



A Secure Audio Encryption Scheme Based on Chaotic Maps and Boolean Operations

Abdullah Jaafar¹, Ahmed Abdulqader Mohammed²
and Abdul-Gabbar Tarish Al-Tamimi³

¹Dean of Faculty of Science and Engineering- National
University- Taiz, Faculty of Computers and Information
Technology- Taiz University

²Dept. of Computer Science- Faculty of Computers and Information
Technology- Taiz University

³Dean of Postgraduate Studies- National University- Taiz, Faculty
of Applied Sciences- Taiz University

2

Abstract:

The advancement of wireless and mobile communications has facilitated the expansion of digital audio exchange over computer networks, creating a significant need to protect audio content across various digital applications such as banking, military, politics, commerce, economics, e-learning, and voice and video conferencing. Audio encryption is a widely adopted method to secure digital audio. In this paper, we present a secure audio encryption scheme utilizing chaotic maps. The encryption process involves three stages: permutation, confusion, and diffusion. The proposed scheme employs three chaotic maps for permuting, confusing, and diffusing audio signals, along with two additional chaotic maps to initialize and control these processes. The key space of our scheme, measuring 2^{128} , makes brute-force attacks impractical. To evaluate the security and robustness of our scheme, we conducted several security tests, including peak signal-to-noise ratio (PSNR), signal-to-noise ratio (SNR), histogram analysis, correlation coefficient analysis, information entropy, differential attack resistance, keyspace, and key sensitivity. The results from these analyses indicate that the proposed audio encryption scheme offers high sensitivity and robust security.

Keywords: Audio Encryption, Chaotic Maps, Symmetrical Encryption, Boolean Operations.

1 .Introduction

The advancement of wireless and mobile communications has significantly expanded the use of digital audio in various applications, including banking, military, politics, commerce, economics, e-learning, and voice and visual conferencing. However, these applications are susceptible to numerous security threats, such as unauthorized eavesdropping and illegal use over shared and open networks. Consequently, protecting sensitive audio content from such threats has become essential. Audio encryption is one approach to safeguarding this content [1]. Encrypting digital audio is generally more complex and challenging than text encryption due to intrinsic features of audio signals, such as large data capacity and high redundancy, which are difficult to manage with traditional methods [2,3,4,5]. Recently, chaotic maps have been employed in cryptography for large-scale data encryption, including text, images, videos, and audio data [5,6,7,8,9] et al, due to their robust properties, such as extreme sensitivity to initial conditions, unpredictability, and random-like behavior [1, 10].

In [11], Mosa et al. introduced a speech cryptosystem based on segment permutation using the chaotic Baker map and substitution using masks in both time and transform domains. The cryptosystem involves three rounds: the first round includes permutation with the chaotic Baker map and masking; the second round involves applying the DCT or DST, followed by permutation with the chaotic Baker map, masking, and applying the Inverse DCT (IDCT) or Inverse DST (IDST); and the third round includes permutation with the chaotic Baker map.

The work in [12] employs two chaotic maps, the circle map and logistic map, for speech confusion and diffusion, respectively. In the confusion stage, the circle map generates a permutation vector to shuffle the speech signal, altering the order of speech segments. During the diffusion stage, the speech sample values are modified using a one-time pad, with the sequence generated by the logistic map serving as the key.

In [13], Elshamy et al. proposed a cryptosystem that combines optical

encryption with chaotic maps. The cryptosystem employs two security phases: the first phase uses a chaotic system based on either the Baker or Cat map to provide an initial security level, while the second phase involves optical encryption using double random phase encoding (DRPE) for additional security.

Mahmood et al. in [14] presented a hybrid cryptosystem and steganography method for digital audio based on a chaos system and secret sharing scheme. The first phase encrypts the digital audio using the Lorenz chaos map, and in the second phase, the encrypted audio is divided into N parts based on the secret sharing scheme. Finally, the N encrypted audio parts are hidden within N cover images using a chaotic system.

Parvees et al. in [9] introduced a cryptosystem that converts plain digital 8-bit audio bytes into cipher audio bytes. The encryption scheme utilizes the Henon map and chaotic economic map to generate sequences. The algorithm comprises two security phases: in the first phase, a permutation operation is conducted using the chaotic economic map, and in the second phase, an XOR operation is applied between the audio samples and the Henon map sequences.

In [7], Yussra et al. presented a symmetric block audio encryption approach consisting of two parts: confusion and diffusion. The confusion process generates two arrays of logistic maps, which are then used to shuffle the plain audio data. The diffusion mechanism is achieved by applying an XOR operation between the audio samples, a random value, and a chaotic logistic map array.

Kordov in [15] introduced a new cryptosystem designed for audio file security, based on classic symmetric models using a pseudo-random number generator combined with a chaotic circle map and modified rotation equations. The algorithm involves two security phases: in the first phase, the bits from the current sample are shifted using the value P obtained from the chaotic circle map, and in the second phase, an XOR operation is applied between the audio samples and the sequences generated by the modified rotation equations.

In [16], Farsana et al. proposed an audio encryption algorithm based on chaos maps. Initially, the audio file is compressed using the Fast Walsh Hadamard Transform (FWHT). The algorithm then employs two security phases: in the first phase, a permutation operation is carried out using a modified discrete Henon map, and in the second phase, a modified Lorenz hyper-chaotic system is used for a substitution operation to fill the silent periods within the speech conversation.

Alemami et al. in [17] introduced an audio cryptosystem using Fast Fourier Transform (FFT) and chaotic maps (Logistic Map and Sine Maps). First, the audio samples are encrypted using FFT, followed by confusion using the logistic map, and finally, the audio samples are masked by XORing with the sine map sequences.

In [8], Faragallah et al. presented a secure opto-audio cryptosystem utilizing an XORing mask and the Hartley Transform (HT). Initially, audio samples are masked by XORing with a chosen secret image. The audio samples are then scrambled using a logistic-adjusted-sine map, and finally, they are optically encrypted using the Hartley Transform.

Al Zahawy & Hreshee [42] presented a novel hybrid approach to enhance audio/voice encryption security by integrating the International Data Encryption Algorithm (IDEA) with a Digital Chaotic Scrambler (DCS) based on the Lorenz chaotic system. The study identifies inherent limitations in using IDEA alone for voice encryption and proposes the incorporation of chaotic scrambling to improve resistance against cryptanalytic attacks. The DCS augments the cryptographic strength of IDEA by leveraging the high unpredictability and sensitivity to initial conditions characteristic of chaotic systems.

