ELECTRICAL ENGINEERING AND ENERGY

OPEN ACCESS

Secure Audio Steganography using Vectorized LSB and Chaos-Based Encryption

Zeynel Ümit Korkmaz, Fahrettin Horasan, and Zeynep Çetinkaya

Dept. of Computer Engineering, Kırıkkale University, Kırıkkale, Türkiye

Submitted: 26 September 2025
Accepted: 27 October 2025
Online First: 31 October 2025

Corresponding author
Fahrettin Horasan,
fhorasan@kku.edu.tr

DOI:10.64470/elene.2025

Abstract: In the era of digital transformation, the protection of sensitive multimedia data against growing cyber threats has become increasingly critical. Traditional cryptographic and steganographic techniques, while effective individually, often fall short when faced with advanced detection and attack methods, making hybrid security approaches a necessity. In this study, a hybrid security approach combining chaotic algorithms and the Least Significant Bit (LSB) embedding method is proposed. The method is enhanced through key-dependent parameter assignment, as well as additional steps such as transient periods and square matrix transformation. Furthermore, vectorization after square matrix transformation simplified indexing in embedding and extraction steps, thereby improving computational efficiency. As a result, high security and integrity were achieved for both visual and audio data. In the encryption process, seven different chaotic structures (Logistic Map, Lorenz System, Piecewise Linear Chaotic Map, Tent Map, Hénon Map, Chua Circuit, Chebyshev Map) were supported, and the method was tested on these algorithms. The original content was encrypted using XOR and then embedded into the audio signal via the LSB method. The proposed method was evaluated using the EBU SQAM audio dataset and standard test images with Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), Mean Squared Error (MSE), Structural Similarity Index Measure (SSIM), and Bit Error Rate (BER) metrics. Experimental results demonstrated that for all tests, the extracted images achieved Visual_PSNR = ∞, Visual_SSIM = 1, and Visual_BER = 0. For audio data, PSNR values ranged between 102–107 dB and SNR values approximately 53–99 dB depending on the content type. These findings reveal that the proposed method ensures both the integrity of the content and the reliable preservation of the hidden data.

Keywords: Audio Stenography, Chaotic Algorithms, Data Security, Hybrid Encryption, LSB Data Hiding

1. Introduction

In today's digital era, the rapid pace of digitalization creates both new opportunities and significant challenges in the field of data security. The storage of personal and sensitive information in digital environments has become increasingly vulnerable to growing cyber threats. Therefore, digital data must be protected not only against unauthorized access but, in some cases, also through concealing the very existence of the data itself. For critical digital assets such as medical images, financial documents, written reports, or security records, such protection techniques play a vital role (Emin et al, 2024; Stallings, 2020; Pfleeger, Pfleeger, & Margulies, 2015; Katzenbeisser & Petitcolas, 2000; Balasubramanian et al., 2024).

Two fundamental approaches are commonly employed to ensure data security: cryptography and steganography. Cryptography protects data by rendering its content unintelligible to unauthorized parties, while steganography aims to completely conceal the existence of the data. However, steganography alone often fails to provide sufficient protection, as hidden information can still be detected using advanced statistical and spectral analysis techniques (Horasan et al, 2022; Katzenbeisser & Petitcolas, 2000). As a result, integrated security models that combine cryptography and steganography have gained increasing importance, offering stronger solutions to emerging security demands. Encrypting data with cryptographic methods and embedding it into digital media using steganography provides both content confidentiality and existence concealment, thereby creating a multilayered security model. Such approaches extend beyond conventional methods and enable the development of systems that are more resilient to attacks (Nasr et al., 2024; Khalil et al., 2024; Balasubramanian et al., 2024).

In recent years, the use of chaotic systems in hybrid security structures has attracted significant attention. Although chaotic systems are deterministic, they exhibit extreme sensitivity to initial conditions, which enables them to generate unpredictable pseudo-random sequences. This property makes chaotic systems powerful candidates for cryptographic applications (Alvarez & Li, 2006; Chen et al., 2004). In the literature, the number of encryption and embedding frameworks employing chaotic systems has been steadily increasing, yet the overall performance of these frameworks largely depends on the randomness quality of the generated sequences.

In this study, a hybrid security scheme that combines cryptography and steganography is proposed. The method consists of two main stages. In the first stage, input data are encrypted using pseudo-random sequences generated by chaotic systems through XOR-based operations. In the second stage, the encrypted data are embedded into a digital audio signal using the LSB method. This design ensures not only the confidentiality of the content but also the concealment of its existence. Moreover, the proposed system is reinforced with additional mechanisms, including key-dependent parameter assignment, transient (warm-up) periods, square matrix transformation, and vectorization, to improve both robustness and efficiency.

For key generation, seven different chaotic systems were employed: Logistic Map (May, 1976), Lorenz System (Lorenz, 1963), PWLCM (Chen, Tang, & Yi, 2020), Tent Map (Alligood, Sauer, & Yorke, 1996), Hénon Map (Hénon, 1976), Chua Circuit (Matsumoto, 1987), and Chebyshev Map (Strogatz, 2014). Each of these systems was independently configured to produce pseudo-random sequences according to the length of the input data and was utilized as a key generator in the encryption stage.

The remainder of this paper is structured as follows. First, related works addressing the combined use of cryptography and steganography are reviewed. Next, the theoretical foundations of the proposed method, along with the algorithms and evaluation metrics, are presented. The subsequent section introduces the system architecture and experimental results, followed by a discussion of the findings and a conclusion highlighting the contributions of this work.

2. Related Works

In the literature, there are studies that can be classified according to the domain where the data hiding is performed (spatial or transform) and the structure of the security layer. Spatial domain (time domain) methods aim to hide data by directly modifying the sample values of the carrier signal. The most basic and common technique in this category is the LSB substitution method (Alwahbani & Elshoush, 2018a). The popularity of LSB stems from its ease of implementation and its ability to offer high data embedding capacity (Abood et al., 2022).

In contrast, transform domain (frequency domain) approaches embed data into frequency components obtained through mathematical transformations such as the Discrete Wavelet Transform (DWT) or the Discrete Cosine Transform (DCT). These methods generally offer higher robustness against signal processing attacks, such as compression, but they also **entail** higher computational complexity. The choice between these two approaches depends on the application's goal: LSB is ideal for pure steganography where imperceptibility is the priority, while DWT/DCT are more suitable for digital watermarking, where the goal is for the message to survive manipulations (Katzenbeisser & Petitcolas, 2000). Beyond these general approaches, the use of chaotic structures has also become widespread, particularly in the fields of cryptography and steganography, with the aim of enhancing security and randomness.

Chaotic systems have long been employed in the fields of cryptography and steganography for various purposes. In image encryption applications, pseudo-random sequences generated through chaos maps sensitive to initial conditions have often been used to perform pixel permutation or substitution. For instance, Khanzadi et al. (2014) adopted this approach by employing Logistic and Tent maps for image encryption; however, their work focused solely on content security and did not address data confidentiality in a layered manner. Similarly, Li (2024) proposed a hyperchaotic structure to overcome the limitations of classical chaos maps and evaluated randomness performance using NPCR and UACI metrics. Nevertheless, this method remained limited to encryption and did not incorporate embedding into an external carrier. Kiran and Parameshachari (2022) developed a selective encryption method targeting regions of interest in medical images and employed Arnold's Cat Map and the Duffing system to balance efficiency with security. Yet, this approach also emphasized content protection rather than integrating layered confidentiality.

