Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Encryption of Audio Signals by employing the Elzaki Transformation and the Lorenz Chaotic System

Shadman R. Kareem

shadman.rahman@koyauniversity.org

Koya University

Research Article

Keywords: Cryptography, Lorenz Chaotic System, Elzaki Transformations, Audio Encryptions

Posted Date: September 14th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-7190186/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Encryption of Audio Signals by employing the Elzaki Transformation and the Lorenz Chaotic System

Shadman R. Kareem [1,2]

Department of Mathematics, Faculty of Science and Health, Koya University, Kurdistan Region – F.R. Iraq
Cybersecurity Department, Tishk International University, Kurdistan Region, Iraq.

shadman.rahman@koyauniversity.org

0000-0002-7982-156X

Abstract

Protecting multimedia communications, particularly audio data, is a significant challenge in information security. Audio signals possess strong time-based correlations and floating-point structures, rendering conventional encryption methods ineffective. A wide variety of cryptographic techniques have been purposefully developed to maintain the confidentiality and security of audio data in digital communications. The present research introduces a unique chaos-based audio encryption algorithm that combines the Elzaki transformation along with the Lorenz chaotic system to improve confidentiality and adaptation. The Lorenz chaotic system improves initial key generation; however, the Kushare transformation enhances security. The proposed technique sets off by scrambling the audio signal, utilising the Lorenz chaotic system to produce a random key that is XORed with the audio pixels for pre-encryption. This step is followed by a second layer of encryption that uses a mix of hyperbolic Maclaurin series expansion and the Elzaki transform, with keys created through modular arithmetic. Decryption is performed through the inverse Elzaki transform and XORs the cypher pixels alongside the key generator. Our multi-layered proposed method design provides considerable resiliency to assaults. Experimental validation confirms the efficacy of the indicated approach in preserving audio data while maintaining efficiency and security. Comparisons between the techniques are conducted based on several performance measures, including entropy analysis, spectrogram plotting, and correlation coefficients. Theoretical analysis and simulation indicate the efficacy of the proposed approach and confirm that this method is suitable for actual audio encryption. Moreover, the security inquiry reveals that the provided audio encryption approach provides an extra layer of security.

KEY WORDS: Cryptography, Lorenz Chaotic System, Elzaki Transformations, Audio Encryptions.

1. Introduction

Individuals worldwide are currently required to transmit large amounts of digital data over networks that lack security. Transmitting private and personal images and audio over an unsecured network always exposes them to the potential for unauthorized access, illustrating the critical importance of addressing security considerations when exchanging information. Cryptography, one of the oldest and most efficient techniques for secure information transmission, has a long history. It preserves confidentiality and integrity by employing many different encryption techniques.

Conventional encryption methods, notably AES, DES, and RSA, are deemed insufficient for A encryption due to their higher processing time requirements. Also, as multimedia data grows, there is often a strong connection between

pixels, making these encryption methods not good enough for efficient data transfer. To address these challenges, various audio techniques for encryption have been indicated, with just a few of them based on transformation [1], [2], and applying discrete wavelet transforms. In addition, in [3] , this study investigates an innovative approach for encrypting audio that utilises the combined capabilities of Laplace transforms and hyperbolic functions. The suggested approach offers an original technique for converting audio data into a mathematically obscured format, rendering it unintelligible to anybody without the decryption key. Digital content often uses non-traditional encryption techniques to improve both speed and security. These unconventional methods include various techniques for altering and restructuring data, with some relying on visual alterations.

The combined use of chaos theory with encryption in current technologies presents a new framework for ensuring data security. Researchers are extremely interested in these improvements as they attempt to create innovative methods for cryptography. The unique aspects of chaos theory have resulted in its extensive use in the encryption of various data types. Right now, many chaos-based encryption techniques are being proposed. In [4] This study presents a novel encryption technique that uses a chaotic standard map that performs a diffusion effect in the replacement phase. Utilizes the basic features of chaos, including its sensitivity to initial conditions and pseudo-randomness, to provide safe encryption. in [5] This research presents a novel technique for picture encryption that employs an advanced Lorenz system to boost both the security and efficiency of the encryption process. This method enhances the nonlinear kinetic complexity and ergodicity of the Lorenz system. We use the Lorenz system to provide key streams for executing diffusion via XOR operations as a pre-encryption method, hence enhancing security. Chaotic system has several benefits, such as a vast array of potential keys and a significant level of security. Considering its inherent stochasticity and indeterminacy, chaos theory is often used in the encryption of audio and visual data.

While chaos-based encryption creates extremely random numbers, it is inherently complicated and unpredictable, which has attracted a lot of curiosity in its application in recent years [6]. Studies encourage the use of chaotic systems as sources of entropy for producing true random numbers in both discrete and continuous time. Identical random number generators based on chaos are preferred according to scholars. An adequate supply of random numbers is essential for a secure communication system and multiple cryptographic applications. The security and reliability of these systems are influenced by the generated random numbers' accuracy and unpredictable characteristics [7].

The proposed Lorenz approach is an increasingly common option for designing chaotic systems with random number generators requiring an entropy point of deduction. A decentralized three-dimensional system with an odd attractor, the fact that changes depending on initial conditions is referred to as the Lorenz system, indicates how certain patterns of differential equations alongside certain parameters can result from chaotic attitude. [8]. Multiple research efforts have applied the Lorenz system to various cryptographic applications. The standard form has been adopted in the design of built-on hardware true random number generators, while discrete-time modifications have been carried out on field-programmable gate arrays (FPGAs) for flexible chaotic pseudorandom number generation. Improved iterations regarding the Lorenz system have been suggested to enhance image encryption effectiveness [11]. The Lorenz system, according to its intrinsic complexity and flexibility, serves as an effective mechanism for cryptographic purposes, encompassed by image encryption [12], initial value uniformity in circuit executions [13], and secure unpredictability bit generation by means of designed initial condition selection [14].

The latest study proposes effective encryption methods that incorporate proficient image processing and use powerful new chaotic systems to generate a random key, which is essential for the encryption process. However, there are

existing cryptographic methodologies. This integrated approach significantly improves security and efficiency, rendering it perfect for real-time applications against different kinds of attack systems that need confidential information transfer.

The study [15] proposes a new image encryption technique that combines chaos theory with a convolutional neural network to enhance both security and complexity. In [16], the encryption is made better by using the 2D chaotic Arnold transform together with public key RSA, which mixes up pixel positions before using asymmetric Additionally, [17] offers an audio encryption methodology that utilises the chaotic 2D Hénon map and wavelet transformations to ensure efficient and secure signal preservation. Th recommended approach leverages the lifting wavelet transform to decompose the audio signal into multiple frequency components, resulting in the enhanced effectiveness and robustness associated with the encryption process. Following that, we use the chaotic nature of the Hénon map to encode and influence data.

The Elzaki transform, an innovative family of integral transforms comparable to the Laplace and Fourier transforms, indicates a beneficial tool for resolving differential and integral equations [18, 19]. Named in honour of mathematician Taha Elzaki, it has garnered recognition for its extensive application spanning several fields, including mathematics and engineering challenges, notably in signal processing. Recently, its ability to transfer across domains has been employed in cryptography, emphasising the potential for safe data transformation and encryption. In the context of [20], authors propose an innovative image encryption technique that applies the Elzaki transform as a confusion mechanism, coupled with a Maclaurin series coefficient expansion for improving execution. The encryption procedure involves applying a power series of hyperbolic functions in conjunction with the Elzaki transform, while decryption is accomplished through the inverse Elzaki transform. In a similar manner in this study I implement the Elzaki transform for audio encryption to enhance the effectiveness of encryption systems through transforming audio signals into an alternative representation contingent on their mathematical features. I develop an innovative cryptography method that integrates a chaotic system coupled with the Elzaki transform to boost security and efficiency in general. First, the technique encrypts the audio data with a key generated as a solution of the Lorenz system to perform confusion to obscure the relationship between plaintext and ciphertext with a bit XOR operation, then represents the result as a vector, and then employs the inherently chaotic and nonlinear mapping properties of the Lorenz system to generate unpredictable key sequences. The second part of the algorithm tries to get around this problem by using the Elzaki transform, along with a replacement method made possible by the expansion of Maclaurin series coefficients. This method entails encrypting the picture with an unending sequence of hyperbolic functions. The incorporation of the Elzaki transformation in that manner considerably augments the complexity and robustness of the encryption method, guaranteeing enhanced security for the audio data.