Gebereselassie et al. [43] proposed a secure audio encryption algorithm that exploits the inherent properties of chaotic systems, specifically the Gauss map and the Henon map, to enhance the confidentiality of digital audio signals. In their approach, chaotic sequences generated from the two maps are used to perform permutation and diffusion operations on the audio samples, ensuring high sensitivity to initial conditions and control

parameters. The combination of Gauss and Henon chaotic maps increases the complexity of the encryption process and enlarges the key space, making the scheme more resistant to brute-force and statistical attacks.

The study by Jawad, Karimi, and Radmalekshahi [44] proposes a novel chaos-based voice encryption scheme termed the Lorenz–Rössler–Chan (LRC) algorithm, aiming to enhance the security and efficiency of digital voice communications. The proposed algorithm integrates three chaotic systems—Lorenz, Rössler, and Chan—into a unified encryption framework to increase system complexity and key sensitivity. By exploiting the nonlinear dynamics and high sensitivity to initial conditions of these chaotic maps, the LRC algorithm achieves effective scrambling of voice signals in both time and amplitude domains. The authors design the encryption process to generate multiple chaotic sequences that are used for permutation and diffusion of the voice data, thereby strengthening resistance against statistical, brute-force, and differential attacks.

Maity and Dhara [45] proposed a novel audio encryption scheme that integrates Empirical Mode Decomposition (EMD) with a two-dimensional Cosine Logistic chaotic map to enhance the security of digital audio signals. In their approach, the original audio signal is first decomposed into a set of Intrinsic Mode Functions (IMFs) using EMD, enabling adaptive and data-driven signal representation. Selected IMFs are then encrypted through permutation and diffusion processes governed by the 2D Cosine Logistic map, which provides high sensitivity to initial conditions and strong randomness characteristics. The encrypted IMFs are subsequently recombined to produce the final cipher audio.

Farsana, Devi, and Gopakumar [46] proposed a robust audio encryption scheme that integrates the Fast Walsh–Hadamard Transform (FWHT) with mixed chaotic keystreams to enhance the security of digital audio signals. In the proposed approach, the input audio signal is first transformed into the FWHT domain to reduce statistical redundancy and decorrelate adjacent samples. Subsequently, multiple chaotic maps are employed to generate complex and highly sensitive keystreams, which are combined to perform confusion and diffusion operations on the

transformed audio data. The encryption process is symmetric and relies on secret initial conditions and control parameters of the chaotic systems, ensuring a large key space and high key sensitivity.

Though numerous chaos-based audio cryptosystems have been proposed, chaos-based audio encryption still faces various security challenges from the perspective of modern cryptology [2]. In this paper, we propose an audio encryption scheme based on chaotic maps. The proposed scheme uses three chaotic maps for permutation, confusion, and diffusion, and two other chaotic maps to initialize and control the above chaotic maps. The key space of the proposed scheme is 2^{128} . The proposed audio encryption scheme offers high security with relatively fast encryption speed and can be implemented in both hardware and software. The rest of the paper is organized as follows: Section 2 presents the chaotic maps employed in the proposed encryption scheme; Section 3 describes the proposed algorithm; Section 4 discusses the security analysis and various results obtained from testing the system on audio files of different sizes; and finally, Section 5 concludes the paper.

2 Chaotic Maps Employed in the Proposed Encryption Scheme

In this section, we discuss the chaotic maps utilized in the proposed algorithm. These chaotic maps generate random sequences, which are then used to shuffle the positions of signals within the audio file, confuse the signal values, and aid in the diffusion process.

2.1 Chebyshev Chaotic Map

The Chebyshev chaotic map is a one-dimensional chaotic system characterized by an initial condition x_0 and a control parameter k . Mathematically, the Chebyshev chaotic map is expressed as follows [18]:

$$x_{(n+1)} = \cos(k \cos^{-1}(x_n)) \quad (1)$$

where $x_n \in [-1, 1]$ represents the initial condition, n is the number of iterations, and $k \in [2, \infty)$ is the control parameter of the map. In the proposed algorithm, the Chebyshev chaotic map is employed to generate

random sequences, which are used to shuffle the positions of signals within the audio file.

2.2 The Logistic Map

Proposed by Pierre Verhulst in 1845, the logistic map is one of the simplest and most well-known chaotic maps. Mathematically, the logistic map is expressed as follows [19]:

$$x_{n+1} = \mu x_n (1 - x_n) \quad (2)$$

where n is the number of iterations, μ is the system parameter with $3.57 < \mu < 4$, and x_0 is the initial condition of the map. In our proposed encryption scheme, the logistic map is used to generate random sequences based on Equation 2, which are then employed in the confusion process.

2.3 Henon Map

In 1976, Michel Hénon proposed a two-dimensional nonlinear discrete chaotic map. The Henon map takes two inputs, (x_i, y_i) , and produces two sets of random values as output. It was developed as a simplified version of the Poincaré map for the Lorenz system [20], and is represented by state equations with a chaotic attractor [21]. While retaining the essential properties of the Lorenz system, the Henon map is more accurate, faster, and allows for more thorough mathematical analysis. Mathematically, the Henon chaotic map is expressed as follows [20]:

$$\begin{aligned} x_{(n+1)} &= 1 - \alpha x_n^2 + y_n \\ y_{(n+1)} &= \beta x_n \end{aligned} \quad (3)$$

where x_0 and y_0 are the initial conditions of the map, n is the number of iterations, and $\alpha \in (0, 1.4]$ and $\beta \in (0.2, 0.314]$ are the control parameters. In our proposed encryption scheme, the Henon map is employed to generate random sequences using Equation 3, which are then utilized in the diffusion process.

2.4 Chaotic Standard Map

The chaotic properties of the standard map were established by Boris

Chirikov in 1969. The standard chaotic map has a large key space [22]. Mathematically, the standard chaotic map can be written as follows [23]:

$$\begin{aligned} p_{(n+1)} &= p_n + c \sin(q_n) \\ q_{(n+1)} &= q_n + p_{(n+1)} \end{aligned} \quad (4)$$

where p_0 and q_0 are the initial conditions of the map, n is the number of iterations, and c is the control parameter of the map. The values of p_n and q_n are taken modulo 2π . In the proposed algorithm, the chaotic standard map is used to generate the initial values for the chaotic Henon map.