Approaches primarily concerned with concealing data rather than encrypting content have typically been found in steganography-based studies. Khalil et al. (2024) introduced an LSB-based hiding method using 2D chaos maps and optimization techniques, but without a cryptographic encryption layer. In their work, imperceptibility, carrier capacity, and PSNR were emphasized, while content security was secondary. Abd et al. (2025) combined chaotic encryption with LSB embedding of both image and audio data into a color image carrier. However, in this case, audio data were treated solely as content rather than as the carrier medium.

Among works combining encryption and steganography, Nasr et al. (2024) encrypted images using Henon, Baker, and Arnold maps and embedded them into audio signals by means of an ISTFT-based approach. While the use of an audio carrier distinguished this study, frequency-domain processing introduced significant computational complexity. Alternatively, You et al. (2025) proposed a selective and layered security model in a face-detection-based framework, where only facial regions were encrypted using Logistic and PWLCM maps. Although this method did not employ an audio carrier, its lightweight and region-specific design was noteworthy.

A review of the literature reveals that chaotic systems have typically been applied either for encryption or for hiding purposes alone, with relatively few studies combining both aspects into hybrid frameworks. The method proposed in this study aims to address this gap by simultaneously ensuring content security and data confidentiality through a multilayered approach. The core design integrates XOR-based encryption with LSB-based embedding. This hybrid structure is further reinforced with key-dependent parameter assignment, transient (warm-up) periods, and square matrix transformation. Additionally, seven distinct chaotic systems were employed to generate pseudo-random keys for encryption, and the encrypted data were embedded directly into digital audio signals in the time domain. By avoiding frequency-domain operations, the proposed system achieves both high security and computational efficiency, while the comparative evaluation of randomness performance across the chaotic systems provides a complementary contribution to existing studies.

3. Theoretical Background

This section introduces the fundamental components used in the study. First, the XOR operation employed for content encryption is explained. Then, the LSB technique applied in the data hiding process is discussed. Finally, the mathematical foundations of the chaotic algorithms used for pseudo-random key generation are summarized.

3.1 XOR Encryption

XOR (Exclusive OR) encryption is one of the simplest and fastest methods among symmetric cryptographic techniques. When the data bit and the key bit are identical, the result is 0; otherwise, it is 1. The same operation can be used for both encryption and decryption (Stallings, 2020).

$$C_i = P_i \oplus K_i, \quad P_i = C_i \oplus K_i \qquad (1)$$

Here, Pi denotes the plaintext bit, Ki the key bit, and Ci the ciphertext bit sequence. The self-inverse property of the XOR operation provides a strong security layer, especially when combined with keys generated from chaotic systems.

3.2 LSB Data Hiding

The LSB method is a message embedding technique based on modifying the least significant bits of the carrier data. Since such changes are imperceptible to the human eye, the method provides high hiding capacity and low detectability (Katzenbeisser & Petitcolas, 2000).

$$S' = (S \ \& \ \sim 1) \ | \ M \qquad (2)$$

Here, S is the original sample, M the message bit, and S' the embedded sample.

3.3 Chaotic Systems and Pseudo-Random Key Generation

Chaotic systems, although deterministic in nature, exhibit extreme sensitivity to initial conditions and therefore generate unpredictable sequences (Alvarez & Li, 2006). This property makes them highly suitable for pseudo-random key generation in cryptographic applications. The seven chaotic structures used in this study are summarized below.

3.3.1 Logistic Map

The Logistic map is a one-dimensional chaotic system originally developed to model population dynamics (May, 1976). Despite its simplicity, it produces highly complex and unpredictable sequences for certain parameter values. Here, x_n, denotes the state of the system at the nth iteration, r is the growth rate, and x_0 is the initial condition. The range of rrr between 3.57 and 4 corresponds to fully chaotic behavior.

$$x_{n+1} = r\,x_n(1 - x_n), \quad r \in [3.57,4],\ x_0 \in (0,1) \qquad (3)$$

3.3.2 Lorenz System

The Lorenz system was derived from a simplified three-dimensional model of atmospheric convection (Lorenz, 1963). Here, x,y,z denote the system variables; σ is the Prandtl number, ϱ the Rayleigh number, and β a geometric factor. Controlled by these parameters, the system exhibits chaotic dynamics due to its extreme sensitivity to initial conditions. In cryptography, it is widely used for secure key generation.

$$\frac{dx}{dt} = \sigma\,(y - x),$$

$$\frac{dy}{dt} = x\,(\rho\ -\ z) -\ y\ ,$$
$$\frac{dz}{dt} = xy\ -\ \beta\, z \tag{4}$$

3.3.3 PWLCM (Piecewise Linear Chaotic Map)

The Piecewise Linear Chaotic Map is defined in the unit interval and consists of linear segments. Here, x_n denotes the system state at the n-th iteration, and the parameter p determines the breakpoints. Its mathematical simplicity and unpredictability make it suitable for high-speed pseudo-random number generation, particularly for XOR-based encryption keys (Chen et al., 2020).

$$x_{n+1} = \begin{cases} \frac{x_n}{p}, & 0 \le x_n < p \\ \frac{1-x_n}{1-p}, & p \le x_n \le 1 \end{cases} \quad 0 < p < 1 \tag{5}$$

3.3.4 Tent Map

The Tent map is characterized by its simple triangular iterative structure (Alligood et al., 1996). Here, x_n denotes the system state at the nnn-th iteration, and μ is the control parameter. Depending on μ the system exhibits chaotic behavior within certain ranges. Its lightweight design ensures high performance in both software and hardware implementations, while its sensitivity to initial conditions makes it suitable for cryptographic key generation.

$$x_{n+1} = \begin{cases} \mu\, x_n, & 0 \le x_n < \frac{1}{2} \\ \mu\,(1 - x_n), & \frac{1}{2} \le x_n \le 1 \end{cases} \quad 0 < \mu \le 2 \tag{6}$$

3.3.5 Henon Map

The Hénon map is one of the most studied two-dimensional chaotic systems (Hénon, 1976). Here, x_n and y_n represent the system states at the n-th iteration, while a and b are parameters that govern the chaotic behavior. Its complex dynamics enable the generation of high-entropy pseudo-random sequences, making it a popular choice for chaos-based encryption applications.

$$\begin{cases} x_{n+1} = 1 - a\, x_n^2 + y_n \\ y_{n+1} = b\, x_n \end{cases} \tag{7}$$

3.3.6 Chua Circuit

The Chua circuit is one of the first physical electronic circuits to exhibit chaotic behavior (Matsumoto, 1987). Controlled by parameters α and β, it includes a nonlinear resistance function $f(x)$. At certain parameter values, the system produces multidimensional chaotic dynamics, providing significant advantages in cryptographic key generation.

$$\frac{dx}{dt} = \alpha\,[\,y - x - f(x)\,],$$
$$\frac{dy}{dt} = x - y + z,$$
$$\frac{dz}{dt} = -\beta\, y$$
$$f(x) = m_1\, x + \frac{1}{2}(m_0 - m_1)(|x+1| - |x-1|) \tag{8}$$

3.3.7 Chebshev Map

The Chebyshev map is based on orthogonal polynomials and exhibits strong chaotic properties (Strogatz, 2014). It is defined by the following iterative relation:

$$x_{k+1} = \cos!(n \arccos(x_k)) \quad ; \quad n \geq 2 \tag{9}$$

Here, n denotes the degree of the map and $x_k$the state at the k-th iteration. Although nnn is typically an integer in the classical definition, the system exhibits chaotic behavior in specific ranges. Its ease of computation and strong chaotic features make it suitable for pseudo-random key generation in cryptographic applications.