Lorenz Chaotic System

The Lorenz system, first introduced by *Edward Lorenz* in 1963, is a classic example of a chaotic system characterised by sensitive dependency on initial conditions. This system has found applications beyond its original context in atmospheric convection, including cryptography and secure communication. In this study, we explore the use of the Lorenz chaotic system for encrypting audio signals. The following set of nonlinear ordinary differential equations describes the Lorenz system:

$$\begin{aligned} \dot{x} &= \sigma\,(y - x), \\ \dot{y} &= x(\rho - z) - y, \\ \dot{z} &= xy - \beta z. \end{aligned} \tag{2}$$

where $x, y,$ and z are the state variables, and $\sigma, \rho,$ and β are the parameters of the system with the initial condition $(x_0, y_0, z_0) = (0.02, 0.02, 0.02)$. The behaviour of the Lorenz system exhibits a strange attractor in phase space, which is highly sensitive to initial conditions and shows chaotic behaviour; see the Figures (1-5). For more detail, see the reference [3].

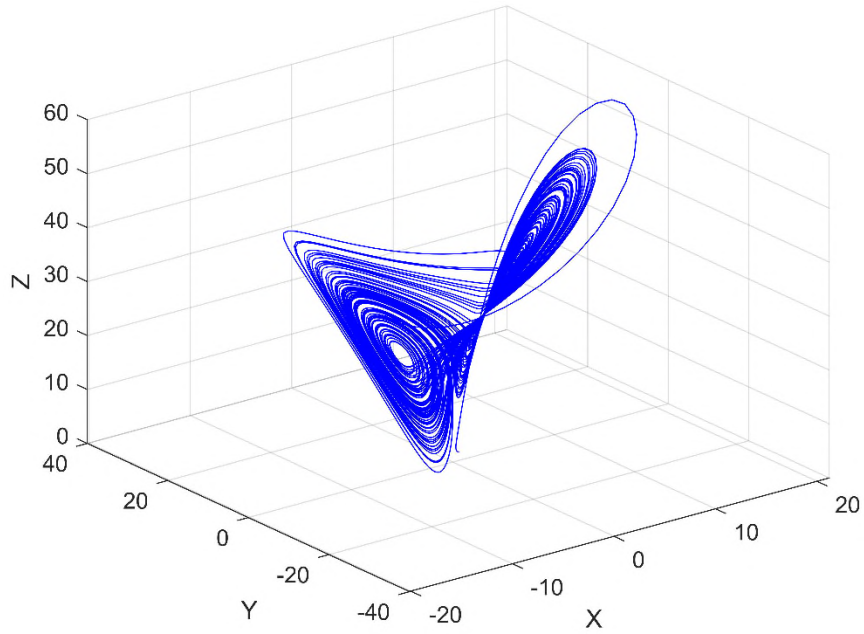


Figure 1: 3D phase portrait for the Lorenz chaotic system.

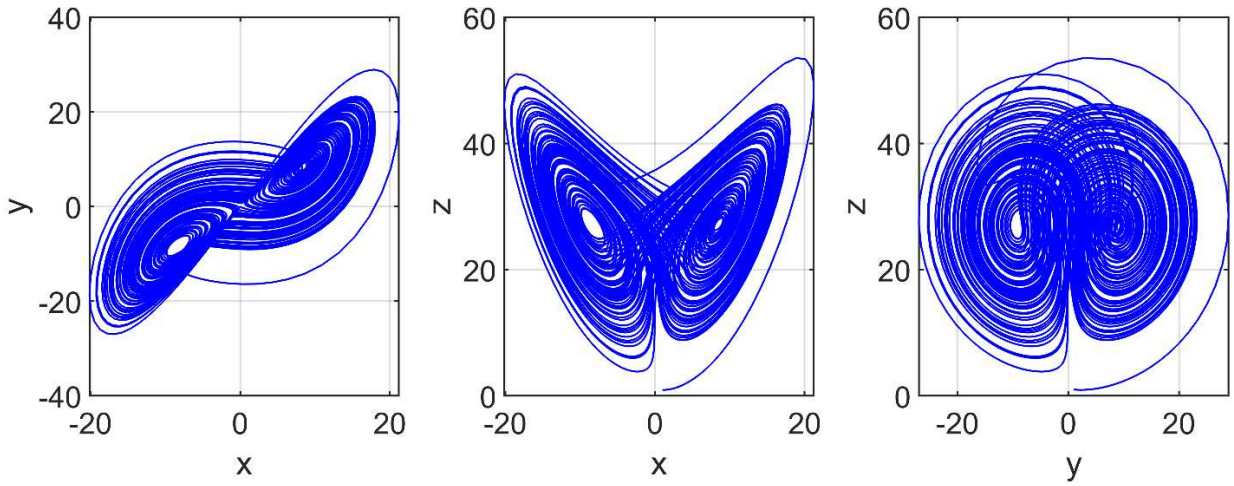


Figure 2: 2D phase portrait of the Lorenz chaotic system.

The chaotic nature of the Lorenz system makes it suitable for cryptography, particularly audio encryption. The Lorenz system is excellent for audio encryption because it is sensitive to initial conditions. This means that even small changes

in the starting parameters can have big effects on the outputs, as shown in Figures 3–5. This unique feature provides a obstruction for unauthorised parties seeking to replicate a specific decryption without key despite having a thorough understanding of the original conditions. The system's solution is chaotic and missing discernible patterns, consequently enhancing security. Moreover, the system's extremely nonlinear construction prevented the prediction about its output employing straightforward linear transformations, accordingly enhancing security.

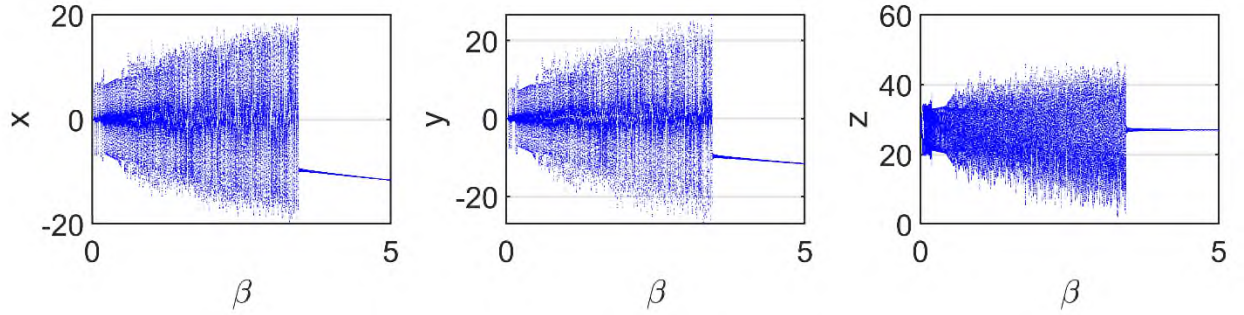


Figure 3: Bifurcation diagram for the Lorenz system, where $\sigma = 10$, $\rho = 28$, and $\beta \in [0, 5]$.

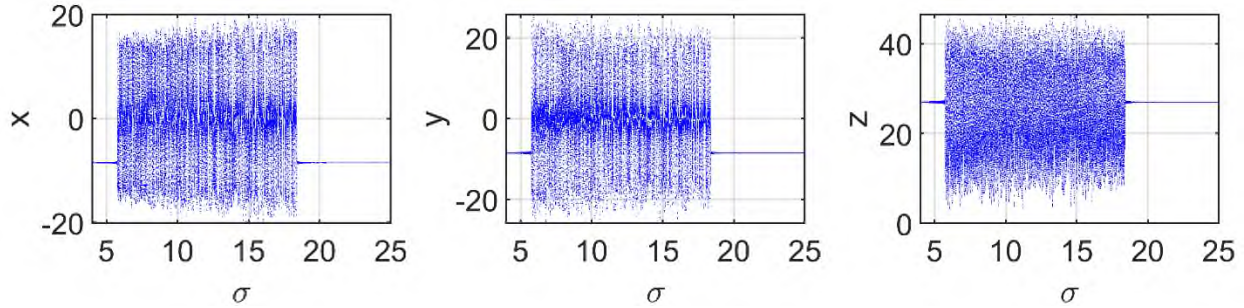


Figure 4: Bifurcation diagram for the Lorenz system, where $\beta = 8/3$, $\rho = 28$, and $\sigma \in [4, 25]$.

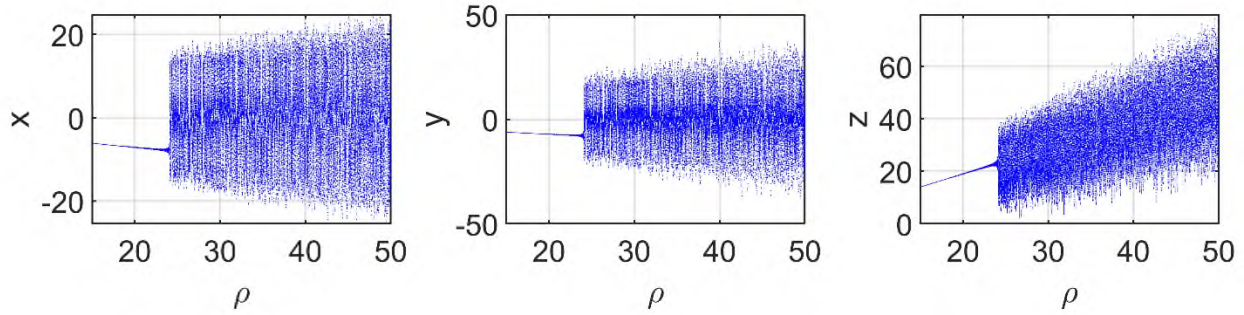


Figure 5: Bifurcation diagram for the Lorenz system, where $\sigma = 10$, $\beta = 8/3$, and $\rho \in [15, 50]$.