2.5 Lorenz Chaotic Map

The Lorenz chaotic map is described by three differential equations, commonly known as the Lorenz equations, which were modeled by Edward Norton Lorenz [24]. Equation 5 represents the Lorenz chaotic map [14]:

$$\begin{aligned} \frac{dx}{dt} &= \alpha (y - x) \\ \frac{dy}{dt} &= \gamma x - xz - y \\ \frac{dz}{dt} &= xy - \beta z \end{aligned} \quad (5)$$

where α , γ , and β are the system parameters. The initial conditions of the Lorenz system are denoted as x_0 , y_0 , and z_0 . When $\alpha = 10$, $\beta = 8/3$, and $\gamma = 28$, the Lorenz system exhibits chaotic behavior. In the proposed algorithm, the Lorenz map is used to generate the initial values for the logistic map.

3 The Proposed Scheme

Audio technology encompasses the processes of storing, processing, reproducing, and generating sound through digital representations of audio signals. In digital audio systems, sound is represented as a sequence of discrete samples obtained by sampling the continuous audio waveform at specific intervals. Each sample corresponds to a numerical value that reflects the amplitude of the audio signal at a given point in time. Consequently, digital audio data consist of a series of discrete values that

collectively describe the temporal and amplitude characteristics of the original sound waveform.

In this paper, we propose a symmetric stream-based audio encryption scheme founded on chaotic maps and Boolean operations. The proposed encryption technique is planned to protect the uncompressed digital audio integer 8 (8 bit) format. The encryption and decryption processes use the same secret key, which characterizes the scheme as symmetric. Initially, the input audio signal is digitized and converted into a sequence of bytes, enabling byte-level stream encryption. The encryption procedure consists of three main stages: permutation, confusion, and diffusion. In the permutation stage, sequences generated by the Chebyshev chaotic map are employed as secret keys to rearrange the audio bytes, thereby reducing statistical correlation within the signal. During the confusion stage, the byte values of the permuted audio stream are modified using a keystream generated by the logistic and Henon chaotic maps through Boolean operations, providing stream-wise encryption. In the diffusion stage, the encrypted audio bytes are sequentially updated by mixing them with keystream elements produced by a two-dimensional Henon chaotic map, ensuring that a small change in the plaintext propagates across the entire ciphertext. The proposed scheme utilizes a 128-bit secret key, represented in binary form, to initialize the chaotic maps and generate the encryption keystream. Owing to its stream-oriented processing at the byte level, the scheme is well suited for real-time audio encryption applications. The overall encryption methodology is illustrated in Figure 1.

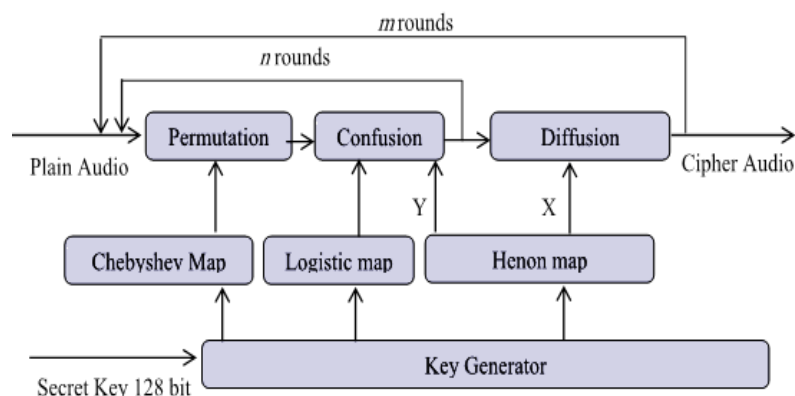


Figure 1 : The architecture and methodology of the proposed encryption scheme

3.1 Key Generation

The proposed method uses a secret key of 128 bits. This binary sequence is divided into seven segments, as outlined in Table 1.

- The key used in the proposed encryption scheme is a binary sequence of 128 bits, divided into seven segments as follows:

$$K = \{K_1, K_2, K_3, K_4, K_5, K_6, K_7\}$$

where K_1 is 32 bits long, and K_2 to K_7 are each 16 bits long.

- The subkey K_5 is converted from binary to decimal using Equation 6, while K_1, K_2, K_3, K_4, K_6 , and K_7 are converted from binary to decimal fraction values using Equations 7 and 8.:

$$K_{int} = \sum_{i=0}^{15} K_5(i) 2^i \quad (6)$$

$$K_{fra}(1) = \sum_{i=1}^{32} K_1(i) 2^{-i} \quad (7)$$

$$K_{fra}(j) = \sum_{i=1}^{16} K_j(i) 2^{-i} \quad j=2,3,4,6,7 \quad (8)$$

where $K_j(i)$ is bit i in the sequence K_j .

- The subkey K_1 is assigned as the initial value for the Chebyshev map $x_0 = K_1$ with $k \in [2, \infty)$ as per Equation 1.
- The subkey K_5 is used as the round number for rotation to determine the initial values of the chaotic maps, where $NR = K_5$.
- Assign $x_0 = K_2$, $y_0 = K_3$, $z_0 = K_4$, $\alpha = 10$, $\beta = 8/3$ and $\gamma = 28$ in Equation 5 to obtain the initial value for the Logistic map (Equation 2) as follows:

$$\begin{aligned} [x, y, z] &= \text{Lorenz_map}(x_0, y_0, z_0, NR) \\ x_0 &= (x + y + z) \bmod 1 \end{aligned} \quad (9)$$

- Assign $p_0 = (K_6 \bmod 2\pi)$, $q_0 = (K_7 \bmod 2\pi)$ and $c = 4.6$ in Equation 4 to obtain the initial values for the Henon map x_0, y_0 in Equation 3, as follows:

$$\begin{aligned} [x, y] &= \text{Standard_map}(p_0, q_0, NR) \\ x_0 &= \frac{x}{100} \\ y_0 &= \frac{y}{100} \end{aligned} \quad (10)$$

Table 1: Subkeys and Parameters

Sub	size	Type	Parameter	Chaotic Map
K_1	32 bit	decimal fraction	X_0	Chebyshev Map
K_2	16 bit	decimal fraction	x_0	Lorenz Map $\rightarrow$ Logistic Map
K_3	16 bit	decimal fraction	y_0	
K_4	16 bit	decimal fraction	z_0	
K_5	16 bit	decimal	NR	Iterations number
K_6	16 bit	decimal fraction	p_0	Standard Map $\rightarrow$ Henon Map
K_7	16 bit	decimal fraction	q_0	

The chaotic key stream (CKS) is generated by iterating the chaotic Chebyshev map, Henon map, and Logistic map using the secret key as follows:

- The permutation key is generated using the chaotic Chebyshev map. A sequence of size N is generated by iterating the Chebyshev map (Equation 1) with the initial condition y_0 and constant $k=2$, as follows:

$$x = Chebyshev_Map(y_0, N)$$

$$[K_{cheby}, f_x] = sort(x) \quad (11)$$

where N is the number of signals in the audio file. The function $sort()$ indicates index sequencing, with f_x index values and K_{cheby} as the sequences obtained after sorting x .