4. Evaluation Metrics

4.1 Peak Signal-to-Noise Ratio (PSNR)

PSNR is a metric that measures the difference between the reference audio and the processed or data-embedded audio. The calculation is based on the Mean Squared Error (MSE) value and expressed on a logarithmic scale in decibels (dB). The formula is defined as follows:

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

Here, MAX_I represents the maximum possible value of the signal, and MSE denotes the mean squared error between the two signals. A higher PSNR value indicates smaller differences between the signals and therefore higher quality. Due to its simplicity and ease of comparison, PSNR is widely used in the literature. However, it may not fully reflect perceptual quality on its own (Gonzalez and Woods 2018; Hore and Ziou 2010).

4.2 Signal-to-Noise Ratio (SNR)

SNR, measures how much the processed signal has degraded compared to the original signal (Oppenheim and Schafer 2010). In the context of audio signals, the SNR value is calculated as the ratio of the energy of the original signal to the energy of the error signal (the difference between the original and the processed signal), expressed in decibels (dB):

$$\text{SNR} = 10 \cdot \log_{10}\left(\frac{\sum_n s[n]^2}{\sum_n (s[n]-\tilde{s}[n])^2}\right) \tag{11}$$

Where: s[n]: Original audio signal, $\tilde{s}[n]$: Processed (stego) audio signal, Numerator: Total power of the original signal (Signal Power), Denominator: Error power between the two signals (Noise Power). A higher SNR value indicates that the processed signal is closer to the original, meaning better perceptual quality.

4.3 Mean Squared Error (MSE)

MSE measures the average squared difference between a reference media signal and a processed one. This media signal may be audio, image, video, or other digital data. The difference may arise from embedding, extraction, or other processing methods. A smaller MSE value indicates higher similarity and less distortion. The PSNR metric is derived from MSE (Gonzalez and Woods 2018).

$$\text{MSE}(x, y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - y_i)^2 \tag{12}$$

Here: n: Number of compared samples, x_i: The i-th sample of the reference (original) media data, y_i: The i-th sample of the processed media data.

4.4 Structural Similarity Index Measure (SSIM)

SSIM, evaluates perceptual similarity between two media signals by considering luminance, contrast, and structural components together. SSIM values range between [0, 1], where values close to 1 indicate high similarity, and values close to 0 indicate low similarity (Wang et al. 2004). Compared to metrics such as PSNR or MSE, which rely solely on numerical error magnitudes, SSIM provides a more accurate assessment of perceptual quality.

$$\mathrm{SSIM}(x, y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \tag{13}$$

Where: μ_x, μ_y → Mean values, σ_x^2, σ_y^2 → Variances, σ_{xy} → Covariance, C_1, C_2 → Stability constants

4.5 Bit Error Rate (BER)

BER, measures the proportion of transmitted or embedded bits that are incorrectly decoded. A BER value of 0 represents maximum accuracy. It directly evaluates the success of the steganography and encryption chain, providing insight into the reliability of the extracted content (Proakis and Salehi 2007). BER is widely used in assessing error rates in embedding-extraction processes.

$$\mathrm{BER} = \frac{1}{n}\sum_{i=1}^{n}\left(b_i \oplus \widehat{b_i}\right) \tag{14}$$

Here: b_i: Transmitted/embedded bit, $\widehat{b_i}$: Received/extracted bit, $\oplus$: XOR operation (1 if different, 0 if identical), n: Total number of bits.

5. Materials and Methods

In this section, the characteristics of the audio and image data used in the study are first explained. Then, the implementation details of the basic hybrid structure (XOR encryption + LSB data hiding) are presented. In practice, this basic hybrid structure is enhanced with additional steps such as key-dependent parameter assignment, transient (warm-up) period, and square matrix transformation. The encryption–hiding process and the extraction–decryption process are described alongside the relevant algorithms.

5.1 Data Set

5.1.1 Audio Data

The audio files used in this study were obtained from the EBU Sound Quality Assessment Material (SQAM) dataset, which provides standardized references for audio quality evaluation. To ensure diversity in the experimental setup, four distinct categories were selected, covering a range of acoustic characteristics from simple tonal signals to complex speech patterns. Table 1 presents the selected audio categories along with their descriptions, formats, and durations.

5.1.2 Visual Data

The images used in this study are grayscale with a resolution of 256×256 pixels. To provide a standardized and diverse evaluation basis, three widely used benchmark test images were selected. These images exhibit different visual characteristics such as texture complexity, tonal variations, and edge clarity. Table 2 summarizes the visual dataset along with their formats, dimensions, and distinctive features.

Table 1. Selected audio categories from the SQAM dataset

Category	Description	Format	Duration
Tonal	Sine Wave 1 kHz (Mono)	WAV, 16-bit PCM	1:42
Noise	Band-limited pink noise (Stereo)	WAV, 16-bit PCM	0:49
Melodic Instrument	Harpsichord (arpegio/melodious phrase (Stereo)	WAV, 16-bit PCM	0:53
Speech	Female Speech (English, Mono)	WAV, 16-bit PCM	0:23

Table 2. Visual dataset and their characteristics

Image	Image Name	Format	Dimension	Distinctive Feature
	Baboon	PNG	256×256 (8-bit grayscale)	High-textured details
	Pepper	PNG	256×256 (8-bit grayscale)	Mixed tones and edges
	Cameraman	PNG	256×256 (8-bit grayscale)	Clear contours, low contrast

5.1.3 Test Combinations

Seven different chaotic number generator algorithms were tested in combination with four audio categories and three different images. Using these combinations, a total of 84 experiments (7×4×3) were conducted.

5.2 Chaotic System and Key Generation

In all chaotic algorithms employed in this study, the parameters were determined using a method derived from the ASCII values of the user key. For practical stability, the ASCII sum is calculated based only on the first 10 characters of the key, and if the sum exceeds 4000, it is fixed at 4000. This total value (**S**) is then used through modular and division operations to generate three fractional numbers within the range of 0–1 as follows:

$$u = \frac{S \bmod 1000}{1000}, \quad v = \frac{\lfloor S/3 \rfloor \bmod 1000}{1000}, \quad w = \frac{\lfloor S/7 \rfloor \bmod 1000}{1000} \tag{15}$$

These variables are scaled to the respective parameter ranges of each chaotic algorithm. In this way, the same key consistently produces the same parameter set, while different keys yield entirely distinct structures.

A transient (warm-up) period is also applied in all chaotic algorithms. Transients are used to eliminate the influence of initial conditions and numerical errors during the early iterations. For this purpose, the total number of iterations is defined as L+T, where L is the required keystream length and T is an integer value in the range of 100–1000 derived from the user key. The first T iterations are discarded, and the subsequent L iterations are scaled to the range [0,255] to serve as the XOR encryption keystream.

This technique reduces initial correlations, thereby producing a keystream with higher entropy and unpredictability. In the literature, Li, Mou, and Cai (2001) recommended discarding a sufficient number of initial iterations to improve randomness by excluding the first m steps. In this study, the transient period was dynamically determined based on the user key and optimized within the range of 100–1000, enhancing both the randomness and security level of the method.

5.2.1 Key Generation with Logistic Map

The Logistic map is a one-dimensional chaotic system originally developed to model population dynamics. In this study, the growth parameter r is selected from the range [3.57, 4.0], while the initial value x_0 is derived from the interval (0.05–0.95). The transient length T is determined within the range of 100–1000 iterations based on the ASCII sum of the key. The total number of iterations is defined as $L+T$, and after discarding the first T iterations, the remaining sequence is scaled to the range [0,255]. The resulting byte sequence is used as the XOR encryption key.