2. The Elzaki Transform

The Elzaki transform, initially proposed by *Tarig M. Elzaki* in his work to solve differential equations in 2011, then later became an essential tool for applied mathematics and engineering attributable to its powerful transformation capabilities, particularly regarding signal processing and encryption [18]. This work exploits these capabilities to encrypt audio data areas, exhibiting the transform's adaptability in addressing complicated mathematical and technical issues. The application of it in audio encryption underscores its versatility and efficacy in improving signal processing and security in real-time scenarios.

The specified functions through set A are considered as follows:

$$A = \left\{ f(t): \exists M, k_1, k_2 > 0, |f(t)| < Me^{\frac{|t|}{k_j}}, if\ t \in (-1)^j \times [0, \infty) \right\},$$

For a particular function in the set, M must have a finite value, but k_1 and k_2 might be either finite or infinite. The mathematical explanation of the Elzaki transformation is provided through the following integral manner:

$$E[f(t)] = T(s) = s \int_0^{\infty} f(t) e^{\frac{-t}{s}} dt\,, k_1 \leq s \leq k_2, t \geq 0. \qquad (1)$$

This document illustrates the Elzaki transformation as well as its inverse for numerous fundamental functions.

- $E(k) = ks^2$ where a is constant.
- $E(t^m) = m!\, s^{m+2}$,
- $E^{-1}(s^2) = 1$,
- $E^{-1}(s^{m+2}) = t^n/m!$.

3. Proposed Method

The following stages outline the procedural steps that enhance data security and privacy in the proposed hybrid mode of the Elzaki transformation and the Lorenz Chaotic System, which are utilised in cryptography and encryption technology.

4.1 Encryption Algorithm

To construct the Lorenz chaotic key, begin by setting up the Lorenz system (2) with specified parameters, $\sigma = 10$, $\rho = 28$, and $\beta = 8/3$, as well as beginning with the initial condition $(x_0, y_0, z_0) = (0.02, 0.02, 0.02)$. Then, we employ Euler's technique for finding the numerical integration to solve the Lorenz differential equations over a certain number of time steps $dt = 0.01$. The time series data for $x, y,$ and z will display chaotic behavior. These variables are usually denoted as x-component, y-component, and z-component of the Lorenz Chaotic Key. The diagram in Figure (6) depicts the successive processes of the proposed audio encryption method.

We consider the Maclaurin series of $t^2 e^{at}$ to be:

$$t^2 e^{at} = \sum_{n=0}^{\infty} \frac{a^n t^{n+2}}{n!} \qquad (3)$$

For simulation trials, the proposed approach uses an "audio.wav" file as the carrier input. We executed the proposed methodology using MATLAB R2021a, employing two audio files (.wav) as input data. Figure 7 illustrates the behavior of the technique during the encryption and decryption operations. The MATLAB function [$\boldsymbol{X}$,Fs]=audioread('audio1.wav') retrieves the vector $\boldsymbol{X}$, which represents our sample voice's amplitude values per second. This vector contains the message that requires encryption.

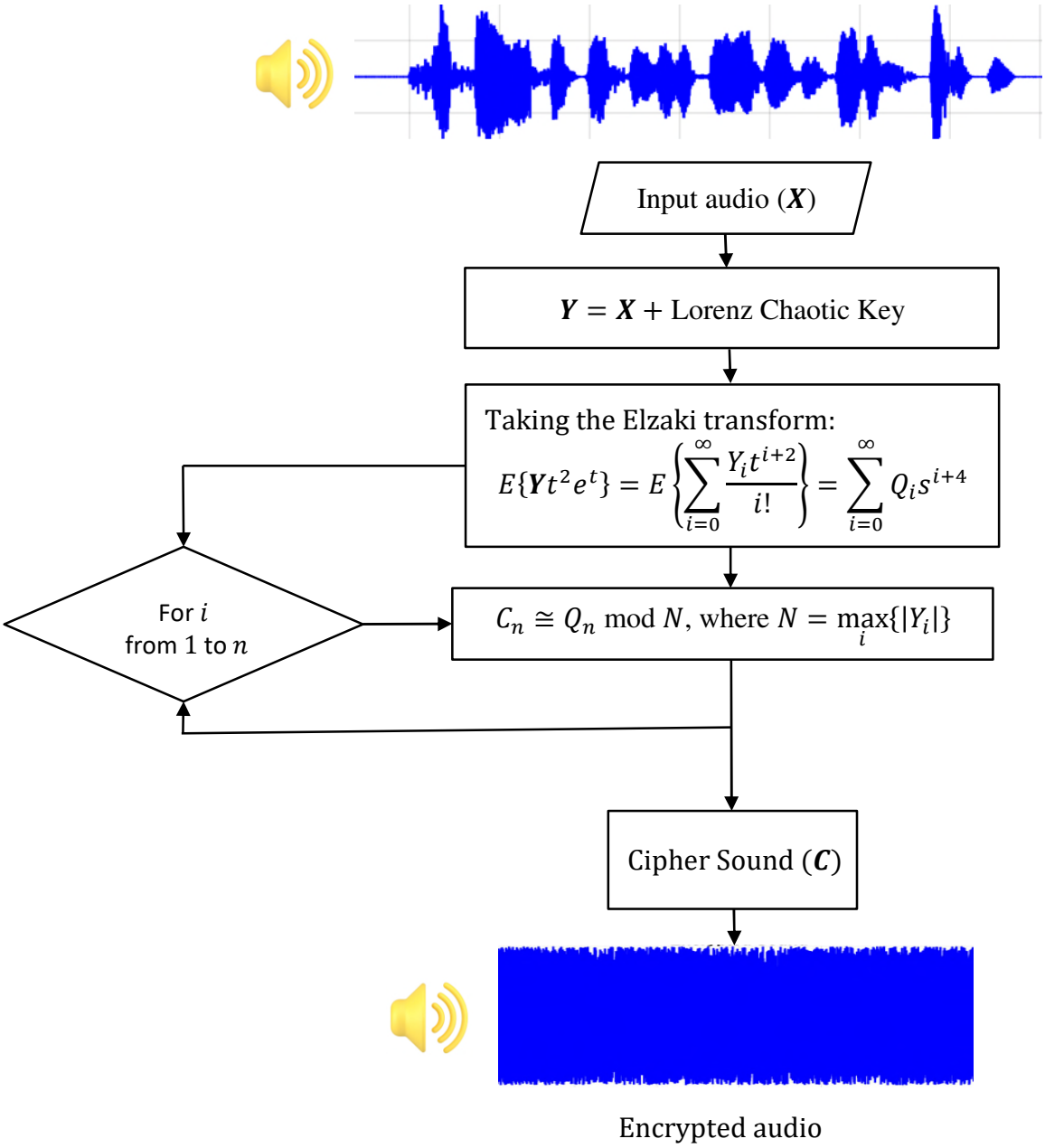


Figure 6: Diagram illustrating the sequence of steps in the audio encryption method being proposed.

Step 1: Inputting and reading audio data as a vector $\boldsymbol{X}$.

Step 2: The pre-encoded audio $\boldsymbol{Y} = \boldsymbol{X}$ + Lorenz Chaotic Key.

Step 3: Make the entries Y_n of the vector $\boldsymbol{Y}$ for the audio data as the coefficients of the Maclaurin series of t^2e^t as follows:

$$\boldsymbol{Y}t^2e^t = \sum_{n=0}^{\infty}\frac{Y_n}{n!}t^{n+2}, \text{ where } X_n = 0, \text{ for } n > \text{length}(\boldsymbol{Y}) . \quad (4)$$

Step 4: Utilizing the Elzaki transformation for Equation (4), we derive the transformed expression, as follows:

$$\mathrm{E}\left[\sum_{n=0}^{\infty}\frac{Y_n}{n!}t^{n+2}\right] = s\int_0^{\infty}\sum_{n=0}^{\infty}\frac{Y_n}{n!}t^{n+2}e^{\frac{-t}{s}}dt = \sum_{\mathrm{n=0}}^{\infty}Y_n(n^2+3n+2)s^{j+4} = \sum_{n=0}^{\infty}Q_n s^{j+4}, \quad (5)$$

where $Q_n = Y_n(n^2+3n+2)$, for $n = 0,1,2,\ldots,\text{length}(\boldsymbol{Y})$.