- The confusion key is generated using the chaotic Logistic map. A sequence of size N is generated by iterating the Logistic map (Equation 2) with the initial condition x_0 obtained in Equation 9, and constant $\mu=3.99$. x is then converted from real numbers to integers, as follows:

$$x = Logisitc_Map(x_0, N)$$

$$key = (\lfloor x \times 10^{14} \rfloor) \bmod 2^L \quad (12)$$

Here $\lfloor \cdot \rfloor$ represents the floor function, and L is the number of bits per signal of the audio file.

- The diffusion key is generated using the chaotic Henon map, keeping the Henon map system parameter values $\alpha=1.4$ and $\beta=0.4$, which correspond to a highly chaotic state. A sequence of size N is generated by iterating the Henon map using the initial conditions x_0 and y_0 obtained in Equation 10. X and Y are then converted from real numbers to positive integers as follows:

$$\begin{aligned} [x, y] &= Henon_Map(x_0, y_0, h, w, t) \\ K_x &= (\lfloor x \times 10^{14} \rfloor) \bmod 2^L \\ K_y &= (\lfloor y \times 10^{14} \rfloor) \bmod 2^L \end{aligned} \quad (13)$$

where L is the number of bits per signal of the audio file.

3.2 Encryption Algorithm

This subsection details the step-by-step process for the proposed audio encryption scheme. The algorithm creates the cipher audio C from the plain audio P . The steps are detailed below, and the entire process is illustrated in Figure 1 and Algorithm 1:

- **Step 1:** Load the audio file.
- **Step 2:** Key generation: Select a sequence of 128 bits as the key and split it into seven groups to initialize the chaotic maps, as discussed in subsection 3.1.
- **Step 3:** Perform permutation using the Chebyshev map (Equation 1) and (Equation 11), as follows:

$$swap(signal(index), signal(K(index)))$$

where $index = 1, 2, \dots, N$.

- **Step 4:** Perform confusion using the Logistic Map (Equation 2) and Henon Map (Equation 3), as follows:
- $$signal = ((signal + K_1) \bmod 2^L) \oplus K_2$$
- where $K_1 = X_{\text{Logistic}}$ (Equation 12) and $K_2 = Y_{\text{Henon}}$ (Equation 13).
- **Step 5:** Repeat Steps 3 and 4 for n rounds.
 - **Step 6:** Perform diffusion using the X-Henon Map (Equation 3). Perform "XOR plus mod" operations on $signal(index)$, $signal(index-1)$, and the chaotic key stream $K = X\text{-Henon}$ (Equation 13), as follows:

$$\begin{aligned} &signal(index) \\ &= ((signal(index) \oplus signal(index-1)) \\ &+ K(index)) \bmod 2^L \end{aligned}$$

where $index = 1, 2, \dots, N$ and $signal(0) = K(1)$.

- **Step 7:** Repeat **Steps 3** through **6** for m rounds.

Algorithm 1: The Full Audio Encryption System

input : Plain Audio File

output: Cipher Audio File

```

1  Begin
2  | Select a sequence of 128 bits as the key
   | /* Key generation */
3  | key=Chebyshev( $X_0, N$ )
4  |  $K_1$ =Logistic_Map( $X_0, N$ )
5  | [ $K, K_2$ ]=Henon_Map( $x_0, y_0, N$ )
   | /* Encryption Process */
6  | for  $ch = 1$  to  $numchannel$  do
7  | | signal=channel( $ch$ );
8  | | for  $m = 1$  to  $M\_rounds$  do
9  | | | for  $n = 1$  to  $N\_rounds$  do
   | | | | /* Permutation Process */
10 | | | | signal = swap(signal,key)
   | | | | /* Confusion Process */
11 | | | | signal= ((signal+ $K_1$ ) mod  $2^L$ )  $\oplus K_2$ 
12 | | | end
   | | | /* Diffusion Process */
13 | | | signal(1) = ((signal(1)  $\oplus K(1)$ )+ $K(1)$ ) mod  $2^L$ 
14 | | | for  $i = 2$  to  $N$  do
15 | | | | signal(i) = ((signal(i)  $\oplus$  signal(i-1))+ $K(i)$ ) mod  $2^L$ 
16 | | | end
17 | | end
18 | end
19 end

```

3.3 Decryption Algorithm

This subsection details the step-by-step process for the proposed audio decryption scheme. The algorithm regenerates the plain audio P from the cipher audio C . The steps are detailed below, with the entire process illustrated in Algorithm 2:

- **Step 1:** Load the cipher audio file.
- **Step 2:** Key generation: Select a sequence of 128 bits as the key and split it into seven groups to initialize the chaotic maps, as discussed in subsection 3.1.
- **Step 3:** Perform inverse diffusion using the X-Henon Map (Equation 3) and (Equation 13), as follows:

$$signal(i) = ((signal(i) - K(i)) \bmod 2^L) \oplus signal(i - 1)$$

where index $i=N, N-1, \dots, 2$.

- **Step 4:** Perform inverse confusion using the Logistic Map (Equation 2) and Y-Henon Map (Equation 3) as follows:

$$signal = ((signal \oplus K_2) - K_1) \bmod 2^L$$
 where $K_1 = X_{\text{Logistic}}$ (Equation 12) and $K_2 = Y_{\text{Henon}}$ (Equation 13).
- **Step 5:** Perform inverse permutation using the Chebyshev Map (Equation 1) and (Equation 11), as follows:

$$signal(K(index)) \leftrightarrow signal(index)$$
 where $index = (1, 2, \dots, N)$.
- **Step 6:** Repeat Steps 4 and 5 for n rounds.
- **Step 7:** Repeat Steps 3 through 6 for m rounds.

