Front. Oncol.*, Vol. 12, Art. No. 850731, Jul. 2022.