Step 5: Find C_n such that $C_n \cong Q_n \mod N$, where $N = \max_i\{|Y_i|\}$, for $n = 0,1,2,\dots,\text{length}(\boldsymbol{Y})$. Then, the cipher audio becomes $\boldsymbol{C}$.

Note that, the pre-encoded audio $\boldsymbol{Y}$ in terms of n, for $n = 0,1,2,\dots,\text{length}(\boldsymbol{Y})$, under the Elzaki transform of $\boldsymbol{Y}t^2e^t$ can be converted to cipher audio C, where the components of this matrix are given by

$$C_n = Q_n - NK_n, \tag{6}$$

and

$$Q_n = (2n+1)Y_n, \tag{7}$$

with the modular-key

$$K_n = \frac{Q_n - C_n}{N}, \tag{8}$$

4.2 Decryption Algorithm

Decryption is the inverse procedure of encryption. During the decryption process, the input consists of the encrypted audio, which is represented as a vector denoted $\boldsymbol{C}$. We use two confidential keys: the Lorenz Chaotic Key's x-component, y-component, and z-component, as well as the modular key (represented as $\boldsymbol{K}$ in Equation (8)). We use these keys throughout the procedure, ultimately leading to the audio decryption. The decryption procedure includes a series of sequential processes with the objective of recovering the original audio from its encrypted state.

Step 1: Choose the encoded audio.

Step 2: Find Q_n such that $Q_n \cong C_n \mod N$, for $n = 0,1,2,\dots,\text{length}(\boldsymbol{X})$. Then, make it as the coefficient of the follow series:

$$T(s) = \sum_{n=0}^{\infty} Q_n s^{j+4},. \tag{9}$$

Step 3: Utilizing the Elzaki inverse transformation for Equation (9), we derive the transformed expression, as follows:

$$\mathrm{E}^{-1}\left[\sum_{\mathrm{i}=0}^{\infty} Q_n s^{j+4}\right] = \mathrm{E}^{-1}\left[\sum_{\mathrm{i}=0}^{\infty} Y_n(n^2+3n+2)s^{j+4}\right] = \sum_{n=0}^{\infty}\frac{Y_n}{n!}t^{n+2} = \boldsymbol{Y}t^2e^t, \tag{10}$$

Step 4: The Decrypted audio $\boldsymbol{X} = \boldsymbol{Y} -$ Lorenz Chaotic Key.

4. Results and Simulation Analysis

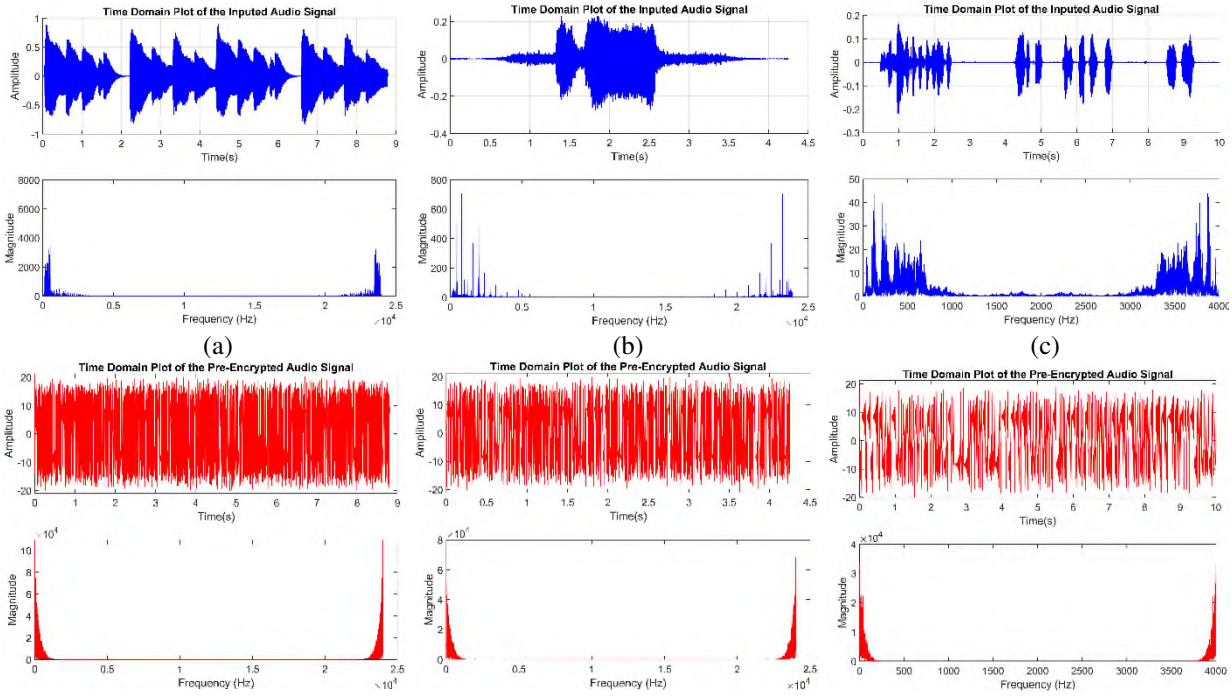
An audio encryption method should be capable of converting any audio into a cipher audio and then returning to the original plain audio during the decryption process. The results of the proposed methodology are presented in Figure 7. We will apply the Lorenz Chaotic key to the original audios, and we will get the pre-encrypted audios for Piano, Car_Horn, and Human, as shown in Figures 7(d), 7(e), and 7(f). After that, we applied the Elzaki transformation to the pre-encrypted audios to get the encrypted audios as shown in Figures 7(g), 7(h) and 7(i). From Figure (7), it is clear that no one can guess anything about the original signal from the encrypted signal. The audio signal, can be recovered exactly (see Figures. 7(j), 7(k) and 7(l)) by using the actual key. However, the original signal cannot be recovered using a slightly modified key. Therefore, the proposed method can properly encrypt and decrypt the audio signals. To analyze the performance of the proposed method, different performance metrics like entropy, mean square

error (MSE), peak signal-to-noise ratio (PSNR), correlation coefficient, histogram analysis, and computational time analysis are used.

We will implement the intended approach using MATLAB R2021a. The implementation occurred on a personal computer system, equipped with an Intel(R) Core (TM) i5-1135G7 CPU running at a clock speed of 2.42 GHz. The processing module has a capacious 1 terabyte optical disc drive and a substantial 8 GB of RAM for enabling effective memory operations. This particular implementation was executed on the Windows 11 operating system.

5.1 Statistical analysis.

We completed several statistical tests regarding the reliability of the proposed cryptographic encryption method. This research presents comprehensive data about the robustness and effectiveness of the encryption technology, as shown in our testing domain. The data analysis evaluates the encryption findings by examining the distribution of audio signal values, their interconnections, and estimating errors by means of mean squared error (MSE) and peak signal-to-noise ratio (PSNR). These tests provide essential data on maintaining the level of audio security and quality throughout encryption and decryption techniques, as well as major insights into the reliability of preserving the encrypted information.