Algorithm 2: The Full Audio Decryption System

input : Cipher Audio File

output: Plain Audio File

```

1  Begin
2  | Select a sequence of 128 bits as the key
   | /* Key generation */
3  | key=Chebyshev( $X_0, N$ )
4  |  $K_1 = \text{Logistic\_Map}(X_0, N)$ 
5  |  $[K, K_2] = \text{Henon\_Map}(x_0, y_0, N)$ 
   | /* Decryption Process */
6  for  $ch = 1$  to  $numchannel$  do
7  | signal=channel( $ch$ );
8  | S=signal;
9  | for  $m = 1$  to  $M\_rounds$  do
   | /* Inverse Diffusion Process */
10 | for  $i = 2$  to  $N$  do
11 | | signal( $i$ )= ((signal( $i$ )- $k(i)$ )  $\bmod 2^L$ )  $\oplus$  S( $i-1$ )
12 | End
13 | signal(1)= ((signal(1) -  $K(1)$ )  $\bmod 2^L$ )  $\oplus$   $K(1)$ 
14 | for  $n = 1$  to  $N\_rounds$  do
   | /* Inverse Confusion Process */
15 | | signal= ((signal  $\oplus K_2$ ) -  $K_1$ )  $\bmod 2^L$ 
   | /* Inverse Permutation Process */
16 | | signal = Inverse_swap(signal, key)
17 | End
18 | End
19 End
20 End

```

4 The Result of the Proposed Experiment

This section discusses the security analysis of the proposed encryption scheme, including statistical analysis, sensitivity analysis, key space

analysis, and time analysis. These analyses demonstrate that the proposed cryptosystem is robust against chosen/known plaintext attacks and suitable for real-time applications. Several experiments were conducted on different audio sequences (male and female) with a sampling frequency of 8-44.1 kHz and 8 bits per sample (M-rounds=1, N-rounds=1), as shown in Table 2. The employed audio samples were sourced from the Internet.

Table 2: Audio samples used in experiments

File name	bit/Sample	Sample/Rate	Duration	Number of channel
female_male.wav	8 bit	8000	5 sec	1
male.wav	8 bit	8000	5 sec	1
female.wav	8 bit	8000	3 sec	1
chimes.wav	8 bit	44100	13 sec	2
music.wav	8 bit	44100	22 sec	2
guitar.wav	8 bit	44100	15 sec	1

4.1 Histogram Analysis

The audio signal histogram represents the intensity distribution of the signal within the audio file. In the original audio file, the signal density varies, while for effective audio signal encryption, the density distribution should be nearly uniform. An example of the simulation results using audio signals is shown in Figures 2 and 3. The encrypted audio signal exhibits a fairly uniform histogram, significantly different from the original audio signal histogram. This ensures that no useful information is provided for attackers attempting any statistical attack on the encrypted audio signal.

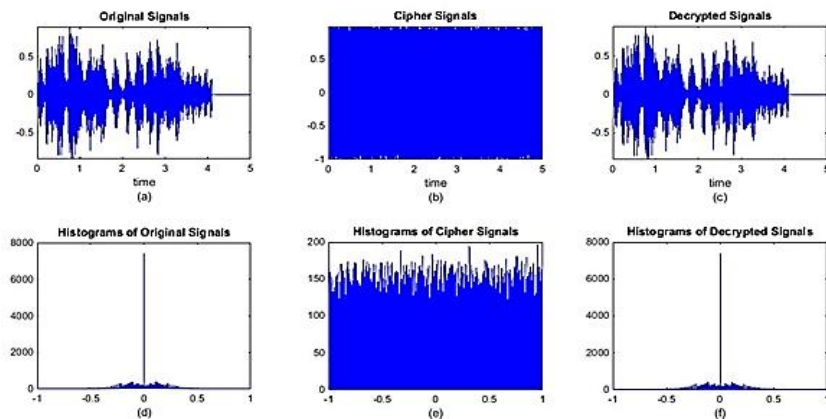
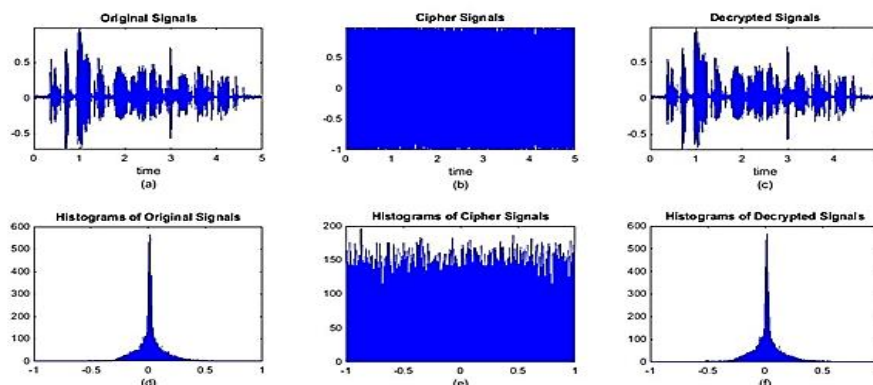


Figure 2: (a) original, (b) encrypted, and (c) decrypted signals. Signals



histograms for female male audio file are shown in (d, e, f), respectively

Figure 3: (a) original, (b) encrypted, and (c) decrypted signals. Signals histograms for male audio file are shown in (d, e, f), respectively

4.2 Statistical Analysis

Statistical analysis was conducted on the proposed audio encryption scheme, demonstrating its strong confusion and diffusion properties, making it highly resistant to statistical attacks. This evaluation included calculating the correlation coefficient, signal-to-noise ratio (SNR), mean square error (MSE), and peak signal-to-noise.

4.2.1 Correlation Coefficient (CC)

The correlation coefficient between the original audio signals and the encrypted audio signals indicates the extent to which the original audio signals are related to the encrypted audio signals. It is used to determine the relationship between the encrypted audio signals and the original audio signals and to assess the key or secret signals. If the CC equals 1, it indicates a direct correlation between the two values, while -1 indicates an inverse correlation, and 0 indicates no correlation [25]. The correlation coefficient between signal values is calculated as follows [4, 9]:

$$CC = \frac{\frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y))}{\sqrt{\frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2} \sqrt{\frac{1}{N} \sum_{i=1}^N (y_i - E(y))^2}} \quad (14)$$

where $E(x) = \frac{1}{N} \sum_{i=1}^N X_i$ and x_i, y_i are the values of the original and encrypted audio signals. Results for different audio samples are shown in Table 3, where the correlation coefficients are very low ($CC \approx 0$), indicating that the plain audio file is nearly independent of the encrypted audio file.