5.2.2 Key Generation with Tent Map

The Tent map is characterized by its triangular iterative structure. The slope parameter r is chosen from the range [1.6, 2.0], with the initial value x_0 set within the range (0.05–0.95). The transient length T is defined in the range of 100–1000, derived from the key. After discarding the transient iterations, the generated values in [0,1] are linearly mapped into the byte range [0,255] and used as the XOR key.

5.2.3 Key Generation with PWLCM

The Piecewise Linear Chaotic Map (PWLCM) consists of two linear segments defined over the unit interval. The breakpoint p is selected from the range [0.2, 0.5], and the initial condition x_0 from the range (0.001–0.999), both derived from the key. If x_0 is too close to p, a shift is applied to avoid dynamic degradation. The transient period T is chosen between 100 and 1000, after which the resulting sequence is normalized into [0,255] to serve as the XOR key.

5.2.4 Key Generation with Hénon Map

The Hénon map is a two-dimensional chaotic system known for producing high-entropy sequences. Parameters a and b are derived from the key within the ranges [1.3, 1.5] and [0.25, 0.35], respectively, while the initial conditions (x_0, y_0) are selected from (0.05–0.45). The transient length T is chosen between 100 and 1000 iterations. After discarding transients, the fractional parts of x and y are combined with weighted sums and scaled into [0,255] to generate the XOR key.

5.2.5 Key Generation with Lorenz System

The Lorenz system is a three-dimensional set of chaotic differential equations. The parameters are derived from the key with ranges $\sigma \in [8, 12]$, $\varrho \in [22, 38]$, and $\beta \in [2.4, 3.0]$. The initial state (x_0, y_0, z_0) is set approximately within (0.1–0.3, 0.8–1.2, 0.8–1.2). After the transient period, the Lorenz equations are numerically solved using the Euler method, and the combined x, y, and z values are scaled to [0,255] to construct the XOR key.

5.2.6 Key Generation with Chua's Circuit

Chua's circuit is a three-variable electronic system incorporating a nonlinear resistor element. The parameters $\alpha \in [12, 16]$, $\beta \in [24, 32]$, $m_0 \in [-1.20, -1.05]$, and $m_1 \in [-0.80, -0.60]$ are derived from the key, along with the initial state. After discarding the transient iterations, the x, y, and z values are combined through weighted summation and normalized into [0,255] to form the XOR key.

5.2.7 Key Generation with Chebyshev Map

In the Chebyshev map, the degree *n* is selected from the range 2–5, while the initial condition x_0 is derived from (–0.95, 0.95). The transient length *T* is determined within 100–1000 iterations based on the key. After discarding the transient values, the resulting sequence in [–1,1] is linearly mapped to the range [0,255] and used in XOR encryption.

5.3 Encryption and Data Hiding Process

From the selected chaotic algorithm, a key-dependent byte sequence (keystream) is generated. This keystream is then used to encrypt the image data through the XOR operation. The resulting encrypted data are bit-sliced and embedded into the LSB of the audio signal. To optimize performance, square matrix transformation and NumPy-based vectorization are employed, which accelerate bit manipulation operations and facilitate efficient capacity management.

```
Algorithm 1: Encrypt and Embed (Image → Audio LSB)

Input: Cover audioA, secret image I, user key K, chaotic map M
Output: Stego audio A' and composite key K'

1. Load the image: Open I; if necessary, convert its mode to RGB or grayscale (L). Record the dimensions W, H and format/color information.
2. Convert image to bytes: Transform I into a uint8 array; to preserve data integrity, convert the bytes into text format using Latin-1 encoding.
3. Derive key parameters: Compute the ASCII sum from K (application-specific deterministic derivation method).
4. Generate chaotic keystream: Initialize map M (e.g., Logistic, Tent, PWLCM, Hénon, Lorenz, Chua, Chebyshev) with parameters from Step 3; discard transient iterations; generate a keystream of length equal to the image byte sequence, scaled into [0,255].
5. XOR encryption: $C = I \oplus keystream$. where $\oplus$ is bitwise XOR.
6. Load the audio: Read the cover audio A and flatten the samples into a 1D sequence.
7. Square matrix embedding: Place the 1D sequence of length $L_A$ into the smallest n×nn \times nn×n square with zero padding; record the original length.
8. Bit expansion: Unpack bytes of C into individual bits; determine total length L.
9. Capacity check: Verify if : $n2 \geq L$. If not satisfied, terminate with error.
10. Select embedding indices: Choose sequential indices (0, 1, 2, …, L−1) for LSB embedding.
11. LSB embedding: Replace selected bits: $sample \leftarrow (sample\& \sim 1) \mid bit$
12. Reconstruction: Flatten the square matrix back to 1D, restore the original channel/dtype format, and obtain the stego audio A'.
13. Generate composite key: $K' =$ ASCII_sum$(K)$ % algo_id % $L$ % image % format@color@W@H
14. Save outputs: Store the stego audio A' and return the composite key K'.
```

The steps of **Algorithm 1** are summarized in **Figure 1**, which presents the corresponding flow diagram. As shown, if the capacity check fails, the process terminates with an error; otherwise, the stego audio and composite key are successfully generated.

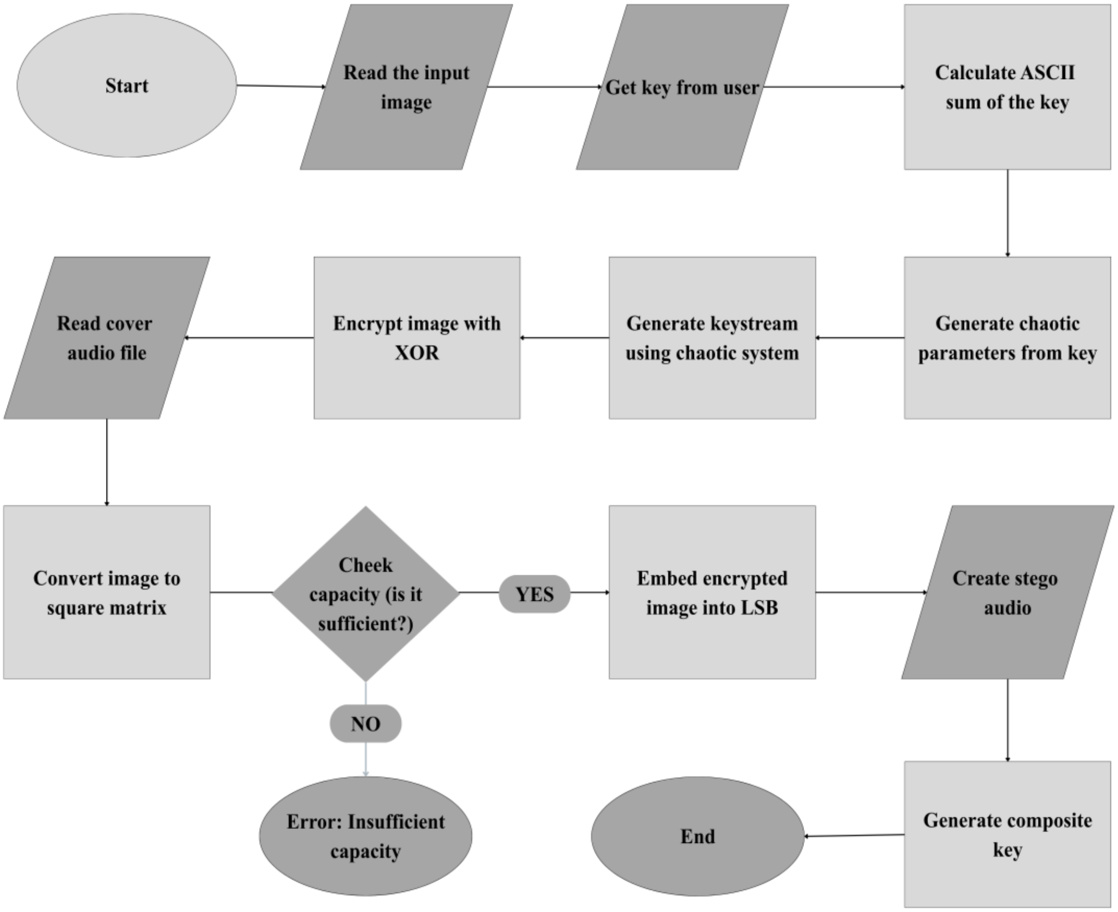
Start
Read the input image
Get key from user
Calculate ASCII sum of the key
Generate chaotic parameters from key
Generate keystream using chaotic system
Encrypt image with XOR
Read cover audio file
Convert image to square matrix
Cheek capacity (is it sufficient?)
YES
Embed encrypted image into LSB
Create stego audio
NO
Error: Insufficient capacity
Generate composite key
End

