Franklin Open 8 (2024) 100158

Contents lists available at ScienceDirect

Franklin Open

journal homepage: www.elsevier.com/locate/fraope

Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems

Thejas Haridas, Upasana S.D., Vyshnavi G., Malavika S. Krishnan, Sishu Shankar Muni *

School of Digital Sciences, Digital University Kerala, Thiruvananthapuram, PIN 695317, Kerala, India

ARTICLE INFO

Keywords:
Chaos-based encryption
Hyperchaotic maps
Audio security
Multimedia encryption
Cryptography
Information security
Digital communication
Encryption algorithms
Chaotic systems
Data protection

ABSTRACT

Secure communication in the digital age is necessary; securing audio data becomes very critical since this is normally transmitted across susceptible networks. Traditional approaches to encryption, like Advanced Encryption Standard and Rivest–Shamir–Adleman, are pretty solid but mostly too computationally intensive for real-time audio applications. This paper presents a new audio encryption scheme using chaotic systems, characterized by high sensitivity to initial conditions, pseudo-randomness, and determinism. These properties make chaotic systems ideal for generating keys for cryptographic purposes. Indeed, complex keys that would be nearly impossible to reverse-engineer without exact initial parameters can be obtained with them. This methodology first digitizes the audio signal and subsequently encrypts each sample according to chaotic sequences from multiple systems, like 2D Memristive Hyperchaotic Maps and 3D Hyperchaotic Quadratic Maps. The encryption processes enormously increase the randomness of the encrypted audio and blind the original data, demonstrating the strength of the chaotic systems in securing audio information.

Simulation of this encryption approach confirms its effectuality in providing strong security for audio data while maintaining efficiency, thus being suitable for real-time applications. The developed encryption schemes show high resistance to differential attacks, while the quality of the encrypted audio remains acceptable after transformation. This result can demonstrate chaotic systems' potential to provide a secure and efficient solution for audio communications, which has broad applications in telecommunications, military communications, and confidential conferencing systems. This work, described in the paper, thus satisfies the growing demand for robust security in digital communications and opens up avenues of future research toward chaotic parameter optimization and an extension to other forms of data, enhancing the security features in all types of digital communication channels.

1. Introduction

Multimedia data, which includes text, music, and image files, are now to be shared and transmitted easily in an open setting because of the internet's rapid expansion. But this brings up several information security issues. Numerous techniques for protecting multimedia information have been proposed, including steganography watermarking [1]and encryption. One of the most popular technologies among them is encryption. Due to its pseudo-randomness, sensitivity to beginning values, and other characteristics, chaos is frequently used in cryptography [2].

Chaos [3] refers to systems that seem random but are governed by deterministic laws. A chaotic system [4] uses deterministic randomness as a source for unpredictable behaviors. Depending on whether the technique encodes floating, decimal, or binary data. Chaos-based encryption has been used to encode various data types by considering the appropriate design modifications each time. Chaos systems are hard to predict [5] since they are sensitive to the initial state such that long-term prediction does not work, as it is almost impossible. Most of the time, chaos will always display complex behaviors and nonlinear dynamics, and the variables will always interact, making it difficult to have a simple analytical solution. However, describing the chaotic system does not provide us with the requirement for study since chaos has no nature. Even though the level of the forecast of chaos limits us, it offers secure evidence access concerning attention to various statistical regularities in other domains [6] Chaotic systems can encrypt audio recordings and convert data to the hardest form [7], preventing unauthorized parties from decoding the original data by using chaos theory.

The steps involved in this voice encryption are:

- The encryption process begins by producing a chaotic signal by a chaotic system. This signal behaves as the cornerstone for encrypting the audio format. Chaotic systems such as logistic maps [8], Lorenz systems [9], Henon maps [10] or any prototypical chaotic systems are mainly found for the occasion.

* Corresponding author.
E-mail address: sishushankarmuni@gmail.com (S.S. Muni).

https://doi.org/10.1016/j.fraope.2024.100158
Received 29 June 2024; Received in revised form 1 September 2024; Accepted 14 September 2024
Available online 20 September 2024

- The audio format should be digitized, that is, changing the analog audio signals to a digital format. This digital data can be treated and encrypted.
- The chaotic signal formed in the earlier stage can be used as the lead for encrypting the audio data. Different encryption algorithms of chaos are chaos-based stream ciphers or chaos synchronization techniques.
- The audio data form is joined with the chaotic signal using mathematical operations such as XOR (exclusive OR), sum, or modulation [11]. This mixes up the audio files in a chaotic form and converts them to indistinct without the right decryption key.
- The encrypted audio data can be transferred through communication mediums, such as the information highway, to the people. It is necessary to ensure safe transmission to prevent the blocking by unlicensed parties.
- At the collecting end, the recipient must utilize the identical chaotic signal generated at first (or a synchronized chaotic system) as the decryption key. The encrypted audio file is treated using the decryption algorithm, altering the encryption process and retrieving the actual audio signal.

A chaotic map often involves repeated procedures in which a nonlinear equation is an iteratively updated subject starting from an initial value, giving a sequence of values [12]. Even with such an equation, maps can produce complex and dynamic behavior such as chaotic dynamics, quasiperiodic, and periodic. Chaotic maps can be incorporated into cryptographic algorithms for voice encryption to increase security and randomness [13]. The main benefits of a chaotic map are that it is sensitive to initial conditions and control parameters, unpredictability, and stochasticity. Compared to a dynamic system modeled by ordinary differential equations, the computational efficiency of chaotic maps is accredited to their discrete nature [14], allowing for easier implementation and lower computational cost. Moreover, the simplicity of chaotic maps increases the suitability for the encryption process, especially when dealing with large amounts of data. That is when considering encryption, chaotic maps offer increased efficiency to the computational approach [15] compared to dynamic systems modeled by ODEs.

The contributions to this paper are as follows:

- The paper significantly contributes to the field of data security by thoroughly exploring the use of chaotic maps in audio encryption. By utilizing the natural chaotic behavior of these maps, the study shows how they can effectively convert audio data into a highly secure and difficult-to-decode form, thus improving data confidentiality.
- Evaluation of Encryption Schemes: The paper evaluates two distinct encryption schemes based on 2D memristive hyperchaotic maps [16] and 3D hyperchaotic systems [17].
- The research paper confirms that using chaotic map-based encryption techniques effectively preserves audio quality while maintaining high levels of security. Through experiments and evaluations, the study demonstrates the effectiveness of chaotic maps in encrypting audio, offering a strong method to protect confidential audio information from unauthorized access and manipulation.

The paper is organized as follows: Section 1 explores the chaos, chaotic map, offering a detailed explanation of its mathematical underpinnings and relevance to our analysis. Following this, in Section 2, we add the various related works, and in Section 3, the bifurcation diagram, discussing the techniques employed and their application to our research objectives. Section presents the algorithm for the encryption and decryption process and Section 5 highlights the results obtained from our analyses, elucidating key findings and insights derived from the data. We then proceed to Section 6 offering the results obtained and Section 7 gives a comprehensive conclusion summarizing our study's outcomes and implications.

2. Related works

Different approaches to speech protection have been studied in several recent research. By considering the appropriate design alterations each time, chaos-based encryption has been used to encrypt various data formats like encoding binary data or floating-point decimal data depending on the approach. For securing telecommunication a three-step audio signal encryption is introduced [18], similarly, an ECG signal encryption technique is used for telemedicine applications [19]. An introduction to a cryptosystem based on chaos for high-resolution digital photos, utilizing an arbitrary precision arithmetic digital chaos generator, running on the Snapdragon Pi 3 SoC [20]. The mod 1023 function [21] is utilized to enhance four chaotic maps for encrypting RGB images in a machine scheme through message queuing telemetry transport on Wifi and the Internet. A built-in cryptosystem utilizing chaos principles with a voice recognition access key that is executed on an FPGA platform [22]. Also, the implementations consist of independent graphical user interfaces that can be utilized on various devices such as microcomputers, computers, etc. A pseudorandom generator based on two-dimensional Henon-Sine hyperchaotic map for microcontrollers is an illustration [23], and also a secure communication system implemented on a microcontroller [24] using a five-term 3D chaotic map [25].

In recent academic works, various research studies have delved into different methods to protect speech. A unique two-phase speech encryption method, utilizes an innovative chaotic map, 2D-LMSM, Fast Fourier Transform, and the Discrete Wavelet Transform [26]. This strategy has shown impressive results in both encrypting techniques. A new 3D chaotic system with a capsule-shaped equilibrium curve is another significant contribution [27]. Two new integrated chaotic maps for speech encryption algorithms and the sine-logistic maps are used to create a Sine-Logistic Integrated Map(SLIM) and the sine and cube maps are used to create Sine Cubic Integrated Map (SCIM) [28].

By using single and double-dimension discrete-time chaotic systems to increase the security of audio data encryption, along with application and security studies was a good improvement [29]. Samples of mono and stereo audio data were encrypted. Discrete-time chaotic systems in both single and double dimensions were employed in this application. A non-linear function was also used in a separate technique to increase security during encryption. Keyspace, key sensitivity, chaotic effect, and histogram analysis were used to obtain findings in the chaos-based application implemented using the developed method. These analysis results were used to test the application's chaotic system safety.