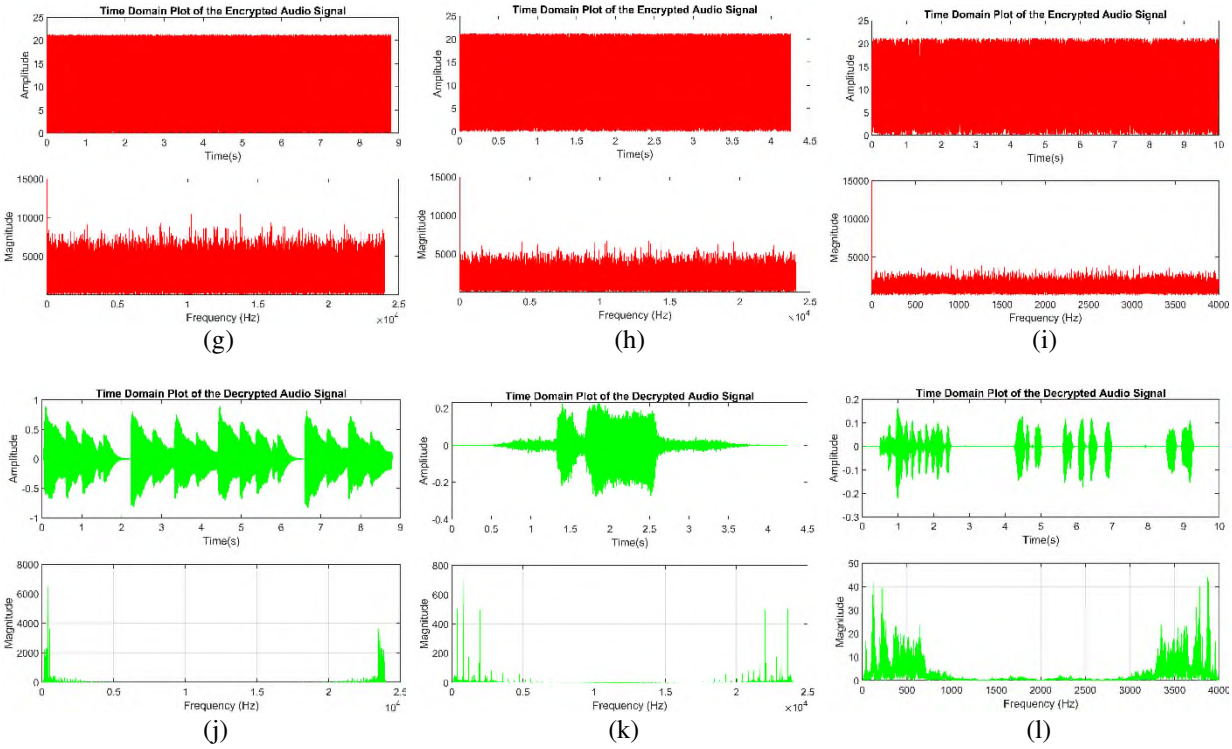
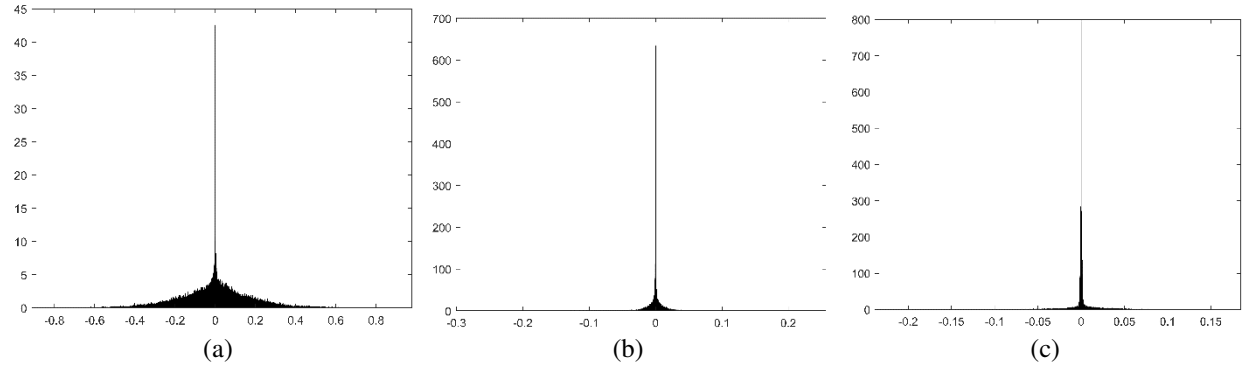


Figure 7: Conclusions regarding audio pre-encryption, encryption, as well as decryption for (a) Piano.wav unprocessed audio; (b) Car_Horn.wav unprocessed audio; (c) Human.wav unprocessed audio; (d) Pre-encrypted Piano.wav; (e) Pre-encrypted Car_Horn.wav; (f) Pre-encrypted Human.wav; (g) Piano.wav encrypted audio; (h) Car_Horn.wav encrypted audio; (i) Encrypted Human.wav; (j) Piano.wav decrypted audio; (k) Car_Horn.wav decrypted audio; (l) Decrypted audio for Human.wav. Then used the x-component of the Lorenz Chaotic Key over (d), (e), and (f), followed by deployed the Elzaki transformation with (g), (h), and (i) immediately following the implementation of the Lorenz Chaotic Key.

5.1.1 Histogram analysis

Figure 8 illustrates a histogram whose services depict the distributions of audio signals at multiple points: pre-encryption, encryption, and decryption. It displays the intensity levels for all considered data, such as Piano.wav (a), Car_Horn.wav (b), and Human.wav (c) in their original, unaltered condition, as well as their pre-encrypted forms using the x-component of the Lorenz Chaotic Key (d, e, f). Likewise, it exhibits the encrypted variants of these audio files (g, h, i) subsequent to the application of the aforementioned Lorenz Chaotic Key and with the Elzaki transformation.



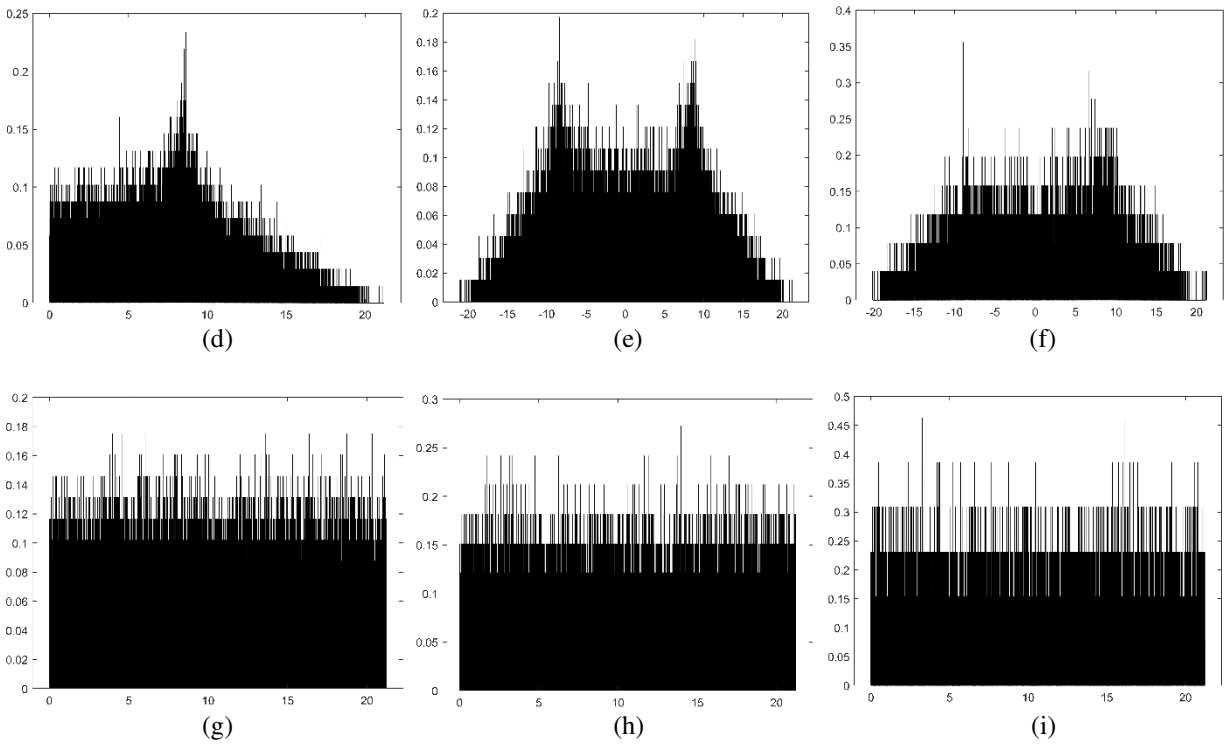


Figure 8: This histogram illustrates the distribution of audio signals at different stages: pre-encryption, encryption, and decryption. It includes the plain audio for Piano.wav (a), Car_Horn.wav (b), and Human.wav (c). Additionally, it displays the pre-encrypted audio for Piano.wav (d), Car_Horn.wav (e), and Human.wav (f) using the x-component of the Lorenz Chaotic Key. Moreover, it shows the encrypted audio for Piano.wav (g), Car_Horn.wav (h), and Human.wav (i) after initially applying the Lorenz Chaotic Key and then employing the Elzaki transformation.

This histogram analysis is critical for understanding how audio signals evolve through the encryption process, particularly concerning the prevention of information leakage. By examining the histograms of plain audio in Figure (8), it becomes evident that the original amplitude levels are preserved. However, the histograms for encrypted audio, also depicted in Figure 8, demonstrate a notable absence of identifiable amplitude patterns, indicating successful encryption.

Ensuring a uniform histogram distribution is paramount for fair energy allocation. Figure (8) shows how the encrypted audio histograms exhibit a smoother and more consistent pattern compared to their plain counterparts. This observation highlights the effectiveness of the proposed encryption approach in bolstering cryptographic security, as evidenced by the enhanced confidentiality of the audio signals.

5.1.2 Correlation Coefficient Analysis

A suitable encryption method should stop the correlation between nearby audio samples. Spreading sample values evenly across the intensity range and ensuring almost no correlation in the encrypted audio can achieve this. Figure 3, with a sample audio clip, illustrates this. The first column shows sample distributions in the plain audio, the second column shows the encrypted audio's correlation patterns, and the third column shows the decrypted audio. The results highlight successful decorrelation in the encrypted audio. Table 1 provides correlation coefficients for some audio samples.