Figure 1 Flowchart of the process for encrypting an image and embedding it into an audio signal using the LSB method.

5.4 Data Extraction and Decryption Process

In this stage, bits are recovered from the processed audio via LSB extraction and then decoded according to the parameters encoded in the key. The composite key is split to obtain the chaotic algorithm identifier, the base parameter derived from the ASCII sum, the embedded data length, the content type, and—when applicable—the format and dimensions. These fields determine which samples and how many bits to read, which chaotic map and parameters to use for keystream regeneration, and how to reconstruct the original data.

The steps in **Algorithm 2** are illustrated in Figure 2, which depicts LSB extraction from the stego audio, XOR-based decryption with the regenerated chaotic keystream, and reconstruction of the original image.

Algorithm 2: Extract and Decrypt (Audio LSB → XOR → Image)

Input: Stego audio A', composite key K'

Output: Recovered image I

1. **Parse the key:** Split K' to obtain $sum\_ascii, algo\_id, L\_bits, mode, W, H, C$ v, and any other required parameters.
2. **Load stego audio:** Read samples of A' and flatten them into a 1D array, preserving mono/stereo information.
3. **Build bit indices:** Generate the sequential index list $0, 1, 2, \ldots, L - 1$ for LSB extraction.
4. **Extract LSBs:** Read exactly L bits from the specified indices.
5. **Repack bits to bytes:** Pack bits into groups of 8 to obtain the encrypted byte sequence C.
6. **Regenerate keystream:** Using sum_ascii and $algo\_id$, initialize the corresponding chaotic map; discard the transient iterations and produce a keystream K_s of length |C|.
7. **XOR decryption:** Compute $P = C \oplus K\_s$ to decrypt the payload.
8. **Reconstruct the data:** Using mode, W, H, and C from the key, reshape P back into the image and restore its format. If specified, save using the indicated file format (e.g., PNG, JPEG).
9. **Output:** Save and/or return the recovered image I.

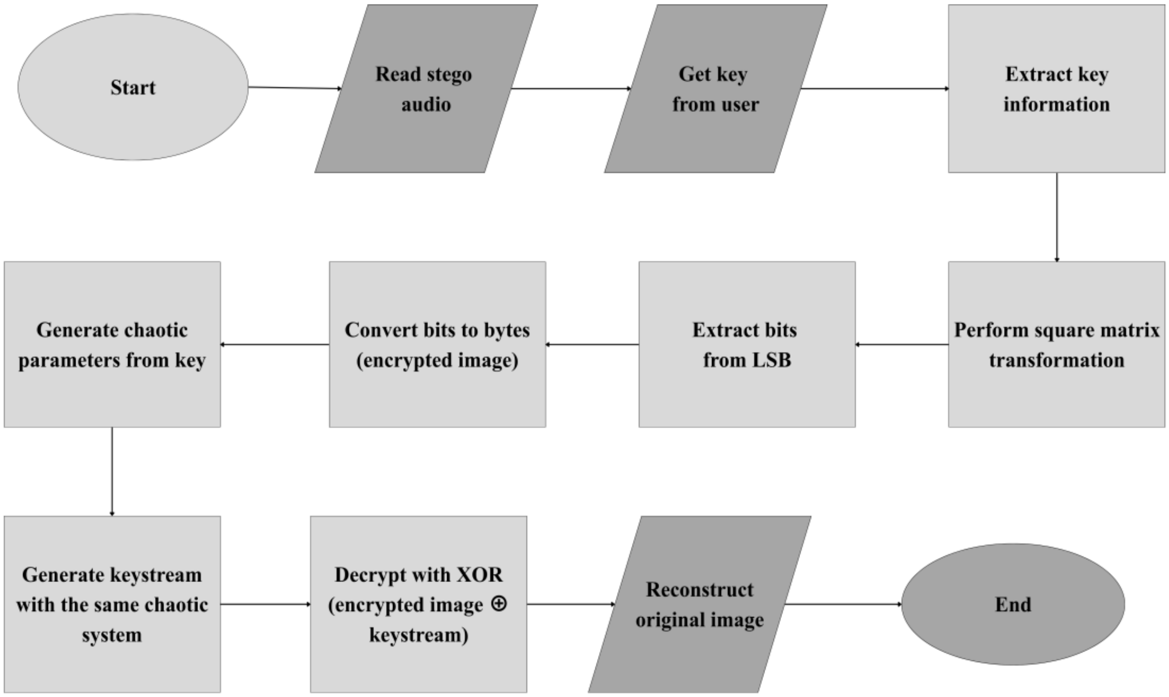
Start
Read stego audio
Get key from user
Extract key information
Perform square matrix transformation
Extract bits from LSB
Convert bits to bytes (encrypted image)
Generate chaotic parameters from key
Generate keystream with the same chaotic system
Decrypt with XOR (encrypted image ⊕ keystream)
Reconstruct original image
End

Figure 2 Flowchart of the process for extracting an embedded image from stego audio and decrypting it using an LSB → XOR pipeline

6. Experimental Results

6.1 Evaluation Metrics and Results

In the experiments, detailed result tables are presented for the three most frequently encountered chaotic algorithms in the literature—Logistic Map**,** Lorenz System**,** and Hénon Map (see Tables 3, 4, and 5). For the remaining algorithms, a summary table comparing their overall performance is provided (Table 6). Since all recovered images consistently yielded **PSNR = ∞, SSIM = 1**, and **BER = 0**, the corresponding image-quality results are not separately tabulated.