Lorenz hyperchaotic systems [30] and the synchronization property of a class of cellular neural networks. This study presents a control approach between various chaotic dimensional systems, analyzing the synchronization stability utilizing the controller and Lyapunov[31] stability theory as a basis. Lastly, a new concept for an audio synchronization encryption technique is presented. The simulation's findings indicate that there is little to no link between the original audio document's waveform and the encrypted version. It is further confirmed by comparing the spectrum that this design has an amazing encryption effect.

Models for encryption and decryption techniques that include synchronizing a 4-D nonlinear fractional-order hyperchaotic system [32] with an external disturbance are crucial. Based on the transformation of audio data samples into visual data, audio encryption and decryption techniques are researched. The audio signals are encrypted and decrypted using a random mask that is created from a chaotic mask. It is demonstrated that the fractional order hyperchaotic system's error path is far superior to the classical one. Furthermore, by examining several measures in addition to numerical simulations, such as MSE, PSNR, SSIM, NPCR, and SNR [33], the high-level security of the suggested work is trusted.

The SVEA [34], was a selective video encryption algorithm based on the theory of chaos and Intellect neural networks. It offers a 2D

extended Schaffer function map (2D-ESFM) for the rapid and secure encryption of sensitive video regions for secure video encryption. This approach can be linked with audio encryption using chaos since authors of that approach employ chaotic systems to ensure secure multimedia data encryption. A new two-dimensional memristive cubic map (2D-MCM) for video encryption along with an improved capability of the pseudorandom sequence generation and complex map dynamics. Therefore, the study provides evidence of the effectiveness of the proposed 2D-MCM for the use of video encryption and vice-versa; hence offering foundation work for other studies in audio encryption using chaotic systems since the procedures adopted in this study are quite similar to the procedures for encryption of data [35]. Also in the following paper titled [36] which explained the new method of video encryption concerning the chaos. This is due to the fact that it encrypts only keyframes, which are segmented through temporal action segmentation which in return reduces the computational load. It also introduces two-dimensional Gramacy and Lee mapping (2D-GLM) for better pseudorandom sequences for encryption over conventional approaches in security and speed with a check on GTEA data. Some papers introduce an efficient facial image encryption method called EFR-CSTP [37], combining chaos theory and semi-tensor product to scramble facial features while preserving efficiency securely. Its approach to securely encrypting visual data using chaotic systems can inspire similar techniques for enhancing the security of audio encryption methods using chaos. In case of image encryption, There are three stages by which the pixel locations of a color image are manipulated to resist attacks during encryption. The method was tested using key-sphere analysis, entropy, noise attack, and correlation analysis; all of which showed that the presented method was effective in image encryption. They suggest that the present algorithm may hold out against regular attacks and is more effective in defending against statistical attacks than previous approaches [38].

3. Bifurcation diagram

Bifurcation is fundamental in applying chaotic systems to realize voice encryption and decryption by using sensitive dependence on initial conditions and parameter values intrinsic in chaotic dynamics. Key sensitivity for a small change in the encryption will result in quite different chaotic sequences owing to bifurcation so that only the exact key can decrypt the message. This sensitivity ensures good encryption since a wrong key will never produce a useful decrypted message. Additionally, the adjustment of the parameters of the chaotic system is an important step towards optimal behavior for encryption. By using bifurcation diagrams, it is possible to find parameter ranges where the required behavior of chaos is obtained, which may provide good encryption. These diagrams help in choosing the parameters so that the most unpredictable and complex chaotic sequences are picked, hence improving the security of the encrypted communication. Bifurcation diagram and Lyapunov exponents give us the parameter values at which the system enters a regular state (periodic regime), chaotic, and hyperchaotic regime. The audio encryption technique will not be effective if we use a periodic regime or a fixed point regime. Therefore, bifurcation diagrams align with their corresponding Lyapunov exponents to help us tune the parameter to a hyperchaotic regime which is then used in the encryption process.

Voice encryption via bifurcation and chaos offers a high gain in terms of security, complexity, and robustness. The most important advantage is intrinsic sensitivity to initial conditions and parameters of the chaotic system itself, which makes it very hard for attackers to decrypt the message without the key. In the abstract, even extremely small variations of the key result in very different outcomes in the end, hence increasing the security. The intrinsic complexity of the chaotic systems also gives an added layer of security, since their very unpredictable and random behavior makes any unauthorized decryption truly a Herculean task. Added to this is its resilience against a wide range of data inputs while ensuring secure encryption for chaotic systems. This adaptiveness keeps the process of encryption effective and robust for all kinds of voice data, hence making this a generally robust solution to various situations while never compromising on security. Also, the Lyapunov exponent is an essential measure in bifurcation diagrams and can be used to approximate the separation rate of infinitesimally close trajectories in some chaotic systems. In connection with the bifurcation diagrams for voice encryption, the Lyapunov exponent defines the stability and chaos tendency of the system for different values of parameters. A positive Lyapunov exponent indicates chaos—very small differences in initial conditions may result in an exponential divergence of trajectories. This means that, at this condition, the encryption is highly sensitive to the initial condition and the keys used, hence providing enhanced security. If plotted against bifurcation diagrams, one has a clear graphical indication of the regimes where the system is exhibiting chaotic behavior; hence, this guides the choice of parameters toward robust and unpredictable sequences for encryption".

In this work, we have considered two hyperchaotic maps namely (a) a 2D quadratic memristor hyperchaotic map, and (b) a 3D hyperchaotic map. We further do a comparative analysis of their efficiency in terms of audio encryption. We describe below some of the properties of the maps under consideration.

3.1. 2D quadratic memristor map

The two-dimensional discrete quadratic memristor mapping is given as follows

$$\begin{aligned} x_{n+1} &= k x_n (q_n^2 - 1), \\ q_{n+1} &= q_n + x_n, \end{aligned} \tag{1}$$

where x, q represents the current and charge variable respectively, and k represents the parameter [39]. The 2D quadratic memristor map is symmetric as $(-x, -q) \rightarrow -(x, q)$. Moreover, the map displays a pinched hysteresis loop property when a discrete periodic current is applied. It has also been shown that the 2D map can be realized in hardware. Moreover, the hyperchaotic signals from the map have been used in the field of image encryption [40]. The motivation for choosing this map in the field of audio encryption is due to the display of extreme hyperchaos with all two positive Lyapunov exponents in a wide range of parameter space. Fig. 1(a) shows a one-parameter bifurcation diagram of the 2D quadratic memristor map with the variation of parameter k. We can observe that the system follows the usual period-doubling route to chaos and then hyperchaos with two positive Lyapunov exponents, see Fig. 1(b). We tune the parameter k where the system enters the hyperchaotic regime with all two positive Lyapunov exponents for audio encryption.

3.2. 3D hyperchaotic map

The 3D map under consideration is a quadratic map that has been found to exhibit rich dynamics such as ergodic doubling bifurcation, resonant torus doubling bifurcation [41], hyperchaotic behavior with all three positive Lyapunov exponents [42]. The three-dimensional hyperchaotic map studied in [41] demonstrates control of chaos via a modified stability transformation method. The three-dimensional mapping is given as follows

$$\begin{aligned} x_{n+1} &= a_1 x_n + a_2 y_n + a_3 y_n^2, \\ y_{n+1} &= b_1 - b_2 z_n, \\ z_{n+1} &= c x_n, \end{aligned} \tag{2}$$

where x, y, z represents the state variables, and $a_1, a_2, a_3, b_1, b_2, c$ are parameters. Recently, the hyperchaotic signals from the map have been used in the field of image encryption [40]. The motivation for choosing this map in the field of audio encryption is the display of extreme hyperchaos with all three positive Lyapunov exponents in a wide range of parameter space. Fig. 2(a) shows a one-parameter

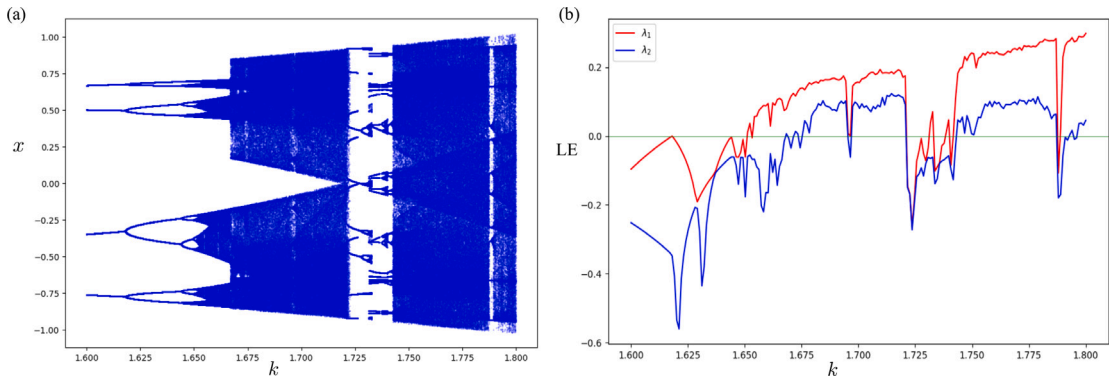

Fig. 1. (a) One-parameter bifurcation diagram illustrates how the system's state changes as a function of the parameter k. (b) Corresponding Lyapunov exponent spectrum.