Table 3: The correlation coefficient values (CC)

File name	CC between original and encryption signal	CC between adjacent samples in the encryption signal	CC between adjacent samples in the original signal
female_	-0.00348	-0.00647	0.94296
male	0.00138	0.00219	0.92742
female	0.00351	-0.00339	0.77871
chimes	0.00074	-0.0005	0.99982
music	0.00086	0.0005	0.99905
guitar	-0.001201	0.0023	0.99891

4.2.2 Peak Signal-to-Noise Ratio (PSNR)

PSNR is used to determine how distorted the original audio signal becomes when encrypted. For a good encryption algorithm, PSNR values should be low. PSNR is defined as follows [9]:

$$PSNR = 10 \times \log_{10} \left[\frac{(2^L - 1)^2}{MSE} \right] \quad (15)$$

where L is the number of bits per signal of the audio file.

4.2.3 Mean Squared Error (MSE)

MSE is used to measure the performance of the decryption process. The smaller the MSE value, the better the recovered audio signal quality. Conversely, the larger the MSE value, the worse the recovered audio signal quality. MSE is defined as follows [9]:

$$MSE = \frac{\sum_{i=1}^N \sum_{j=1}^M (C_1(i,j) - C_2(i,j))^2}{N \times M} \quad (16)$$

where C_1 and C_2 represent the original audio and the encrypted audio, respectively, N represents the number of channels, and M represents the size of each channel in the audio file.

4.2.4 Mean Absolute Error (MAE)

A successful audio encryption scheme should produce frames that are significantly different from the original audio signal before encryption. The average absolute change in intensities between the encrypted audio file and the source audio file is computed as follows [8]:

$$MAE = \frac{\sum_{i=1}^N \sum_{j=1}^M |P(i,j) - E(i,j)|}{N \times M} \quad (17)$$

where P and E denote the intensities of the signal in the plain and encrypted audio files, respectively. N and M are the number of channels and the channel size in the audio file.

4.2.5 Signal to Noise Ratio (SNR)

The signal-to-noise ratio (SNR) measures the noise content in the encrypted audio signal. The SNR values of the encrypted audio files are calculated based on the following equation [2]:

$$SNR = 10 \times \log_{10} \frac{\sum_{i=1}^N |x_i|^2}{\sum_{i=1}^N (|x_i| - |y_i|)^2} \quad (18)$$

where x_i and y_i denote the intensities of the signal in the plain and

encrypted audio files, respectively. Table 4 shows the average values of PSNR, SNR, MSE, and MAE for the sample audio files analyzed using the proposed scheme. The MSE and MAE values are very large, and the PSNR and SNR values are very low, indicating that the proposed algorithm has strong resistance against statistical attacks.

Table 4: The PSNR, SNR, MSE and MAE values of encrypted audio file

File name	PSNR	SNR	MSE	MAE
female_male	8.6993	1.9562	8772.9	76.9
Male	10.5182	4.7207	5771	65.3
female	10.3517	5.525	5996	65.9
chimes	9.91	3.87	6623	68.5
music	10.28	4.19	6093	66.5
guitar	10.63	4.69	5615	64.6

4.3 Entropy Analysis

Entropy measures the randomness of encrypted audio. Since the audio signal carries 8-bit information, the expected ideal entropy value should be 8. By analyzing the entropy, it is possible to understand how the audio signal values are distributed. Entropy H is calculated using the following equation 19 [4, 5]:

$$H(m) = - \sum_{i=0}^{2^N-1} P(m_i) \log_2 [P(m_i)] \quad (19)$$

where $p(m_i)$ is the probability that a signal has a specific value m_i , and N denotes the total number of signal values. Table 5 shows the entropy values of the proposed audio encryption scheme, where the entropy value is 7.999, which is very close to the ideal value. Therefore, the proposed scheme demonstrates robust performance against entropy attacks.

Table 5: Information entropy values of plain and cipher audio files

File name	Original signals	cipher signals
female_male	5.6899	7.9949
male	5.5637	7.9952
Female	5.5005	7.9926
Chimes	6.3464	7.9997
Music	5.4421	7.9998
Guitar	5.496	7.9998

4.4 Differential Attack Analysis

To assess the security of the proposed audio encryption scheme, we conducted several analyses, including key sensitivity, plain-text sensitivity, and key space analysis. Each of these analyses is detailed in the following subsections. The Number of Changing Pixel Rate (NPCR) between two audio files, C_1 and C_2 , is calculated based on the following equation [26, 9, 5]:

$$\text{NPCR} = \frac{\sum_{i=1}^N \sum_{j=1}^M D(i,j)}{N \times M} \times 100\% \quad (20)$$

$$\text{where } D(i, j) = \begin{cases} 0 & \text{if } C_1(i, j) = C_2(i, j) \\ 1 & \text{if } C_1(i, j) \neq C_2(i, j) \end{cases}$$

where N and M represent the number of channels and the channel size in the audio, respectively. Similarly, the Unified Averaged Changed Intensity (UACI) is used to measure the difference between two audio signals, C_1 and C_2 , and is calculated as follows [9, 5]:

$$\text{UACI} = \frac{1}{N \times M} \times \left[\sum_{i=1}^N \sum_{j=1}^M \frac{|C_1(i,j) - C_2(i,j)|}{2^L - 1} \right] \times 100\% \quad (21)$$

where N and M represent the number of channels and the channel size in the audio file, respectively.

4.4.1 Plainaudio Sensitivity Analysis

The NPCR and UACI are commonly used to evaluate the strength of audio encryption algorithms against differential attacks [27]. We tested the proposed scheme by evaluating the impact of a one-signal change on the audio file. First, we encrypted the original audio file using the key k_1 to obtain the encrypted audio file C_1 . Then, we changed one bit in the original audio file and encrypted it again with the same key k_1 to obtain the encrypted audio file C_2 . We measured the similarity between the encrypted audio files C_1 and C_2 using NPCR. Table 6 presents the NPCR and UACI values for encrypted audio files that differ from the plain audio file by just one bit. The results show that even a small change in the original audio file leads to a significant change in the ciphered audio file, indicating that the proposed algorithm is highly resistant to differential attacks.

4.4.2 Key Sensitivity

The output of the cryptosystem should be sensitive to the secret key. To validate this, we applied NPCR. We encrypted the same audio file using two different keys, k1 and k2, and measured the similarity between the resulting encrypted audio files using NPCR. The difference between k1 and k2 was a single bit flipped at a random position. For the proposed algorithm, the percentage difference between the audio encrypted with k1 and that encrypted with k2 is greater than 99.60% for all tested audio files, as shown in Table 7. This indicates that even a slight change in the key value will produce a significantly different output, enhancing the system's security.