Here's how to compute the correlation coefficient:

$$\rho(X,Y) = \frac{cov(X,Y)}{\sqrt{D(X)}\sqrt{D(Y)}}, \tag{11}$$

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} X_i\,, \bar{Y} = \frac{1}{N}\sum_{i=1}^{N} Y_i,$$

$$D(X) = \frac{1}{N}\sum_{i=1}^{N}(X_i - \bar{X})^2\,, D(Y) = \frac{1}{N}\sum_{i=1}^{N}(Y_i - \bar{Y})^2$$

$$cov(X,Y) = \frac{1}{N}\sum_{i=1}^{N}\big((X_i - \bar{X})(Y_i - \bar{Y})\big),$$

The correlation coefficient values, represented as $\rho(x,y)$, range from -1 to 1. When $\rho(x,y)$ is close to 1, it indicates a strong connection between neighboring pixels. A value of $\rho(X,Y)$ near 0 signifies no correlation, while negative values suggest an inverse or flipped relationship between the series. Correlation analysis of horizontal shift for Piano, Car horn, and Human audio signals at different stages of the encryption process is shown in Figure (9). In Table 1, we display the correlation coefficients for both unencrypted and encrypted audio data. To demonstrate the effectiveness of our proposed method, we performed a comparative assessment using Table 1, with the Piano, Car_horn, and Human audios as our reference [6].

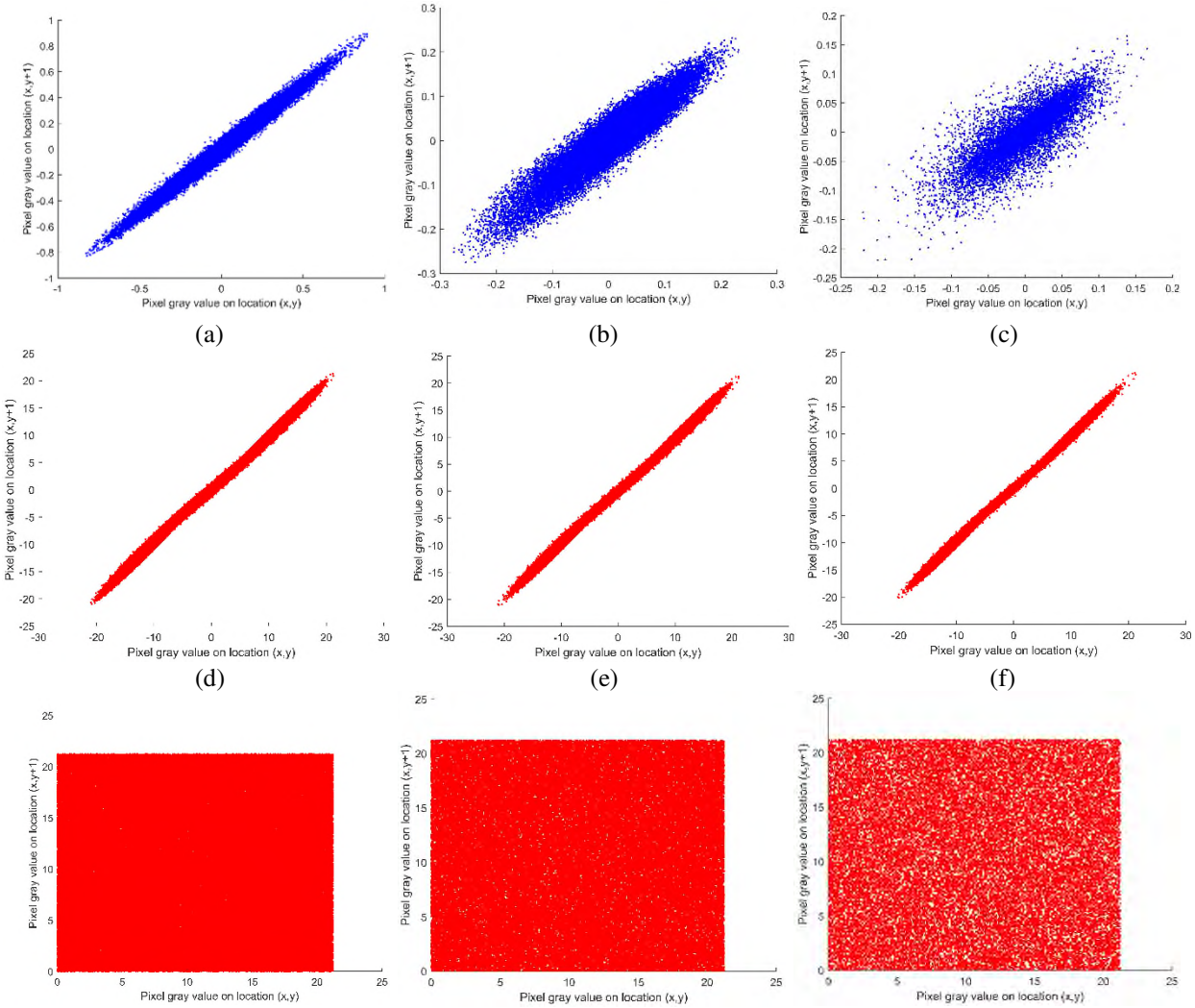


Figure 9: Correlation analysis of horizontal shift for various audio signals at different stages of the encryption process is shown. It includes the original audio for Piano.wav (a), Car_Horn.wav (b), and Human.wav (c). Additionally, it displays the pre-encrypted audio for Piano.wav (d), Car_Horn.wav (e), and Human.wav (f) using the x-component of the Lorenz Chaotic Key. Finally, it presents the fully encrypted audio for Piano.wav (g), Car_Horn.wav (h), and Human.wav (i) after applying the Lorenz Chaotic Key and then the Elzaki transformation.

TABLE 1: Correlation coefficients of horizontal shift for audio signals.

Audios	Components of Lorenz Chaotic Key	Correlation Coefficients of Horizontal Shift		
		Original Audio	Pre-Encrypted Audio	Encrypted Audio
Piano	x	0.9925	0.9987	−0.0014
	y	0.9925	0.9976	−0.0003
	z	0.9925	0.9955	0.0023
Car_Horn	x	0.9334	0.9987	0.0068
	y	0.9334	0.9976	0.0057
	z	0.9334	0.9955	0.0004
Human	x	0.8025	0.9986	−0.0014
	y	0.8025	0.9975	−0.0022
	z	0.8025	0.9954	−0.0025
Ref. [11]		0.9936		-0.1578
Ref. [12]		0.9970		0.0133

Table 1 displays correlation coefficients that illustrate the correlation between horizontally shifted versions of various audio signals (piano, carhorn, and human) across three stages: original audio, pre-encrypted audio, and encrypted audio. The original audio correlation coefficients are consistently high for the audio signals; this indicates a strong relationship between the original audio signals. The pre-encrypted audio also has high correlation coefficients across all audio types and Lorenz components, with values between 0.9954 and 0.9987. This implies that the pre-encryption process preserves the original audio signals' structure. However, the fully encrypted audio correlation coefficients are close to zero, ranging from -0.0025 to 0.0068, showing that encryption effectively removes the correlation between the audio signals and the Lorenz chaotic key components. This disruption means that the encrypted audio appears as noise to the chaotic system, indicating successful encryption that obscures the original signal structure.

TABLE 2: Correlation coefficients for certain audios.

Audios	Components of Lorenz Chaotic Key	Correlation coefficients between original and encrypted audio.	Correlation coefficients between original and decrypted audio.
Piano	x	0.0005	1
	y	-0.0010	1
	z	-0.0015	1
Car_Horn	x	-0.0032	1
	y	-0.0019	1
	z	0.0056	1
Human	x	-0.0026	1
	y	0.0038	1
	z	0.0069	1
Ref. [13]		0.0263	
Ref. [14]		0.0263	
Ref. [15]		0.0119	

Table 2 shows the correlation coefficients between the original and encrypted audio and the original and decrypted audio for different audios with respect to the components of the Lorenz Chaotic Key. The correlation coefficients between the original and encrypted audio are near zero, indicating effective encryption that disrupts the original signal structure. In contrast, the correlation coefficients between the original and decrypted audio are all 1, demonstrating perfect recovery of the original audio after decryption. This highlights the effectiveness of the encryption and decryption processes in maintaining audio integrity while ensuring security. References [21],[22] show a correlation coefficient close to zero between the original audio and the encrypted audio. This ratio is much higher than the near-zero values we saw, which means the encryption is not as good. Reference [23] has a correlation coefficient of 0.0119, which is lower than those in [21],[22], but still higher than the almost-zero values of our proposed method, which can be seen in Table 2. This indicates that our proposed method is more effective at distorting the original audio signal.