Table 3 Logistic Map results

Image	Audio	PSNR (dB)	SNR (dB)	MSE
Baboon	Sine Wave 1 kHz	107.3160	99.2040	1.86E-11
Baboon	Female Speech English	102.3960	78.7884	5.76E-11
Baboon	Harpsichord	106.0130	71.4504	2.50E-11
Baboon	Pink Noise	105.6790	53.3855	2.70E-11
Pepper	Sine Wave 1 kHz	107.2550	99.1462	1.88E-11
Pepper	Female Speech English	102.3510	78.7441	5.82E-11
Pepper	Harpsichord	105.9748	71.4137	2.53E-11
Pepper	Pink Noise	105.6263	53.3346	2.74E-11
Cameraman	Sine Wave 1 kHz	107.2991	99.1880	1.86E-11
Cameraman	Female Speech English	102.3971	78.7895	5.76E-11
Cameraman	Harpsichord	106.0186	71.4558	2.50E-11
Cameraman	Pink Noise	105.6786	53.3851	2.70E-11

Table 4 Lorenz System results

Image	Audio	PSNR (dB)	SNR (dB)	MSE
Baboon	Sine Wave 1 kHz	107.2758	99.1659	1.87E-11
Baboon	Female Speech English	102.3447	78.7379	5.83E-11
Baboon	Harpsichord	105.9747	71.4135	2.53E-11
Baboon	Pink Noise	105.6502	53.3577	2.72E-11
Pepper	Sine Wave 1 kHz	107.2902	99.1795	1.87E-11
Pepper	Female Speech English	102.3528	78.7460	5.82E-11
Pepper	Harpsichord	105.9848	71.4233	2.52E-11
Pepper	Pink Noise	105.6356	53.3436	2.73E-11
Cameraman	Sine Wave 1 kHz	107.2843	99.1740	1.87E-11
Cameraman	Female Speech English	102.3584	78.7514	5.81E-11
Cameraman	Harpsichord	105.9619	71.4013	2.53E-11
Cameraman	Pink Noise	105.6342	53.3423	2.73E-11

To provide a comprehensive comparison, Table 6 presents the average performance metrics of all seven chaotic algorithms across the experimental dataset. The evaluation includes Audio PSNR**,** Audio SNR**,** and Audio MSE, which together reflect the imperceptibility and robustness of the proposed embedding method.

Table 5 Hénon Map results

Image	Audio	PSNR (dB)	SNR (dB)	MSE
Baboon	Sine Wave 1 kHz	107.5228	99.4000	1.77E-11
Baboon	Female Speech English	102.6924	79.0796	5.38E-11
Baboon	Harpsichord	106.3256	71.7505	2.33E-11
Baboon	Pink Noise	105.9735	53.6692	2.53E-11
Pepper	Sine Wave 1 kHz	107.4474	99.3286	1.80E-11
Pepper	Female Speech English	102.5863	78.9754	5.51E-11
Pepper	Harpsichord	106.2137	71.6432	2.39E-11
Pepper	Pink Noise	105.8891	53.5879	2.58E-11
Cameraman	Sine Wave 1 kHz	107.1394	99.0362	1.93E-11
Cameraman	Female Speech English	102.1652	78.5614	6.07E-11
Cameraman	Harpsichord	105.7914	71.2371	2.64E-11
Cameraman	Pink Noise	105.4644	53.1784	2.84E-11

Table 6. Summary results of all seven chaotic algorithms (overall averages)

Algorithm	**Audio PSNR (dB)**	**Audio SNR (dB)**	Audio MSE (×1e-11)
Chebyshev Map	**105.373**	**75.729**	3.19
Chua's Circuit	**105.317**	**75.674**	3.23
Hénon Map	**105.434**	**75.787**	3.15
Logistic Map	**105.334**	**75.690**	3.22
Lorenz System	**105.312**	**75.670**	3.24
Tent Map	**105.259**	**75.618**	3.28
PWLCM	**105.314**	**75.672**	3.23

6.2 Overall Performance Evaluation

Image Quality: For all algorithms, the extracted image achieved a Visual_PSNR = ∞, Visual_SSIM = 1, and Visual_BER = 0. This is visually demonstrated in Figure 3; it can be seen that (a) the original 'Cameraman' image and (c) the image decrypted and extracted from the stego audio are identical (BER=0). Furthermore, the intermediary encrypted image in panel (b) shows that the chaotic encryption layer successfully renders the data unrecognizable. These results demonstrate that the images are preserved in a lossless manner.

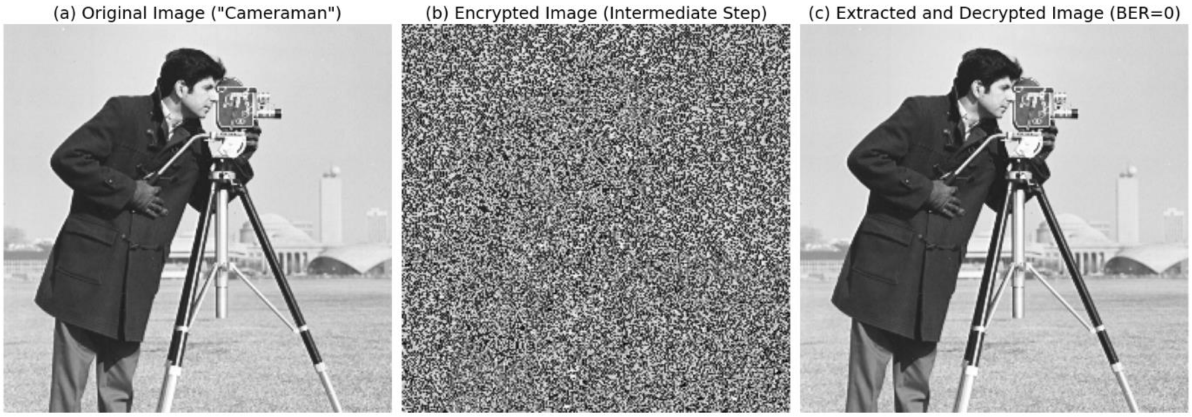
(a) Original Image ("Cameraman")
(b) Encrypted Image (Intermediate Step)
(c) Extracted and Decrypted Image (BER=0)

Figure 3. The encryption and extraction process of the proposed method: (a) Original 'Cameraman' image, (b) Intermediary image encrypted with the chaotic key, (c) Image decrypted and extracted from the stego audio (BER=0)

Audio Quality: The impact of this method on audio quality is visualized in Figure 4. There is no visually discernible difference at the waveform level between (a) a 1-second segment of the original 'Female Speech' signal and (b) the same segment of the data-embedded (stego) signal. Supporting this visual finding, the metric results (See Tables 3-6) show that for tonal sounds, a PSNR of ~107 dB and an SNR of ~99 dB were achieved. In speech and instrument recordings, the SNR is somewhat lower (~79 dB and ~71 dB, respectively), while in the noisy category, the SNR drops to ~53 dB. This difference is due to the structure of the cover signal.