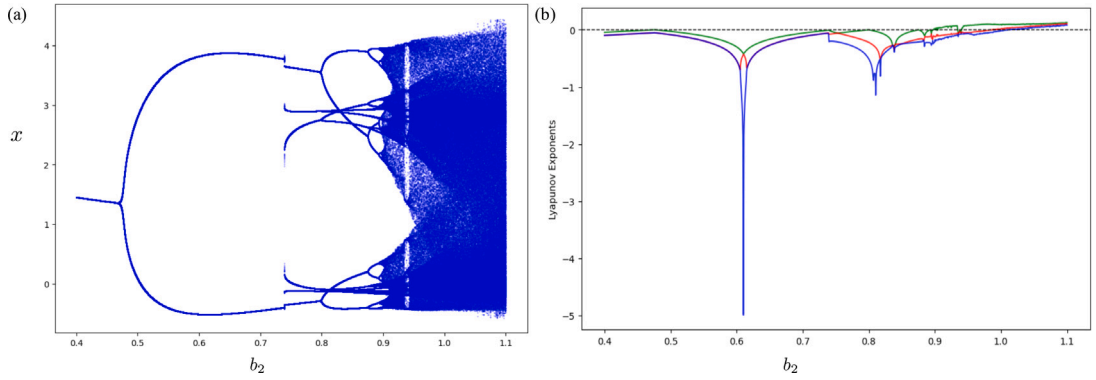

Fig. 2. (a) One-parameter bifurcation diagram illustrates how the system's state changes as a function of the parameter b_2. (b) Corresponding Lyapunov exponent spectrum. The parameters are $a_1 = -0.17, a_2 = 0.25, a_3 = 0.12, b_1 = 4, c = 2.15$.

bifurcation diagram of the 3D quadratic map with the variation of parameter b_2. We can observe that the system follows the usual period-doubling route to chaos and then hyperchaos with all three positive Lyapunov exponents, see Fig. 2(b). We tune the parameter b_2 where the system enters the hyperchaotic regime with all three positive Lyapunov exponents for audio encryption.

4. Experimental setup

The experiment was conducted using Google Colab, which provided a flexible and powerful environment for executing Python-based data analysis and visualization. The following libraries were used to perform various

- `NumPy (numpy)`: For numerical operations and handling arrays.
- `Matplotlib (matplotlib.pyplot)`: For creating visualizations, such as plotting results and saving figures.
- `Librosa (librosa)`: For audio processing, including loading, analyzing, and manipulating audio signals.
- `Hashlib (hashlib)`: To implement hashing functions for encryption purposes.
- `Random (random)`: For generating random values used in encryption schemes.
- `PyEMD (PyEMD)`: To perform Empirical Mode Decomposition (EMD) on audio signals, which was essential for breaking down the signal into Intrinsic Mode Functions (IMFs).
- `Scipy Signal (scipy. signal)`: The `welch` method was employed for spectral density estimation, while `spectrogram` was used to generate spectrograms, visual representations of the signal's frequency content over time.
- `Seaborn (seaborn)`: Used for enhanced data visualization.

The experiment utilized Google Colab as a convenient platform for executing Python-based data analysis and visualization. Essential libraries included NumPy for numerical operations, Matplotlib for creating plots and figures, Librosa for audio processing, Hashlib for hashing functions, Random for generating random values, PyEMD for EMD, Scipy Signal for spectral analysis, and Seaborn for advanced data visualization. These libraries collectively provided the necessary tools to perform tasks such as loading audio data, applying encryption techniques, analyzing spectral properties, and generating visual representations of the results.

5. Algorithm: Chaos-based encryption with 2D and 3D memristive hyperchaotic map

The provided process explains how to encrypt an audio file using signal processing and cryptography techniques. This encryption method is outlined below in a logical sequence which is represented in the flowchart 3. First, the original audio file (*org_aud*) is used to start the encryption process. To separate the raw audio data for additional processing, the audio file's header — which usually includes metadata like file format and properties — is removed. By eliminating additional potentially identifying information, this step ensures the encryption is restricted to the audio material. After that, the SHA3-512 algorithm [43] is used to hash the isolated audio data, the data of audio is given in the Table 1. A fixed-size, 512-bit hash value that precisely represents the audio file's contents generated by this cryptographic hash function. The hashing process secures the uniqueness and integrity of the audio by assuring that even slight alterations in the audio will result in a significantly distinctive hash value [44]. Then, the hash value is split into eight equal parts, which will be utilized for producing the encryption keys and parameters in the following steps

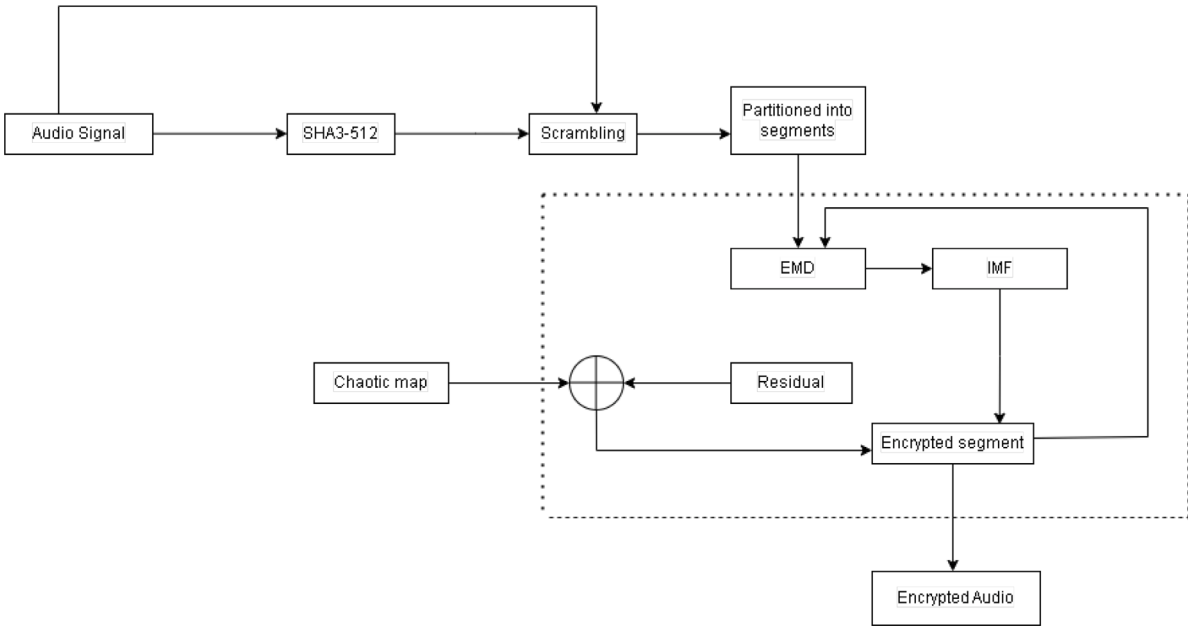

Fig. 3. Visualizing Encryption: From plaintext to ciphertext, witness the transformation of data through cryptographic algorithms and encryption keys, ensuring secure transmission.

A modified equation calculates the first encryption settings from these hash components. $k_0 = (c_0 \oplus c_1) \times 268 + (2.9 \text{ if } i \text{ in } (4,6) \text{ else } 0)$ is the equation for the initial parameter, k_0. This equation's conditional addition and bitwise XOR operations guarantee that the parameters are complex and unique. Iterative calculations are performed using these initial parameters to generate a sequence of encryption keys. Beginning with $x_0 = \frac{c_0}{2^{64}}$ and $q_0 = \frac{c_1}{2^{64}}$, the keys are calculated as follows: $x_i = k_{i-2} \times x_{i-1} \times (c_i^2 - 1)$ and $y_i = y_{i-1} + x_i$. Each key is represented by the formula $key_i = (x_i \times 10^{16}) \mod 256$. Following that, an index produced randomly is used to shuffle the audio data. To add a layer of obfuscation and make it more difficult to reconstruct the original audio without the correct decryption key and knowledge of the shuffling sequence, this stage reorders the audio samples in a non-linear form. Later, the shuffled audio is transformed into a two-dimensional matrix so that Empirical Mode Decomposition (EMD) [45] can be implemented more efficiently. The audio is broken down into residuals and intrinsic mode functions (IMFs) using EMD on each row of the 2D matrix. the 2D matrix is a time–frequency transformation of the original audio signal. The modulus maxima of the wavelet transform are extracted and stored in a matrix where each row corresponds to a different time segment of the signal, including the wavelet coefficients or frequency components. Subsequently, EMD is applied to each of these rows, this decomposes the signal by generating IMFs and residues. This process allows us to manipulate and encrypt the audio signal into smaller and simpler elements. The fundamental components of the audio signal, which are called residuals, are finally encrypted with the generated keys in an XOR process. This ensures that the residuals are strongly encrypted as the keys create a pseudo-random sequence based on the hash value of the audio. The final encrypted signal is obtained by merging IMFs and encrypted residuals. The encrypted audio data is then created by incorporating the encrypted residuals and IMFs. The graphs shown in Fig. 4 bear true to this fact by presenting the histograms of the original and "encryptedaudio. wav" of a 2D quadratic memristor map and in Fig. 5 of the 3D hyperchaotic map which proves that the audio encryption shreds the original signal in a way that renders it securely encrypted and impossible to retrieve in simple methods without decryption. This high level of encryption by several layers is a technique involving numerous layers of encryption and obfuscation during processing to ensure both confidentiality and the integrity of audio data. The result is such that an encrypted, secure copy of the initial audio is significantly hallmarked against possible manipulations and access by unauthorized third parties.