Table 6: NPCR and UACI of encrypted audio files with one bit difference from the plain audio file

File name	NPCR	UACI
female_male	99.8775	33.3662
male	99.8775	33.3657
female	99.8375	33.2961
chimes	99.9915	33.4378
music	99.9949	33.3958
guitar	99.985	33.57

Table 7: Comparison of single difference between audio files encrypted by keys with one-bit difference

File name	NPCR	UACI
female_male	99.5825	33.3108
male	99.5225	33.5823
female	99.6667	33.1656
chimes	99.6108	33.4799
music	99.6117	33.4245
guitar	99.6132	33.46

4.5 Key Space Analysis

The key space is the total number of possible keys that can be used to break the cryptosystem. In the proposed audio encryption scheme, a 128-bit secret key is used, providing 2^{128} different combinations (approximately 3.40×10^{38}), which is a practically large key space to protect the system from brute-force attacks.

4.6 Time Analysis

To evaluate the performance of the proposed audio encryption scheme, we analyzed the encryption speed on an Intel Core i3 CPU at 2.53 GHz with 1.86 GB of RAM using MATLAB R2014b. The average

encryption and decryption times for different audio files are presented in Table 8. For an audio signal with a 5-second duration, a sampling rate of 8000 Hz, and 8 bits per sample, the encryption process takes only 0.046 seconds on average. Therefore, the proposed method is suitable for real-time systems.

Table 8: Encryption / decryption speeds for the proposed scheme (in seconds)

File name	Type	Samples No	Encryption	Decryption
female_male	8 bits	40000	0.062	0.078
male	8 bits	40000	0.046	0.046
female	8 bits	24000	0.015	0.014
chimes	8 bits	1146600	0.431	0.125
music	8 bits	1940400	0.687	0.188
guitar	8 bits	661500	0.125	0.065

4.7 Comparison with Other Works

In this section, we compare our scheme with previous works, focusing on metrics such as NPCR, UACI, correlation coefficient, information entropy, and PSNR.

Table 9: PSNR comparison between our scheme and other works

Scheme	PSNR
Proposed Scheme	8.6
Mahmood Z., Zinah J.	-6.8
M.Y. Mohamed [9]	27
Krasimir Kordov [15]	1.4524 dB
Osama S. and Hala S. [8]	7-8

Table 10: Entropy comparison between our scheme and other works

Scheme	Entropy
Proposed Scheme	7.9967
Mahmood Z., Zinah J.	14
M.Y. Mohamed [9]	7.99995
Yussra Majid, Nada M. [7]	7.9861

Table 11: NPCR & UACI comparison between our scheme and other works

Scheme	NPCR	UACI
Proposed Scheme	99.96	33.43
M.Y. Mohamed [9]	99.6	36.3
F.J. Farsana and	99.99	33.34
Osama S. and Hala S. [8]	99.75	2912

Table 12: Correlation coefficient comparison between our scheme and other works

Scheme	CC
Proposed Scheme	0.0005
Emad, Nagy W. et al [11]	0.01
Samah M. H. et al[12]	0.0017
Mahmood Z., Zinah J.	0.0076
M.Y. Mohamed Parvees	-0.0012
Krasimir Kordov [15]	0.004
F.J. Farsana and V.R.	0.0014
Yahia, Mohamad et al	0.005
Osama S. and Hala S.	0.004
Bushra W. Hussein Al Zahawy [42]	0.0043

5 Conclusion

In this paper, we proposed a secure audio encryption scheme based on chaotic maps. The experiments conducted, along with comparisons to other existing audio encryption schemes, demonstrate the efficiency and security of the proposed approach. The key space of our scheme, 2^{128} , makes brute-force attacks impractical. The entropy values of the encrypted audio signals exceed 7.99, and the correlation coefficient values are close to zero, indicating a near-random uniform distribution of the encrypted audio signals. The peak signal-to-noise ratio (PSNR) of the encrypted audio signals reached 7 dB. Additionally, the proposed algorithm is highly sensitive to both the plaintext and the secret key, with NPCR values exceeding 99.90% and UACI values at 33.46%. These results confirm the effectiveness and security of our scheme.

REFERENCES

1. Ibrahim, M. K., & Hamood, L. A. (2018). Video encryption based on chaotic system and stream cipher. *International Journal of Information and Communications Technology (IJICT)*, 1(2).
2. Li, S., Zheng, X., Mou, X., & Cai, Y. (2002). Chaotic encryption scheme for real-time digital video. *In Proceedings of SPIE 4666: Real-Time Imaging VI* (pp. 149–160). SPIE.
3. Kezia, H., & Sudha, G. F. (2008). Encryption of digital video based on Lorenz chaotic system. In *Proceedings of the 16th International Conference on Advanced Computing and Communications* (pp. 40–45). IEEE Computer Society Press.
4. Eid, M. M., El Kenawy, E. S. M., & Ibrahi, A. (2021). A new hybrid video encryption technique based on chaos cryptography. *Journal of Computer Science and Information Systems*, 2.
5. Abdelfatah, R. I., Nasr, M. E., & Alsharqawy, M. A. (2020). Encryption for multimedia based on chaotic map: Several scenarios. *Multimedia Tools and Applications*, 79, 19717–19738.
6. Yasser, I., Mohamed, M. A., Samra, A. S., & Khalifa, F. (2020). A chaotic-based encryption/decryption framework for secure multimedia communications. *Entropy*, 22, Article 1253.
7. Hameed, Y. M., & Ali, N. H. M. (2018). An efficient audio encryption based on chaotic logistic map with 3D matrix. *Journal of Theoretical and Applied Information Technology*, 96(16), 5142–5152.
8. Faragallah, O. S., & El-Sayed, H. S. (2021). Secure opto-audio cryptosystem using XORing mask and Hartley transform. *IEEE Access*, 9.
9. Mohamed Parvees, M. Y. (2018). Audio encryption: A chaos-based data byte scrambling technique. *International Journal of Applied Systemic Studies*, 8(1).
10. Li, C., Luo, G., Qin, K., & Li, C. (2017). Chaotic image encryption schemes: A review. *Advances in Engineering Research*, 86.