.5.2 Spectrogram Plotting

The spectrogram analysis provides a crucial method for examining audio signals, focusing on their frequency distribution over time. Contrasting plaintext and encrypted information reveals insight into the impact of encryption as well as enables the assessment of the indicated audio encryption algorithm's efficiency.

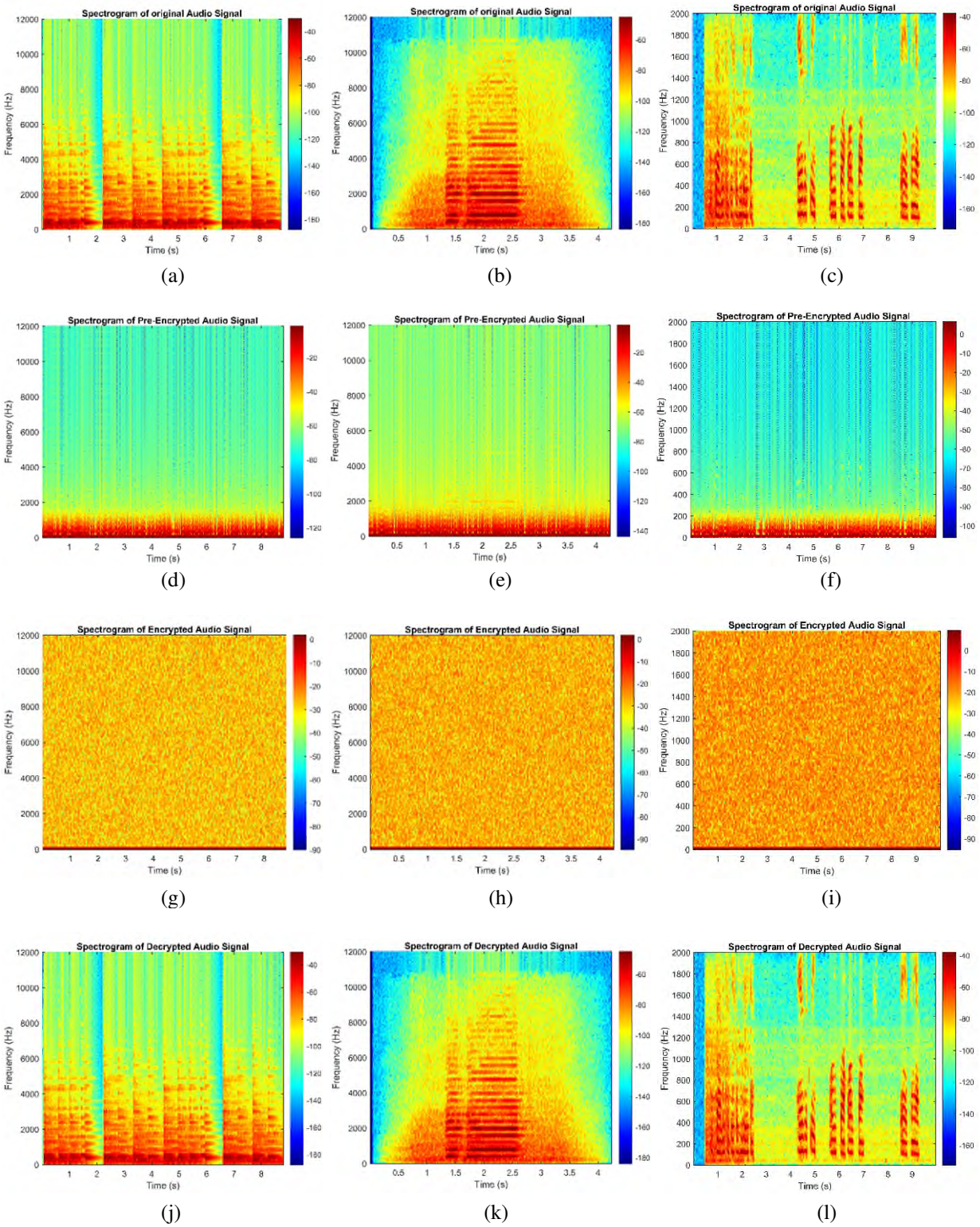


Figure 10: Spectrogram illustrations of audio signals at multiple stages, including pre-encryption, encryption, and decryption. The original audio files include Piano.wav (a), Car_Horn.wav (b), and Human.wav (c). The pre-encrypted audio for Piano.wav (d), Car_Horn.wav (e), and Human.wav (f) is presented as well, employing the x-component of the Lorenz Chaotic Key. Furthermore, it demonstrates the encrypted audio for Piano.wav (g), Car_Horn.wav (h), and Human.wav (i) subsequent with the application utilising the Lorenz Chaotic Key along the Elzaki transformation. Eventually, it exposes the interpreted audio files for Piano.wav (j), Car_Horn.wav (k), and Human.wav (l).

Figure 10 provides spectrum graphs demonstrating audio signals at multiple stages, including pre-encryption, encryption, and decryption. Most original audio files, including Piano.wav (a), Car_Horn.wav (b), and Human.wav (c), are included with their appropriate pre-encrypted versions using the x-component of the Lorenz Chaotic Key (d, e, f). At that point, the encrypted audio files (g, h, i) appear, exhibiting the effects of the Lorenz Chaotic Key and the Elzaki transformation. Several comprehended audio files (j, k, l) are currently displayed. The spectrogram charts offer important clues about the encryption process. The spectrogram charts specifically indicate how the original signals' frequency components are obscured in the encrypted files, which demonstrates the loss of the original signal's frequency content. The outcome proves that the recommended technique performs exceptionally in encryption, shown by the noticeable difference in the spectrogram between unencrypted and encrypted audio files.

4.3 Entropy Analysis

The rule for computing entropy, often referred to as Shannon's entropy, is a fundamental concept in information theory. It quantifies a random variable's uncertainty, or randomness. Here's Shannon's entropy rule [3]:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log_2 P(x_i),$$

where function $H(X)$ is perform indicates the entropy of the random variable X, $P(x_i)$ indicates the probability of the occurrence of x_i and n symbolizes the total number of potential occurrences. Shannon's entropy attempts to provide a robust instrument for measuring uncertainty and unpredictability spanning various erea such as information theory, cryptography, and data analysis. It offers the basis for learning about and evaluating the qualities of random variables and probability distributions.

TABLE 3: Information entropy analysis.

Audios	Original Audio	Encrypted Audio	Decrypted Audio
Piano	14.2966	17.6896	14.2966
Car_Horn	10.975	16.6375	10.975
Human	9.6897	15.2877	9.6897

In Table 3 the information entropy analysis of both the original and encrypted audio is presented, utilizing components X, Y, and Z of the Lorenz chaotic system's key sequence when combined with the Elzaki transformation. The information entropy is a technique for measuring the randomness or unpredictability of data. Further, it is revealed that for piano, car horn, and human audio, the initial entropy values substantially rise post-encryption among all components. The considerable rise in entropy from the original sound to the encrypted sound implies that the encryption process successfully provides randomness and predictability to the data, which is beneficial for safe encryption. In entropy quantity measurements for both stages of encrypted and decrypted sounds, similarity demonstrates that the decryption procedure effectively recovers the original randomness supplied during encryption. The result matters considering that it guarantees the integrity and security of the decryption mechanism. The computed

entropy values supply helpful insights into both the randomness and uncertainty of the sound data, in addition to the effectiveness of the encryption and decryption tasks.

5.4 Perceptual security

This section examines the visual comparison between the encrypted data and the original unencrypted audio. We perform two distinct evaluations to assess the extent to which the proposed encryption technology preserves visual quality. The tests include subjective and objective exams, which, when combined, provide a comprehensive review of the visual security of the encryption process [24].

An alternating evaluation is conducted to examine the main criteria employed in assessing outstanding performance, as indicated in Table 3. The subsequent section provides a mathematical elucidation of these specific measures of inaccuracies. I urge readers to pay attention to the subtleties in Table 4 to gain a comprehensive understanding of the results that were obtained.

.

1) Mean Squared Error (MSE) constitutes an essential statistic that determines the effectiveness of audio techniques for encryption. It assesses the average squared deviation across the original and encrypted audio signals, measuring the distortion resulting from the encryption procedure.

$$\mathrm{MSE} = \frac{\sum_{i=1}^{\mathrm{length}(\boldsymbol{X})} (X_i - \mathrm{C}_i)^2}{\mathrm{length}(\boldsymbol{X})}, \tag{12}$$

What exactly are the distinctions between the encrypted audio and the original audio. An increased mean squared error (MSE) indicates an additional perturbation to the original signal, indicating a higher level of encryption security. In the context of audio encryption, a signal containing a diminished mean square error (MSE) may nevertheless be susceptible to attacks on security, simply because it maintains much more of the original signal's attributes. Regarding audio encryption, a high mean signal error (MSE) is helpful given that it signifies that the encryption algorithm successfully and effectively obscured the original audio, keeping it unrecognisable and enhancing defence against outside interference.