Table 1
Data of audio.

Audio file	File size	Duration (s)
CantinaBand3	129 KB	3
PinkPanther60	2.52 MB	60
StarWars60	2.52 MB	60

Another encryption algorithm technique is Discrete Cosine Transform (DCT) [46] different from the EMD encryption algorithm technique in which a hybrid 1D chaotic map is used to develop the key for encryption. The audio signal is first compressed by DCT, followed by the XOR operation between the compressed signal and the key; thereby EMD uses an altered equation for parameters determination of initial and subsequent encryption keys are determined through iterative calculations. To this end, the audio data is shuffled, normalized, and reshaped into a 2D matrix that undergoes EMD. The Empirical Mode Decomposition (EMD) in essence buried the signal into Intrinsic Mode Functions and residuals. Finally, the residues are encrypted by using XOR operation with the generated keys but use Discrete Cosine Transform (DCT) for the audio signal compression prior to encryption.

Encryption process

1. **Input:** Original audio file (`org_aud`).
2. **Remove header:** Remove the header from the original audio.
3. **Hash value creation:** Compute the SHA3-512 hash value of the audio.

   hash_val = SHA3-512(repr(audio))

4. **Divide hash value:** Divide the hash value into 8 equal components.

   components = $[c_0, c_1, c_2, c_3, c_4, c_5, c_6, c_7]$

5. **Initial parameters:** Calculate initial parameters for the modified equation.

   $$k_0 = \frac{(c_0 \oplus c_1)}{2^{68}} + (2.9 \text{ if } i \text{ in } (4,6) \text{ else } 0)$$

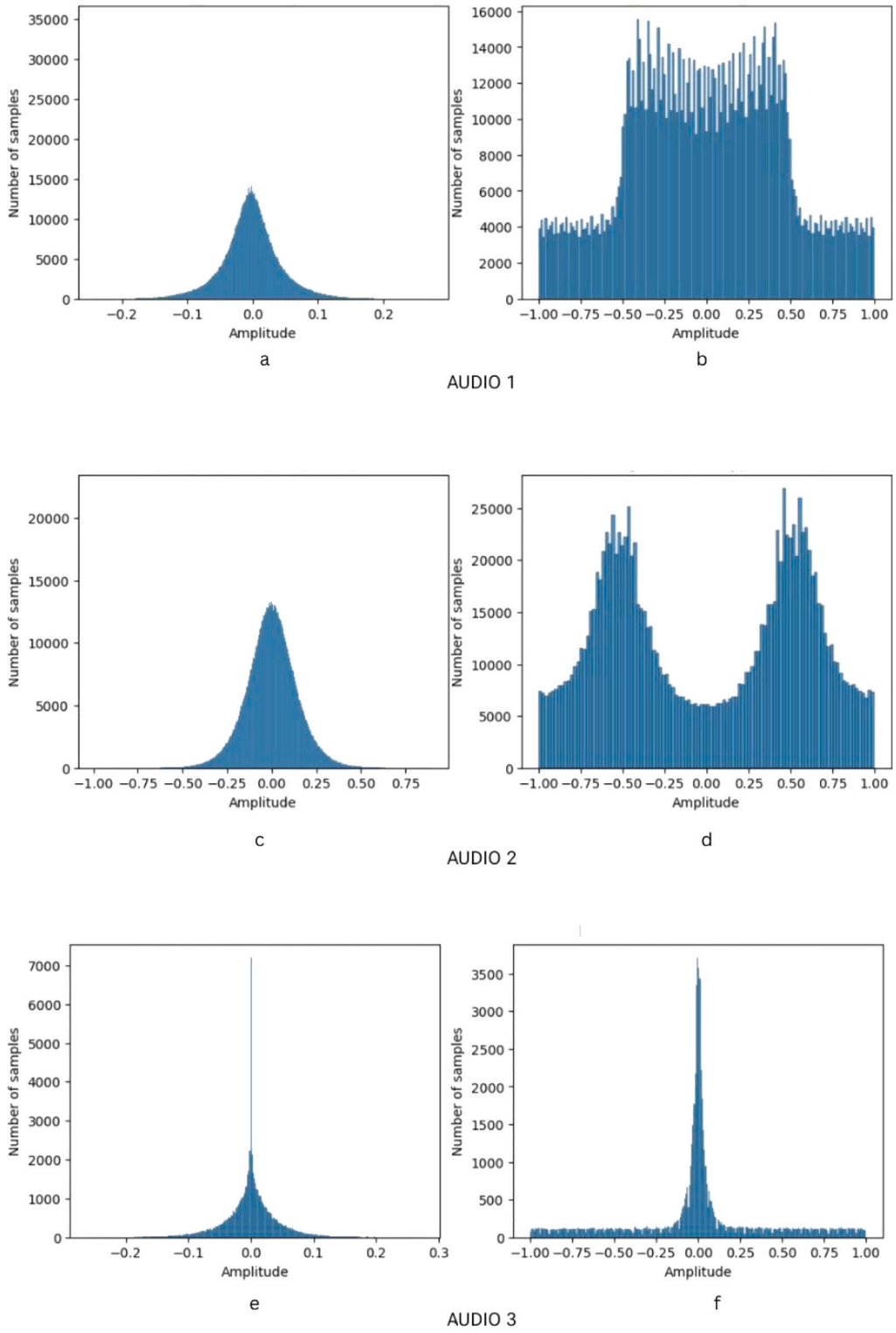

Fig. 4. Histogram comparison of various audio signals pre- and post-encryption via a 2D quadratic memristor map. It showcases discernible alterations in signal distribution.

6. **Generate Keys:** Generate encryption keys using the modified equations.

$$x_0 = \frac{c_0}{2^{64}}, \quad q_0 = \frac{c_1}{2^{64}}$$

$$x_i = k_{i-2} \times x_{i-1} \times (q_{i-1}^2 - 1), \quad y_i = y_{i-1} + x_i$$

$$\text{key}_i = (x_i \times 10^{16}) \mod 256, \quad \text{for } i = 0 \text{ to len(audio)}$$

7. **Shuffle audio:** Shuffle the audio based on a randomly generated index.

$$\text{index} = \text{random.sample}([0, 1, \ldots, \text{len(audio)} - 1], \text{len(audio)})$$

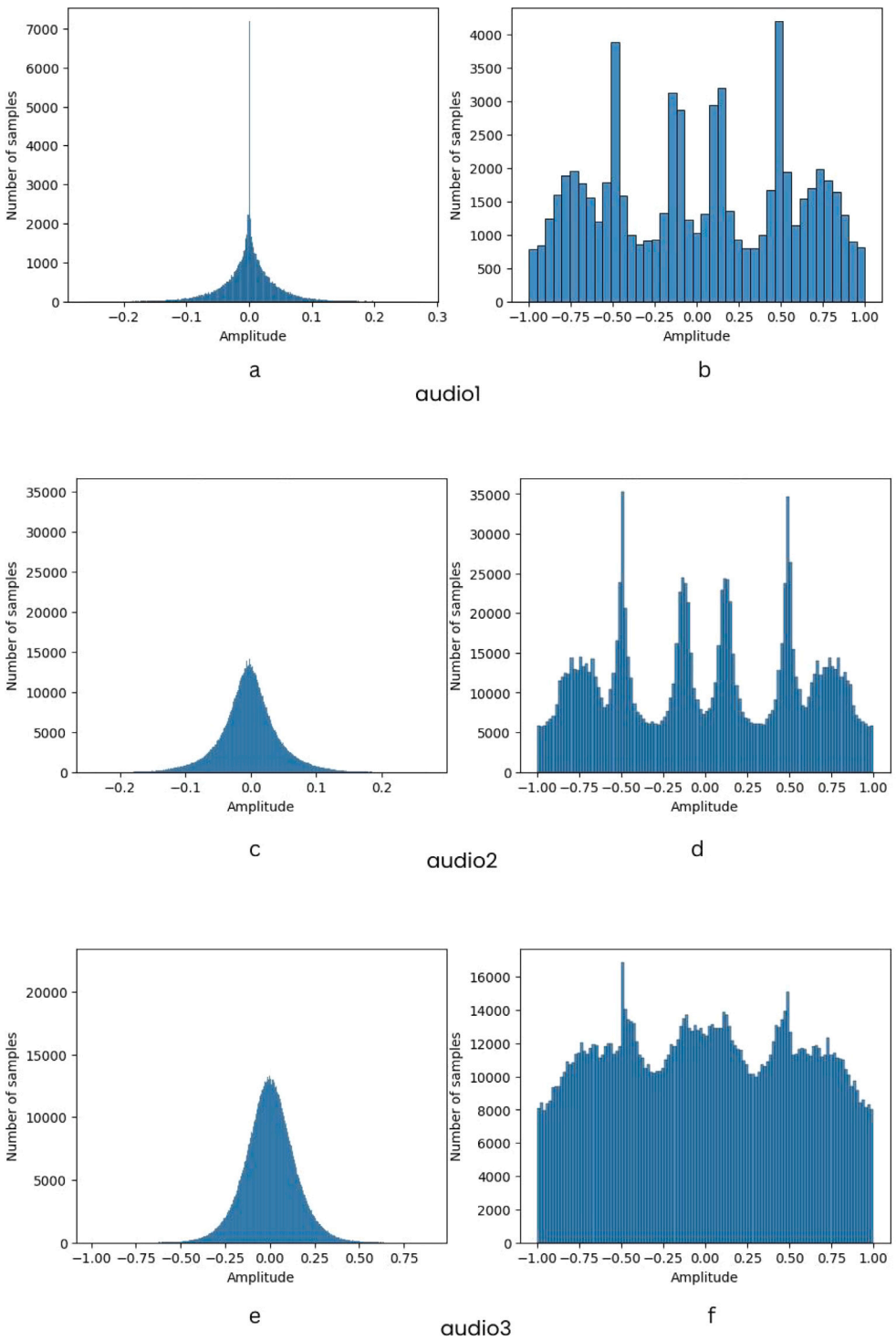

Fig. 5. Histogram comparison of various audio signals pre- and post-encryption via a 3D hyperchaotic map showcases discernible alterations in signal distribution.