11. Mosa, E., Messiha, N. W., Zahran, O., & Abd El-Samie, F. E. (2011). Chaotic encryption of speech signals. *International Journal of Speech Technology*, 14, 285–296.
12. Alwahbani, S. M. H., & Bashier, E. B. M. (2013). Speech scrambling based on chaotic maps and one time pad. In *Proceedings of the International Conference on Computing, Electrical and Electronic Engineering (ICCEEE)*.
13. Faragallah, O. S., Elshakankiry, O. A., Abd El-Samie, F. E., El-Sayed, H. S., Elshamy, M. M., & El-Rabaie, E. S. M. (2015). Efficient audio cryptosystem based on chaotic maps and double random phase encoding. *International Journal of Speech Technology*, 18, 619–631.
14. Abdullah, M. Z., & Khaleefah, Z. J. (2017). Design a hybrid cryptosystem based chaos and sharing for digital audio. **Iraqi Journal of Computers, Communication and Control & System Engineering**, 17, 59–70.
15. Kordov, K. (2019). A novel audio encryption algorithm with permutation-substitution architecture. *Electronics*, 8, Article 530.
16. Farsana, F. J., & Devi, V. R. (2023). An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. *Applied Computing and Informatics*, 19(3–4), 239–264. <https://doi.org/10.1016/j.aci.2019.10.001>
17. Alemami, Y., Mohamed, M. A., Atiewi, S., & Mamat, M. (2020). Speech encryption by multiple chaotic maps with fast Fourier transform. *International Journal of Electrical and Computer Engineering*, 10(6), 5658–5664.
18. Geisel, T., & Fairén, V. (1984). Statistical properties of chaos in Chebyshev maps. **Physics Letters A**, 105(6), 263–266.
19. Alligood, K. T., Sauer, T. D., & Yorke, J. A. (1996). *Chaos: An introduction to dynamical systems*. Springer-Verlag.
20. Khan, J., Ahmad, J., & Hwang, S. O. (2015). An efficient image encryption scheme based on Henon map, skew tent map and S-Box. In *Proceedings of the International Conference on Modeling, Simulation, and Applied Optimization (ICMSAO)* (pp. 1–6).

21. Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications in Mathematical Physics*, 50, 69–77.
22. Lian, S., Sun, J., & Wang, Z. (2005). A block cipher based on a suitable use of chaotic standard map. *Chaos, Solitons & Fractals*, 26, 17–29.
23. Chen, J. X., Zhu, Z. L., Zhang, L. B., Fu, C., & Yu, H. (2014). An efficient diffusion scheme for chaos-based digital image encryption. *The Scientific World Journal*, 2014, Article 427349.
24. Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences*, 20(2), 130–141.
25. Ramadan, N., Ahmed, H. E. H., Elkhamy, S. E., & Abd El-Samie, F. E. (2016). Chaos-based image encryption using an improved quadratic chaotic map. *American Journal of Signal Processing*, 6(1), 1–13.
26. Song, X. H., Wang, H. Q., Venegas-Andraca, S. E., & Abd El-Latif, A. A. (2020). Quantum video encryption based on qubit-planes controlled-XOR operations and improved logistic map. *Physica A: Statistical Mechanics and Its Applications*, 573, Article 122660.
27. Wu, Y., Noonan, J. P., & Agaian, S. (2011). NPCR and UACI randomness tests for image encryption. *Journal of Selected Areas in Telecommunications (JSAT)*, 1(2), 31–38.
28. Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, 8(6), 1259–1284.
29. 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.
30. Patidar, V., Pareek, N. K., & Sud, K. K. (2009). A new substitution-diffusion based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation*, 14(7), 3056–3075.
31. Mondal, B., Singh, S., & Kumar, P. (2018). A chaotic permutation and diffusion based image encryption algorithm for secure communications. *Springer Science+Business Media*.

32. Qayyum, A., Ahmad, J., Boulila, W., & Rubaiee, S. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access*, 8, 140876–140895.
33. Diffie, W., & Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6), 644–654.
34. Yu, X. Y., Zhang, J., Ren, H. E., Xu, G. S., & Luo, X. Y. (2006). Chaotic image scrambling algorithm based on S-DES. *Journal of Physics: Conference Series*, 48, 349–353.
35. Sud, V., Pareek, K. K., & Patidar, N. K. (2006). Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9), 926–934.
36. Akhshani, A., Akhavan, A., Lim, S. C., & Hassan, Z. (2012). An image encryption scheme based on quantum logistic map. *Communications in Nonlinear Science and Numerical Simulation*, 17(12), 4653–4661.
37. Tian, P., & Li, D. (2013). A novel image encryption using Arnold cat map. *International Journal of Security and Its Applications*, 7(5).
38. Parker, T. S., & Chua, L. (1995). Chaos: A tutorial for engineers. *Proceedings of the IEEE*, 75(8), 982–1008.
39. Dachsel, F., & Schwarz, W. (2001). Chaos and cryptography. *IEEE Transactions on Circuits and Systems*, 48, 498–509.
40. Wu, C. W., & Rulkov, N. F. (1993). Studying chaos via 1-D maps—A tutorial. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, 40(10), 707–721.
41. Qayyum, A. (2020). Chaos-based confusion and diffusion of image pixels using dynamic substitution. *IEEE Access*, 8.
42. Al Zahawy, B. W. H. (2025). Merging the International Data Encryption Algorithm and Digital Chaotic Scrambler (DCS) to enhance audio security. *Engineering, Technology & Applied Science Research*, 15(5).
43. Gebereselassie, S. A., Sahoo, S., & Tiwari, A. (2023). A secured audio encryption algorithm based on Gauss and Henon chaotic

- maps. In *2023 International Conference on Computer, Electronics & Electrical Engineering & Their Applications (IC2E3)*. IEEE. <https://doi.org/10.1109/IC2E357697.2023.10262456>
44. Jawad, A. K., Karimi, G., & Radmalekshahi, M. (2024). A novel Lorenz-Rossler-Chan (LRC) algorithm for efficient chaos-based voice encryption. *In 2024 3rd International Conference on Advances in Engineering Science and Technology* (pp. 114–119). IEEE. <https://doi.org/10.1109/AEST63017.2024.10959812>
45. Maity, A., & Dhara, B. C. (2024). An audio encryption scheme based on empirical mode decomposition and 2D cosine logistic map. *IEEE Latin America Transactions*, 22(4), 267–275. <https://doi.org/10.1109/TLA.2024.10472959>
46. Farsana, F. J., Devi, V. R., & Gopakumar, K. (2023). An audio encryption scheme based on Fast Walsh Hadamard Transform and mixed chaotic keystreams. *Applied Computing and Informatics*, 19(3–4), 239–264. <https://doi.org/10.1016/j.aci.2019.10.001>