2) Peak Signal-to-Noise Ratio (PSNR): provides an essential factor for evaluating the practicality of cryptographic systems, notably our suggested audio encryption approaches. PSNR quantifies the quality that is in the original audio signal compared to the noise generated during encryption, expressed as decibels (dB). A higher quantity of PSNR indicates the fact that the encrypted audio maintains a better quality of the original signal, leading to less distortion and noise.

.

$$\mathrm{PSNR} = 10 \times \log_{10}\left(\frac{Max^2}{\mathrm{MSE}}\right), \tag{13}$$

Eventually, Max indicates the higher intensity level of the audio for the encryption data, while a lower peak signal-to-

noise ratio (PSNR) is frequently utilised since it effectively reduces the original signal, consequently boosting its security against unauthorised manipulation. Establishing a balance is essential since an inappropriately low PSNR could compromise signal quality along with affecting the effectiveness of the decrypted audio. PSNR provides an essential metric to assess the relationship between security and audio quality in encryption techniques.

TABLE 4: Quantitative metrics measuring the perceptual quality of the plain audio in comparison to the encrypted audio and the audio after decryption.

Audios	Components of Lorenz Chaotic Key	Original plain audio with encrypted audio		Original plain audio with decrypted audio.	
		MSE	$PSNR\ (dB)$	MSE	$PSNR$
Piano	x	149.7306	4.78	0	∞
	y	278.9325	4.78	0	∞
	z	954.4959	4.78	0	∞
Car_Horn	x	150.6632	4.75	0	∞
	y	280.1603	4.76	0	∞
	z	956.3056	4.77	0	∞
Human	x	149.8758	4.78	0	∞
	y	280.1483	4.76	0	∞
	z	949.5719	4.80	0	∞

The differences in the original plain audio, encrypted audio, and decrypted audio quality are presented in Table 4. Quantitative measures such as mean squared error (MSE) and peak signal-to-noise ratio (PSNR), both measured in decibels (dB), are employed to achieve this. Using components x, y, and z of the Lorenz Chaotic Key, we analyse the three sample types of command audio, including piano, car horn, and human. In the context of every instance of simple audio, the corresponding PSNR values are low, fluctuating between 4.75 and 4.80 dB, indicating detectable noise, while the MSE measure between the original and encrypted audio remains noticeably high, indicating significant change. On the other hand, the PSNR is infinite, and the MSE between the original and decrypted audio is zero, implying a flawless reconstruction with no audio quality loss that complies with decryption.

CONCLUSION

The present research presents a creative method for audio encryption employing two methodologies: the chaotic dynamics of the Lorenz system along with the Elzaki transformation. The starting layer utilises the chaotic Lorenz system, noted for its sensitivity to initial conditions and unpredictable behaviours, to generate a random key sequence. The resulting sequence is employed to execute confusion, covering the relationship between the generated key and audio within a bitwise XOR operation as a form regarding pre-encryption.

The Elzaki transformation provides a secondary encryption layer, recognised for its robust aptitude to modify data, thus improving audio security by adapting the coefficients of the Maclaurin series, which constitutes the output vector resulting from the pre-encryption stage, and performing a modular operation. The procedure of encryption effectively distorts the original audio signals, as confirmed by statistical and correlational analysis. The encrypted audio has a substantially high degree of entropy, indicating more unpredictability and security. The encrypted audio sustains the original quality, revealing no discernible interruptions or information loss, and verifying the reliability of the entire technique.

.The recommended encryption methods successfully improve security for audio dedication, as shown by performance measures like Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR). The functionality in MATLAB

exhibits the method's computing efficiency. In conclusion, the proposed encryption approach provides a secure and dependable means for preserving audio data since it preserves audio quality while providing robust defence. Future research may investigate the applicability of this study methodology across different forms of multimedia data and its usefulness in real-time communication channels and Incorporate a diffusion layer based on the Lorenz system solution for a single component to disseminate the statistical characteristics of the original audio across the encrypted audio. This means that modifying a single bit of the original audio will result in several bits of the encrypted audio shifting and inversely.

Author Declaration

I confirm that all the Figures and Tables in the manuscript are mine.

References

1. Gupta S, Dhanda N. Audio steganography using discrete wavelet transformation (DWT) & discrete cosine transformation (DCT). IOSR Journal of Computer Engineering. 2015 Mar;17(2):32-44.

2. Hameed AS. Speech compression and encryption based on discrete wavelet transform and chaotic signals. Multimedia Tools and Applications. 2021 Apr;80(9):13663-76.

3. Pirdawood MA, Kareem SR, Zahir DC. Audio encryption framework using the laplace transformation. aro-the scientific journal of koya university. 2023 Aug 25;11(2):31-7.

4. Wong KW, Kwok BS, Law WS. A fast image encryption scheme based on chaotic standard map. Physics Letters A. 2008 Apr 7;372(15):2645-52.

5. Zou C, Zhang Q, Wei X, Liu C. Image encryption based on improved Lorenz system. IEEE Access. 2020 Apr 20;8:75728-40.

6. Lynnyk V, Sakamoto N, Čelikovský S. Pseudo random number generator based on the generalized Lorenz chaotic system. IFAC-PapersOnLine. 2015 Jan 1;48(18):257-61.

7. Gupta MD, Chauhan RK. Hardware efficient pseudo-random number generator using Chen chaotic system on FPGA. Journal of Circuits, Systems and Computers. 2022 Feb 2;31(03):2250043.

8. Lorenz EN. Deterministic nonperiodic flow. Journal of atmospheric sciences. 1963 Mar;20(2):130-41.

9. Azzaz MS, Fellah R, Tanougast C, Kaibou R. Design and FPGA implementation of TRNG based on a new multi-wing attractor in Lorenz chaotic system. The European Physical Journal Special Topics. 2021 Nov;230(18):3469-80.

10. Rezk AA, Madian AH, Radwan AG, Soliman AM. Reconfigurable chaotic pseudo random number generator based on FPGA. AEU-international Journal of Electronics and Communications. 2019 Jan 1;98:174-80.

11. Zou C, Zhang Q, Wei X, Liu C. Image encryption based on improved Lorenz system. IEEE Access. 2020 Apr 20;8:75728-40.

12. Karakaya B. Chaotic system-based pseudo random bit generator and post-processor design for image encryption. In2022 13th National Conference with International Participation (ELECTRONICA) 2022 May 19 (pp. 1-4). IEEE.

13. Arıcıoğlu B, Kaçar S. Circuit implementation and PRNG applications of time delayed Lorenz System. Chaos Theory and Applications. 2022;4(1):4-9.
14. Yildirim G, Tanyildizi E. An innovative approach based on optimization for the determination of initial conditions of continuous-time chaotic system as a random number generator. Chaos, Solitons & Fractals. 2023 Jul 1;172:113548.
15. Feng L, Du J, Fu C, Song W. Image encryption algorithm combining chaotic image encryption and convolutional neural network. Electronics. 2023 Aug 15;12(16):3455.
16. Soni GK, Arora H, Jain B. A novel image encryption technique using Arnold transform and asymmetric RSA algorithm. InInternational Conference on Artificial Intelligence: Advances and Applications 2019: Proceedings of ICAIAA 2019 2020 (pp. 83-90). Springer Singapore.
17. Roy A, Misra AP. Audio signal encryption using chaotic Hénon map and lifting wavelet transforms. The European Physical Journal Plus. 2017 Dec;132:1-0.
18. Elzaki TM. The new integral transform Elzaki transform. Global Journal of pure and applied mathematics. 2011 Jan 1;7(1):57-64.
19. Elzaki TM. On the connections between Laplace and Elzaki transforms. Advances in Theoretical and Applied mathematics. 2011 Jan 1;6(1):1-1.
20. Pirdawood MA, Kareem S, Al-Rassam O. Encryption of Color Images with a New Framework. ARO-THE SCIENTIFIC JOURNAL OF KOYA UNIVERSITY. 2024 Jun 14;12(1):170-80.
21. Mohamed Parvees MY, Abdul Samath J, Parameswaran Bose B. Cryptographically secure diffusion sequences—An attempt to prove sequences are random. InAdvances in Big Data and Cloud Computing: Proceedings of ICBDCC18 2019 (pp. 433-442). Springer Singapore.
22. Lima JB, da Silva Neto EF. Audio encryption based on the cosine number transform. Multimedia Tools and Applications. 2016 Jul;75:8403-18.
23. Sathiyamurthi P, Ramakrishnan S. Speech encryption using chaotic shift keying for secured speech communication. EURASIP Journal on Audio, Speech, and Music Processing. 2017 Dec;2017:1-1.
24. Lian S. Multimedia content encryption: techniques and applications. Auerbach Publications; 2008 Sep 17.

.