suff_aud = audio[$index$]

8. **Convert to 2D matrix:** Convert the shuffled audio into a 2D matrix.

   td_mat = reshape(suff_aud, (height, width))

9. **Calculate IMFs:** Perform Empirical Mode Decomposition (EMD) on each row of the matrix to obtain Intrinsic Mode Functions (IMFs) and residuals.

   IMFs, all_residuals = EMD(td_mat)

10. **Encrypt residuals:** Encrypt the residuals using XOR with the generated key.

    enc_residual[i][j] = all_residuals[i][j] $\oplus$ key[k]

11. **Combine IMFs and encrypted residuals:** Combine the sum of IMFs and encrypted residuals to get the encrypted signal.

    encrypt_signal[i][j] = IMFs[i] + enc_residual[i][j]

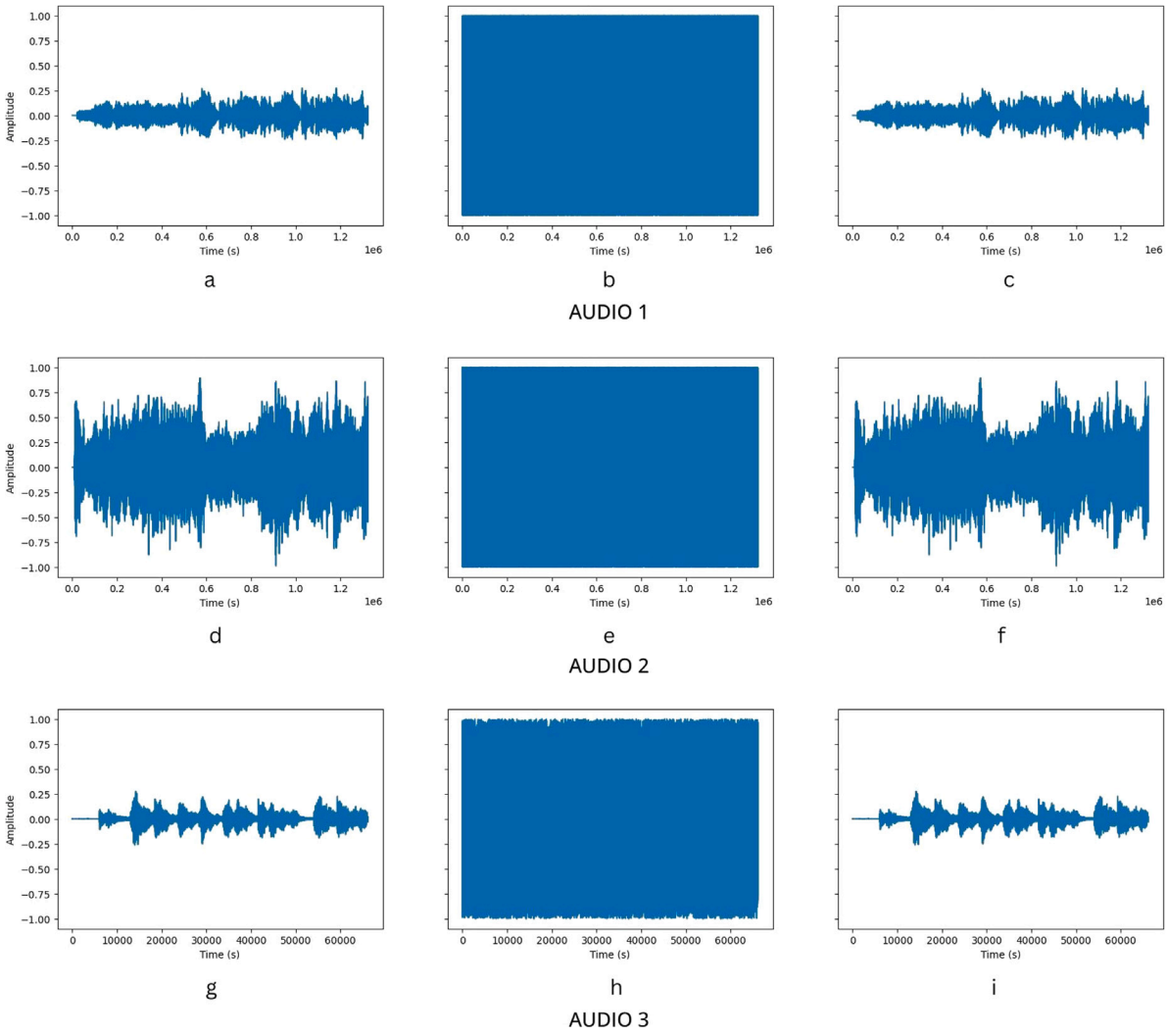

Fig. 6. Comparison of amplitude versus number of samples plots for three different audio files before and after encryption. The encrypted versions exhibit significant noise, indicating substantial alteration from the original signals.

12. **Output:** Encrypted audio file (`encryptedaudio.wav`).

Decryption process

The encrypted audio file "encryptedaudio.wav", which contains a series of digital audio samples, must be read to access the contents and initiate the decryption process. The encrypted audio file's header is retrieved to reveal important details about the encryption technique used and any pertinent metadata. Using the same key that was used for encryption, the encrypted residuals in the audio file are decoded after the header has been retrieved.

The encrypted audio data must first be modified into a 2D matrix with the same dimensions as before encryption to initiate the decryption procedure. To replicate the structure in which the original audio was processed, this step is essential. To ensure consistency in the matrix dimensions, the reshaping process computes the width and height factors based on the length of the audio data. By performing an XOR (exclusive OR) operation with the original key, the encryption is reversed and the decrypted residuals are generated. To effectively decrypt the encrypted residuals, each element is XORed with the associated key element.

The residuals must then be combined with the intrinsic mode functions (IMFs) [47] after the decryption. While the audio signal was encrypted, empirical mode decomposition was implemented to initially determine the different scales or frequency bands that constitute the IMFs. IMFs are unique to each row of the 2D matrix, indicating distinct audio signal segments. The fundamental elements and residual noise of the original signal are reconstructed by adding these IMFs row-wise to the decrypted residuals.

The resulting matrix, which now contains the regenerated audio data, is transformed back into a 1D array once the IMFs and decrypted residuals are added. The next step reverses the previous transformation, restoring the 2D matrix to its original linear version of the audio signal. After shaping the audio data, the samples are rearranged in the original sequence by unscrambling it. In the process of unshuffling, the shuffle index which is assigned during the cryptography process is reversed to make sure that the audio samples are aligned properly.

The final step of the decryption is to add the restored header to the part together with the reshuffled and regenerated audio data. Audio content and the associated metadata in the form of segments and annotations are recreated by using this combination. Finally, overwriting the damaged spots with the completely restored audio stream results in creating a new file named "decrypt2. wav", ready for further analysis or simply replaying. It can be observed from Fig. 6 that the implication of encryption and decryption on three distinct audio clips. The signals of the first column are also presented as clear waveforms which contain and represent the original audio signals. These waveforms as seen in the second column are transformed into noise after encryption thus

making audio uninterpretable. Still, as outlined in the third column, the decryption process is shown more in detail, and the original pure audio signal is revealed. This is important in order to allow the listeners to hear the content as intended by the producer with no hindrance or distortion.

The accurate methodical and thorough decryption includes several significant steps. Some of these procedures include reading and extractions of the header, reshaping and decryption of residuals, integration with IMFs, and reshaping of the hybrid structures. These steps include the first, and second steps of reading and extracting the headers, the third and fourth of reshaping and decrypting the residuals similar to the first steps, followed by the fifth of merging with the IMFs, the final step of reshaping back to 1D, unshuffling, and the last of storing the decoded audio. Every step is a deliberate bid to reverse the entire procedure of encryption in a manner that guarantees an authentic reproduction of the original voice signal. This assures that the decrypted audio is identical to the encrypted one, and it proves that the kinds of encryption and decryption used are reliable and efficient.