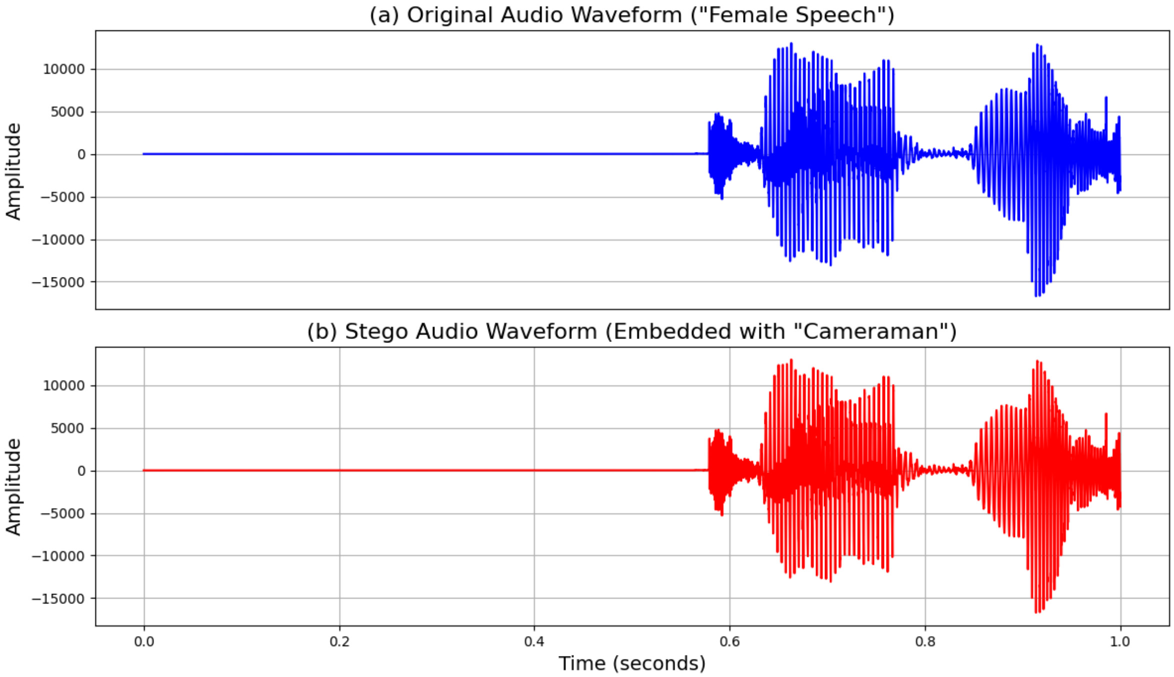

Figure 4. (a) Waveform comparison of a 1-second segment from the original 'Female Speech' audio signal and (b) the stego audio signal with the 'Cameraman' image embedded.

MSE: Across all scenarios, the mean squared error remained on the order of 10^{-11}, showing only theoretical-level variations.

Inter-Algorithm Comparison: All algorithms, including Logistic, Lorenz, and Hénon, demonstrated comparable performance. While the Hénon map exhibited a marginal advantage on average, the difference was not statistically significant.

These findings demonstrate that the method ensures complete data integrity for the images (PSNR = ∞, SSIM = 1, BER = 0) while also maintaining very high perceptual quality on the audio side (Figure 4). Similar high-quality values were obtained with all the different chaotic algorithms. This indicates that the method can operate reliably, independent of the specific chaotic algorithm used.

6.3 Comparative Evaluation with the Literature

A methodological and quantitative comparison with studies sharing similar objectives was conducted to situate this study's performance and original contribution within the context of the literature. Although a study using the exact same audio and image datasets could not be found, Table 7 provides a quantitative perspective by comparing it with the closest available studies.

Table 7 A Methodological and Quantitative Comparison of Chaos-Based Audio Steganography Systems

Study (Author, Year)	Core Methodology	Carrier Audio Dataset	Hidden Data Type	Reported Audio PSNR (dB)	Reported Audio SNR (dB)	Core Innovation Claim / Focus
Alwahbani & Elshoush (2018b)	PWLCM + One-Time Pad + Randomized Upper-Layer LSB	Web-Sourced Speech Audio (1speechsoft.com)	Encrypted Message	Not explicitly reported (focus on robustness)	~9.16 dB – 39.8 dB	Using upper LSB layers for robustness against noise/compression.
Abood et al. (2022)	Bit Cycle Encryption + Improved LSB (Randomized)	.wav audio	Encrypted Text	60–65	Not Reported (SSIM=0.999)	High security with low computational cost and random embedding.
Nasr et al. (2024)	Henon/Baker/Arnold + Image Encryption + ISTFT (Frequency Domain)	Unspecified Audio	Image	~91.2 dB	~72.2 dB	Robustness through frequency domain embedding.
This Study	7 Chaotic Maps + XOR + Sequential 1-bit LSB (Time Domain)	EBU SQAM (Tonal, Noise, Music, Speech)	Standard Test Images (256×256 grayscale)	102–107	53–99	Key-dependent parameters, transient time, vectorization for efficiency

7. Discussion

Experimental findings revealed that high performance was achieved for both image and audio **data.** In all tests, the values of Visual_PSNR = ∞, Visual_SSIM = 1, and Visual_BER = 0 prove that the extracted images are identical to the original data. This result demonstrates that the employed chaotic encryption and LSB embedding structure perfectly preserves visual data integrity.

The original contribution of this work to the literature can be summarized in three main points. First is its superior imperceptibility performance. As seen in Table 7, the PSNR values reported by our method (102–107 dB) are quantitatively significantly higher than those reported in the literature for similar hybrid methods (e.g., 60–65 dB in the study by Abood et al., 2022). This directly indicates a measurable improvement in perceptual transparency, one of the most critical metrics in steganography, over the current state-of-the-art.

Second is the rigorous and principled application of chaos theory. The innovation of the method lies not merely in using chaotic maps, but in consciously enhancing their cryptographic security through specific steps. Key-dependent parameterization creates a much larger key space compared to methods using fixed schemes, thereby complicating brute-force attacks. Furthermore, in line with the literature (Li, Mou, & Cai, 2001), the use of a transient (warm-up) period ensures the statistical randomness of the key stream by discarding the system's initial predictable states. This represents a deeper security approach that is overlooked in many other steganography studies.

Third is computational efficiency. The use of square matrix transformation and NumPy vectorization is a practical contribution that reduces processing time for large files compared to frequency-domain-based methods, like that of Nasr et al. (2024), which are more computationally intensive.

Regarding the generalizability of the method, the strategic choice of the EBU SQAM dataset used in the experiments is of paramount importance. Studies in literature are often tested on statistically homogeneous datasets, such as human speech. In contrast, the EBU SQAM dataset used here inherently contains completely different signal types, such as tonal signals, noise, music, and speech. The method's consistent high performance across these four distinct categories proves that its capability for imperceptibility and quality preservation is not specific to a particular signal type but is valid across a much wider range of signals. This provides stronger evidence for the method's generalizability than tests conducted on a homogeneous dataset.

When different chaotic algorithms were used, all seven systems exhibited similar quality levels. Although the Hénon Map showed a slight advantage in average values, this difference was statistically insignificant. These findings indicate that the method can provide high quality independently of the specific chaotic algorithm.

On the other hand, the study is limited to images of fixed resolution and audio of specific durations/formats. Performance tests with different resolutions, formats, and content types could provide more comprehensive results regarding the method's generalizability. Future work could investigate time-frequency domain embedding, different modulation techniques, or deep learning-based optimization of chaotic system parameters. Furthermore, to enhance security, methods such as the hybrid use of multiple chaotic systems, dynamic key exchange, adaptive LSB strategies, and randomization of the data embedding steps could also be evaluated.

8. Conclusion

In this study, a hybrid framework integrating **k**ey-dependent chaotic number generation, XOR encryption, and LSB data hiding was implemented and tested across seven different chaotic systems. Additional steps—such as the square-matrix structure, parameter derivation, and transient (warm-up) iterations**—**were incorporated to strengthen the security and randomness properties of the method. Furthermore, the vectorization process applied after the square-matrix transformation simplified indexing during embedding and extraction, thereby improving computational efficiency and enhancing the practical applicability of the scheme.

The experimental results demonstrated that, for all chaotic systems, the method achieved comparable PSNR, SNR, and MSE values, ensuring perfect data integrity for images (PSNR = ∞, SSIM = 1, BER = 0) and very high perceptual quality for audio. The highest values were obtained in tonal audio, whereas the expected decrease in SNR was observed in the noisy category.

These findings confirm that the proposed framework, capable of operating with different data types and multiple chaotic systems**,** provides secure embedding and error-free extraction without compromising media quality**.** Moreover, the results highlight that the method can deliver consistently high performance independent of the specific chaotic algorithm employed**.**

Declaration of Ethical Standards

As the authors of this study, we declare that he complies with all ethical standards.