1. **Input:** Encrypted audio file (`encryptedaudio.wav`).
2. **Read audio:** Read the encrypted audio file.
3. **Extract header:** Extract the header from the encrypted audio.
4. **Decrypt residuals:** Decrypt the encrypted residuals using XOR with the original key.

   $$\text{dec\_residual}[i][j] = \text{enc\_residual}[i][j] \oplus \text{key}[k]$$

5. **Combine IMFs and decrypted residuals:** Combine the sum of IMFs and decrypted residuals to get the decrypted signal.

   $$\text{decrypt\_signal}[i][j] = \text{IMFs}[i] + \text{dec\_residual}[i][j]$$

6. **Output:** Decrypted audio file (`decript.wav`).

6. Evaluation metrics

In this section, we will discuss the evaluation metrics for two different maps for encryption schemes used with audio data, such as the 2D memristive hyperchaotic map and the 3D hyperchaotic quadratic map [48]. These metrics are going to help determine how great the encryption process is and how useful it is going to be for preserving the quality and security of the audible signals.

6.1. Entropy analysis

Entropy is the measure of encrypted audio signals to appear nearly unpredictable or have high randomness. The Table 5 below demonstrates the entropy values of the encrypted audio generated using two different encryption methods. The 2D memristive hyperchaotic map yielded an entropy value of 7.8105 although the 3D hyperchaotic quadratic map has an entropy value of 7.7991, which is nominally lower. The findings indicate that the distribution of the audio samples unveils a high level of randomness and complexity.

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

where :

$p(x_i)$: Probability of the ith value in the signal X.

6.2. Correlation coefficients

Correlation coefficients provide a perception of the relationship between the original and encrypted audio signals. The correlation coefficients between the encrypted version and the original audio for both encryption algorithms are also numbered in Table 2. The 2D memristive hyperchaotic map's correlation coefficient is 0.2562, which denotes that the correlation between the encrypted and original audio signals is weak which is demonstrated graphically in Fig. 9, graphs a and b represent the original and encrypted version of Audio 1. Similarly, graphs c and d show the original and encrypted versions of Audio 2, and graphs e and f represent the original and encrypted versions of Audio 3. On the other hand, the 3D hyperchaotic quadratic map generated a negative correlation coefficient of −0.0635, which signifies that there is no linear correlation between the two signals, as shown in Fig. 10, here also Graphs labeled a and b correspond respectively to Audio 1 in the original form and encrypted form. Likely to the results obtained in the previous section, graphs *c and d represent the original and the encrypted Audio 2, while graphs *e and f represent the original and the encrypted Audio 3.

Table 2
Correlation analysis.

Audio	Correlation Original	Correlation Encrypted
2D map	0.9346	0.2562
3D map	0.9351	−0.0635
FF(Ref. [49])	0.973813	0.000006
GB(Ref. [49])	0.974584	−0.000424
IM(Ref. [49])	0.948969	0.000014
PP(Ref. [49])	0.963028	−0.000013

$$r(X,Y) = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2 \sum_{i=1}^{n}(Y_i - \overline{Y})^2}} \tag{3}$$

where:

$\overline{X}$ and $\overline{Y}$ are the means of X and Y, respectively.

X: The original audio signal values.

Y: The encrypted audio signal values.

6.3. Peak signal-to-noise ratio (PSNR)

Peak transmission-to-noise Ratio (PSNR) [50] is a crucial statistic for assessing how well the encrypted audio transmission is performing. It calculates the ratio of a signal's full potential power to the power of noise that tampers with the representation of the signal, reducing its accuracy. Greater PSNR numbers, which tend to infinity, show that the encryption procedure preserved the signal quality very well. Higher PSNR values generally indicate greater quality of the encrypted audio. The evaluation revealed that the 3D hyperchaotic quadratic map and the 2D memristive hyperchaotic map both attained PSNR values that tended to infinity, indicating exceptional signal quality retention during encryption.

$$\text{PSNR} = 10 \cdot \log_{10}\left(\frac{\text{MSE}}{\text{MAX}^2}\right) \tag{4}$$

where:

MAX is the maximum possible pixel value of the signal (usually 255 for 8-bit signals),

MSE is the mean squared error between the original and distorted signals.

6.4. Signal-to-noise ratio (SNR)

The Signal-to-noise ratio (SNR) [51] is the key metric when determining how well the encryption process is negotiated. The Signal-to-noise ratio (SNR) is the ratio of a useful logical signal to background noise. The more the number that SNR is, the better the operation of your encryption. The above figures depict the SNR value obtained during testing, where both of the encryption algorithms show the

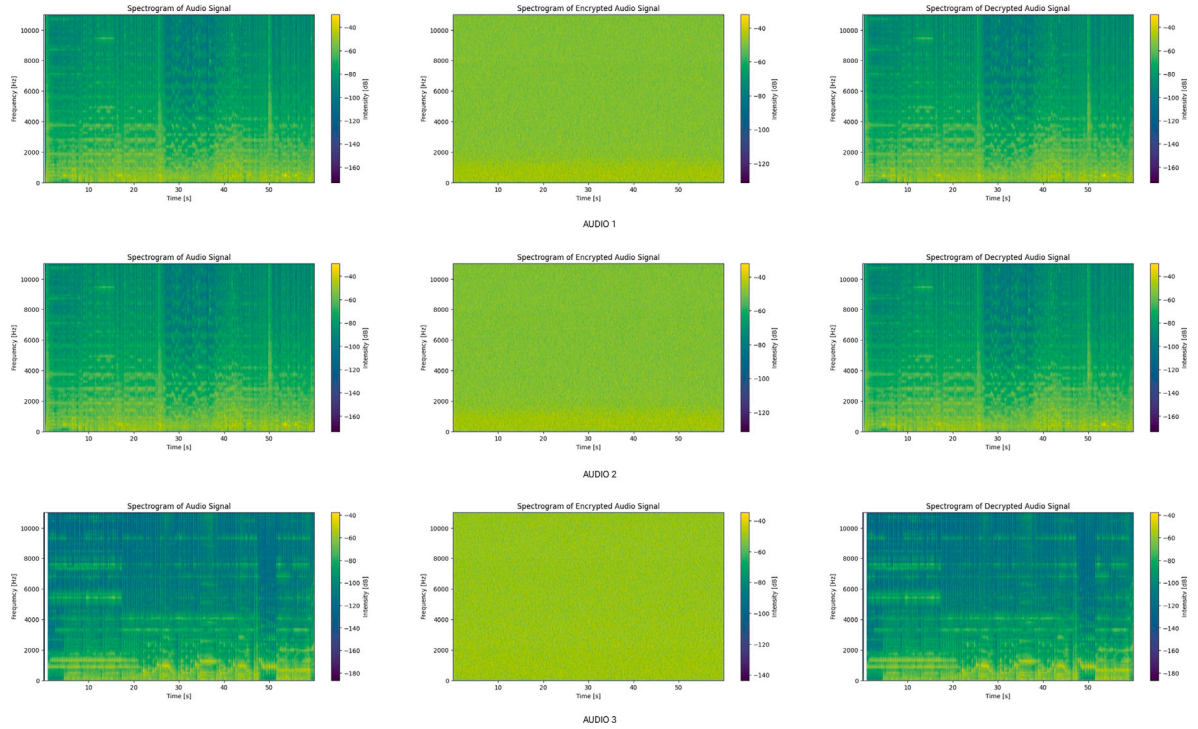

Fig. 7. Comparison of spectrograms before and after encryption using a 2D map, highlighting the similarity between the original and decrypted signals.

results as infinity, which clearly shows that there is no loss in signal quality while doing encryption.

$$\text{SNR} = 10\log_{10}\left(\frac{\sum_{i=1}^{N} S_i^2}{\sum_{i=1}^{N}(S_i - D_i)^2}\right)$$

where:

S_i represents the original audio signal samples.

D_i represents the decrypted (or reconstructed) audio signal samples.

N is the total number of samples in the audio signal.

In this formula, $\sum_{i=1}^{N} S_i^2$ is the power of the original signal, and $\sum_{i=1}^{N}(S_i - D_i)^2$ is the power of the noise, which is the difference between the original and decrypted signals.

6.5. Key sensitivity analysis

To assess the protection and resistance of encryption techniques, key sensitivity analysis is important. It scrutinizes how modifications in the encryption key affect audio quality after it has been decrypted for audio encryption. The 3D map encryption technique under examination herein, as well as the two-dimensional (2D) map encryption scheme, is unique. In this regard, a little difference between original and decrypted audio signals that amounted to 3.78e−07 was observed among a sample of users on average. This indicates high sensitivity to changes in audible decrypted audio even with slight fluctuations in key settings. Nevertheless, the 3D map encryption technique displayed an average distinction of 16424.11 and a highest variation of 32691. This large difference implies that the 3D map encryption technique is highly reactive to key alterations leading to large differences in decrypted audio. The above findings demonstrate issues associated with audio quality and data integrity when even minimal changes are made to a key. Further study is needed on the general mechanisms of this high level of sensitivity to identify opportunities for enhancing audio encryption algorithms.

Table 3
Comparison of UACI values for different audio files.

AUDIO FILE	UACI
AUDIO 2D	34.5287
AUDIO 3D	32.6787
Ref. [52]	33.682
Ref. [53]	33.00
Ref. [54]	33.2824

6.6. Unified average changing intensity (UACI)

Unified Average Changing Intensity (UACI) [55] computes the average intensity change rate between the original signal and the encrypted signal. High UACI values show that the encrypted audio has changed substantially, which means that the encryption algorithms work well by disturbing the original signal completely. This disturbance plays an important role in making sure that the encrypted audio does not contain any recognizable patterns from the original signal and therefore enhancing security for those using it. In the 2D memristive hyperchaotic map, the UACI score was 34.5287; whereas the 3D hyperchaotic quadratic Map was 32.6787, refer to Table 3.

$$\text{UACI} = \frac{1}{N}\sum_{i=1}^{N}\left(\frac{|S_i - D_i|}{255}\right) \times 100$$

where:

S_i represents the original signal samples.

D_i represents the encrypted signal samples.

N is the total number of samples in the signal.

6.7. Spectrogram comparison: 2D vs. 3D encryption

The images provide a visual comparison of spectrograms before and after encryption using two different methods: a 2D map and a 3D map. In the 2D map encryption method, the original spectrogram

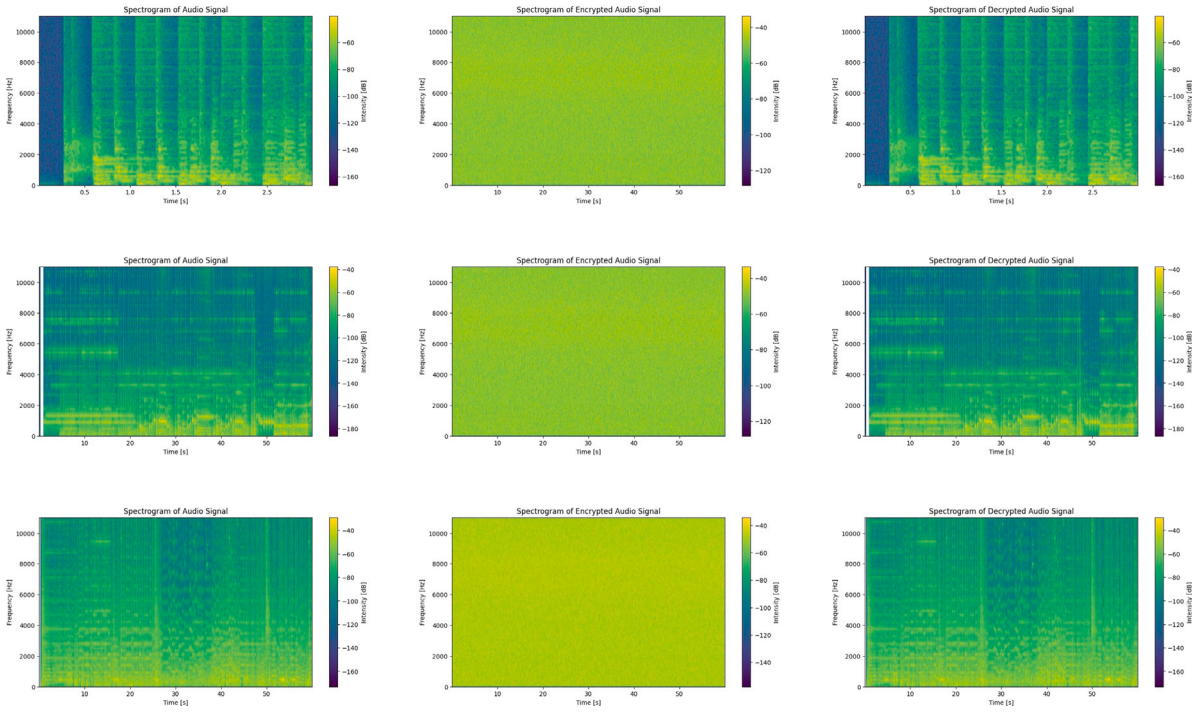

Fig. 8. Comparison of spectrograms before and after encryption using 3D hyperchaotic map, highlighting the similarity between the original and decrypted signals.

Table 4
NSCR values for different audio files.

AUDIO FILE	NSCR
Audio 2D	100.0000
Audio 3D	99.9984
Ref. [52]	99.6300
Ref. [53]	98.0000

shows the time–frequency representation of the audio signal before encryption, which transforms into noise in the encrypted spectrogram, illustrating the encryption's effectiveness in obscuring the signal. The decrypted spectrogram closely matches the original, confirming successful recovery as in Fig. 7. For the 3D chaotic system, the original spectrogram again represents the audio signal before encryption, but the encrypted spectrogram appears as an even more complex noise due to the added security of the 3D chaotic system as shown in Fig. 8. Despite this complexity, the decrypted signal retains similarity with the original, demonstrating both the robustness of the encryption and the effectiveness of the decryption process.

6.8. Number of samples change rate (NSCR)

Number of Samples Change Rate (NSCR) [56] computes the percentage of sample values that differ between the original and encrypted audio signals. Large NSCR values suggest that many of the samples under consideration altered in the course of the encryption step. This statistic is useful for demonstrating that the encryption method completely altered the original audio, resulting in a considerably different encrypted signal that is more secure against unauthorized access. The evaluation revealed that the 2D memristive hyperchaotic map had an NSCR value of 100.0 and the 3D hyperchaotic quadratic map had an NSCR value of 99.9984 as mentioned in Table 4.

$$\text{NSCR} = \left(\frac{D}{N}\right) \times 100$$

where:

Table 5
Evaluation metrics for encryption schemes.

	2D memristive hyperchaotic map	3D hyperchaotic quadratic map
Entropy of Encrypted audio	7.8105	7.7991
Correlation of Original Audio	0.9346	0.9351
Correlation of Original Audio (after encryption)	0.2562	−0.0635
Value of NSCR	100.0	99.9984
Value of UACI	34.5287	32.6787
SNR	46.698 dB	51.250 dB
PSNR	72.11 dB	55.395 dB

D is the number of differing samples between the original and encrypted signals.

N is the total number of samples in the signal.

6.9. Power spectral density (PSD)

The Power Spectral Density (PSD) analysis of decrypted audio signals processed through 3D hyperchaotic quadratic map-based and 2D map-based encryption schemes reveals distinct patterns in frequency content, as shown in Figs. 11 and 12. The PSD plots for the 3D hyperchaotic system exhibit a broad and complex distribution of power across a wide frequency range, indicative of the chaotic nature of the encryption, which effectively disperses spectral power and enhances security by obscuring the original signal's frequency content. In contrast, the PSD plots for the 2D map-based encryption show a more concentrated and predictable power distribution across specific frequency bands, suggesting a less chaotic influence on the signal. The comparison indicates that the 3D hyperchaotic quadratic map introduces greater complexity into the frequency content, potentially offering stronger encryption, while the 2D map, though effective, results in a more constrained spectral impact with different security implications.