Credit Authorship Contribution Statement

Zeynel Ümit Korkmaz: Software, Validation, Formal analysis, Writing -Original Draft, Visualization.
Fahrettin Horasan: Investigation, Resources, Writing, Review & Editing, Supervision.
Zeynep Çetinkaya: Methodology, Writing -Original Draft, Formal analysis, Validation, Visualization.

Declaration of Competing Interest

The authors declared that they have no conflict of interest.

Funding / Acknowledgements

The authors received no financial support for the research, authorship, and/or publication of this article.

Data Availability

The Python-based implementation developed for this study, along with sample datasets and usage guidelines, is publicly accessible (Korkmaz, 2025).

References

Abd, A. S., Al-Thahab, O. Q. J., & Hamad, A. A. (2025). New approach in steganography algorithm by using audio and image as secure information based on chaotic method. *International Journal of Sustainable and Smart Energy, 15*(2), 349–358. https://doi.org/10.18280/ijsse.150216

Abood, E. W., Abdullah, A. M., Al Sibahee, M. A., Abduljabbar, Z. A., Nyangaresi, V. O., Kalafy, S. A. A., & Ghrabata, M. J. J. (2022). Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. *Bulletin of Electrical Engineering and Informatics, 11*(1), 185–194. https://doi.org/10.11591/eei.v11i1.3279

Alligood, K. T., Sauer, T. D., & Yorke, J. A. (1996). *Chaos: An introduction to dynamical systems*. Springer-Verlag.

Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos, 16*(8), 2129–2151. https://doi.org/10.1142/S0218127406015970

Alwahbani, S. M. H., & Elshoush, H. T. I. (2018a). Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad. In Y. Bi, S. Kapoor, & R. Bhatia (Eds.), *Proceedings of SAI Intelligent Systems Conference (IntelliSys) 2016* (Vol. 16, pp. 755–768). Springer, Cham. https://doi.org/10.1007/978-3-319-56991-8_54

Alwahbani, S.M.H., Elshoush, H.T.I. (2018b). Hybrid Audio Steganography and Cryptography Method Based on High Least Significant Bit (LSB) Layers and One-Time Pad—A Novel Approach. In: Bi, Y., Kapoor, S., Bhatia, R. (eds) Intelligent Systems and Applications. IntelliSys 2016. Studies in Computational Intelligence, vol 751. Springer, Cham. https://doi.org/10.1007/978-3-319-69266-1_21

Balasubramanian, K., Kannan, N., & Ganesan, T. (2024, November). A novel encrypted data hiding and image encryption for authentication based communication framework. In *2024 3rd Edition of IEEE Delhi Section Flagship Conference (DELCON)*. IEEE. https://doi.org/10.1109/DELCON64804.2024.10866888

Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3D chaotic cat maps. *Chaos, Solitons & Fractals, 21*(3), 749–761. https://doi.org/10.1016/j.chaos.2003.12.022

Chen, Y., Tang, C., & Yi, Z. (2020). A novel image encryption scheme based on PWLCM and standard map. *Complexity, 2020*, Article 3026972. https://doi.org/10.1155/2020/3026972

Gonzalez, R. C., & Woods, R. E. (2018). *Digital image processing* (4th ed.). Pearson.

Emin, B., Akgul, A., Horasan, F., Gokyildirim, A., Calgan, H., & Volos, C. (2024). Secure encryption of biomedical images based on Arneodo chaotic system with the lowest fractional-order value. *Electronics*, 13(11), 2122. https://doi.org/10.3390/electronics13112122

Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics, 50*(1), 69–77. https://doi.org/10.1007/BF01608556

Hore, A., & Ziou, D. (2010). Image quality metrics: PSNR vs. SSIM. In *2010 20th International Conference on Pattern Recognition* (pp. 2366–2369). IEEE. https://doi.org/10.1109/ICPR.2010.579

Horasan, F., Ali Pala, M., Durdu, A., Akgül, A., Akmeşe, Ö. F., & Yıldız, M. Z. (2022). DWT‐SVD Based Watermarking for High‐Resolution Medical Holographic Images. *Complexity*, 2022(1), 3154650. https://doi.org/10.1155/2022/3154650

Katzenbeisser, S., & Petitcolas, F. A. P. (2000). *Information hiding techniques for steganography and digital watermarking*. Artech House.

Khalil, N., Sarhan, A., & Alshewimy, M. A. M. (2024). A secure image steganography based on LSB technique and 2D chaotic maps. *Computers & Electrical Engineering, 114*, 109566. https://doi.org/10.1016/j.compeleceng.2024.109566

Khanzadi, H., Eshghi, M., & Borujeni, S. E. (2014). Image encryption using random bit sequence based on chaotic maps. *Arabian Journal for Science and Engineering, 39*(2), 1039–1047. https://doi.org/10.1007/s13369-013-0713-z

Kiran, P., & Parameshachari, B. D. (2022). Resource optimized selective image encryption of medical images using multiple chaotic systems. *Microprocessors and Microsystems, 91*, 104546. https://doi.org/10.1016/j.micpro.2022.104546

Korkmaz, Z. Ü. (2025). *Chaotic Audio Steganography (v1.0)* [Computer software]. GitHub. https://github.com/umitkrkmz/Chaotic_Audio_Steganography

Li, L. (2024). A novel chaotic map application in image encryption algorithm. *Expert Systems with Applications, 252*(Part B), 124316. https://doi.org/10.1016/j.eswa.2024.124316

Li, S., Mou, X., & Cai, Y. (2001). Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography. In C. P. Rangan & C. Ding (Eds.), *Progress in cryptology — INDOCRYPT 2001* (pp. 316–329). Springer. https://doi.org/10.1007/3-540-45311-3_30

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences, 20*(2), 130–141. https://doi.org/10.1175/1520-0469(1963)020<0130:DNF>2.0.CO;2

Matsumoto, T. (1987). Chaos in electronic circuits. *Proceedings of the IEEE, 75*(8), 1033–1057. https://doi.org/10.1109/PROC.1987.13848

May, R. M. (1976). Simple mathematical models with very complicated dynamics. *Nature, 261*(5560), 459–467. https://doi.org/10.1038/261459a0

Nasr, M. A., El-Shafai, W., El-Rabaie, E. S. M., et al. (2024). A robust audio steganography technique based on image encryption using different chaotic maps. *Scientific Reports, 14*, 22054. https://doi.org/10.1038/s41598-024-70940-3

Oppenheim, A. V., & Schafer, R. W. (2010). *Discrete-time signal processing* (3rd ed.). Pearson.

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson Education.

Proakis, J. G., & Salehi, M. (2007). *Digital communications* (5th ed.). McGraw-Hill.

Stallings, W. (2020). *Cryptography and network security: Principles and practice* (8th ed.). Pearson.

Strogatz, S. H. (2014). *Nonlinear dynamics and chaos: With applications to physics, biology, chemistry, and engineering* (2nd ed.). Westview Press.

Wang, Z., Bovik, A. C., Sheikh, H. R., & Simoncelli, E. P. (2004). Image quality assessment: From error visibility to structural similarity. *IEEE Transactions on Image Processing, 13*(4), 600–612. https://doi.org/10.1109/TIP.2003.819861

You, L., Liu, Q., Li, S., & Yang, T. (2025). FDAE: Lightweight privacy protection based on face detection and image encryption. *IEEE Access, 13*, 123297–123313. https://doi.org/10.1109/ACCESS.2025.3588006