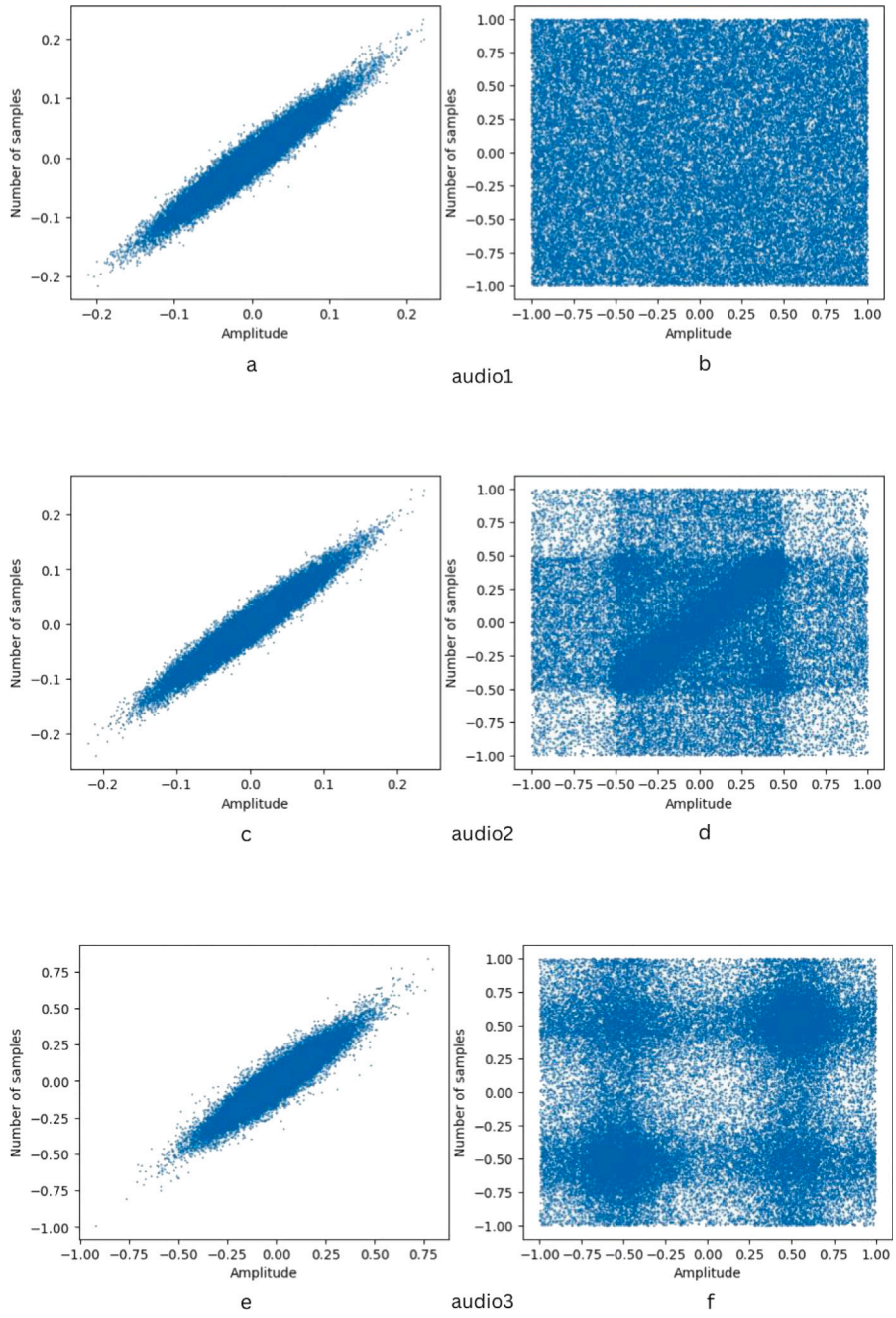

Fig. 9. Comparison of correlation coefficients before and after encryption using a 2D map. The change in correlation values illustrates the impact of encryption on the relationship between original and encrypted data.

7. Results

The results indicate that the encryption method using both maps was extremely effective in achieving high entropy levels, indicating the utmost complexity and randomness of the encrypted audio signals. The encryption process effectively maintained secrecy by disrupting the original audio's correlation. The outcome of the Unified Average Changing Intensity (UACI) and Number Sample Change Rate (NSCR) indicate that the encrypted audio seems to be strongly encrypted with low distortion or alteration. Additionally, the Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR) tended to infinity, implying that the signal quality was preserved well and that low noise was introduced during encryption.

These findings support the usefulness of chaotic maps for audio encryption and offer a safe and dependable way to protect confidential audio information.

8. Conclusion

In this paper, an area of audio encryption using chaotic maps has been explored where we have taken 2D and 3D hyperchaotic maps for the purpose. After analyzing it in detail prominence of a chaotic

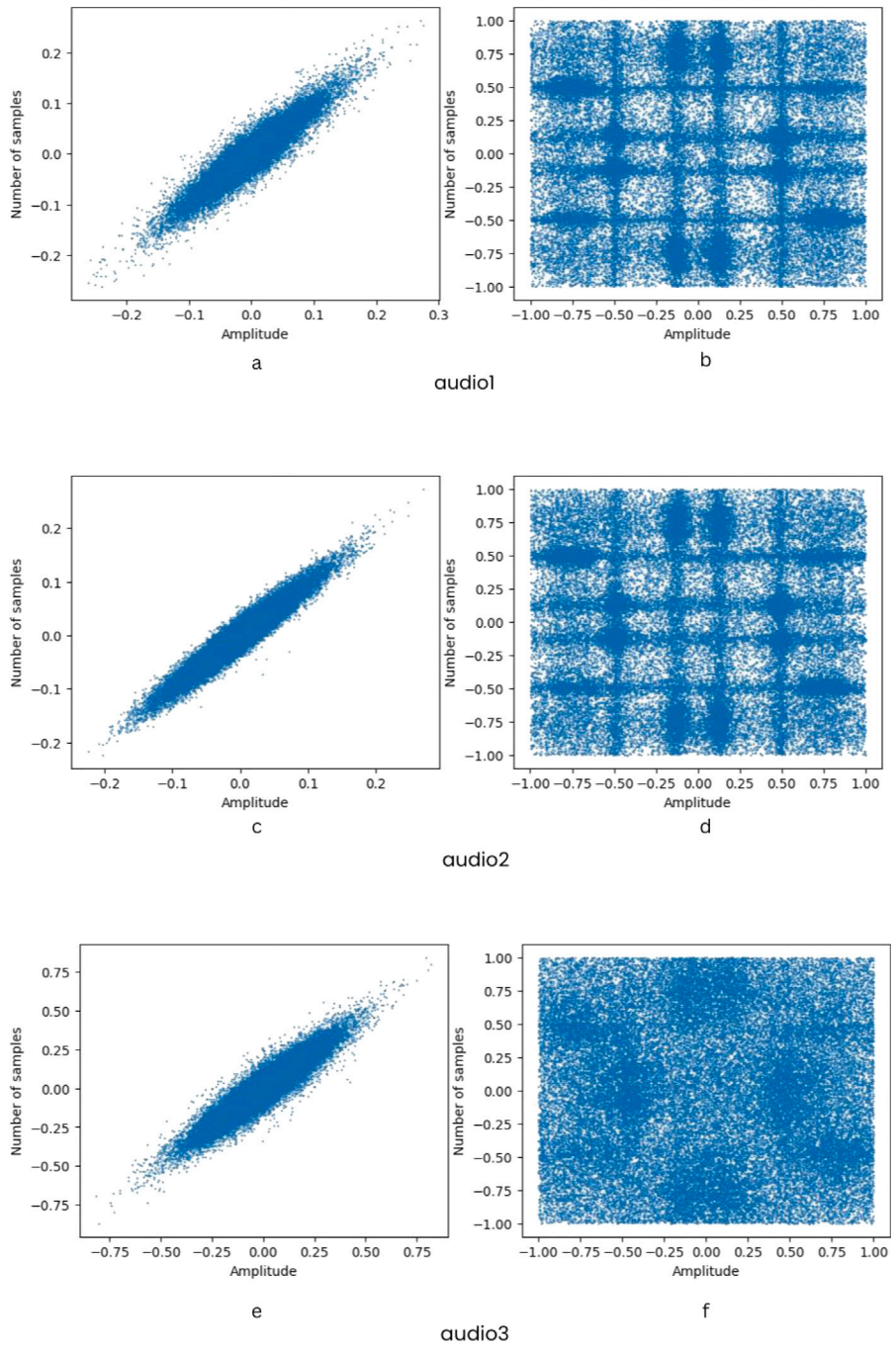

Fig. 10. Comparison of correlation coefficients before and after encryption using a 3D map. The change in correlation values illustrates the impact of encryption on the relationship between original and encrypted data.

system in the area of encryption has been presented due to its initial condition sensitivity and its pseudo-randomness generation capability both of which are required for secure encryption.

Hence, from our research, we can conclude that chaotic maps are efficient carriers of audio encryption. They give a reliable mechanism for converting the audio data into a form that is very hard to decode without the right authorization. In light of this fact, each unpredictable behavior of chaotic dynamics was established by using machine learning methodologies and computational forecasting strategies to understand the complexity and unpredictability of these dynamics. Power Spectral Density (PSD) plot of the 2D map. This plot illustrates the frequency content of the encrypted audio signal generated using the 2D map-based encryption scheme The abundance of other metrics, such as entropy, correlation, NSCR, UACI, SNR, and PSNR, has proved that our experiments confirm the effectiveness of both 2D memristive hyperchaotic maps and 3D hyperchaotic quadratic maps in the encryption of audio data. These results affirm the suitability of chaotic maps for encryption purposes as they offer high levels of secrecy and security.

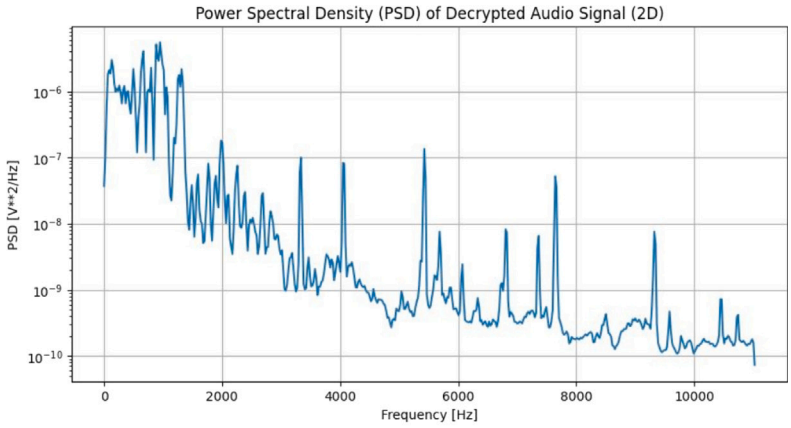

Fig. 11. Power Spectral Density (PSD) plot of the 2D map. This plot illustrates the frequency content of the encrypted audio signal generated using the 2D map-based encryption scheme.

In future research, it would be beneficial to explore higher-dimensional chaotic systems to improve encryption strength and resistance to attacks. Incorporating machine learning into hyperchaotic encryption could offer adaptive security solutions. It would also be valuable to investigate real-time implementation in mobile devices and IoT systems. Additionally, performance analyses, including energy consumption and computational efficiency, will help optimize these methods for resource-constrained environments. Expanding the research to secure other multimedia data, such as video and images, and collaborating with cryptographic experts for formal security evaluations will further establish the credibility and adoption of hyperchaotic encryption schemes.

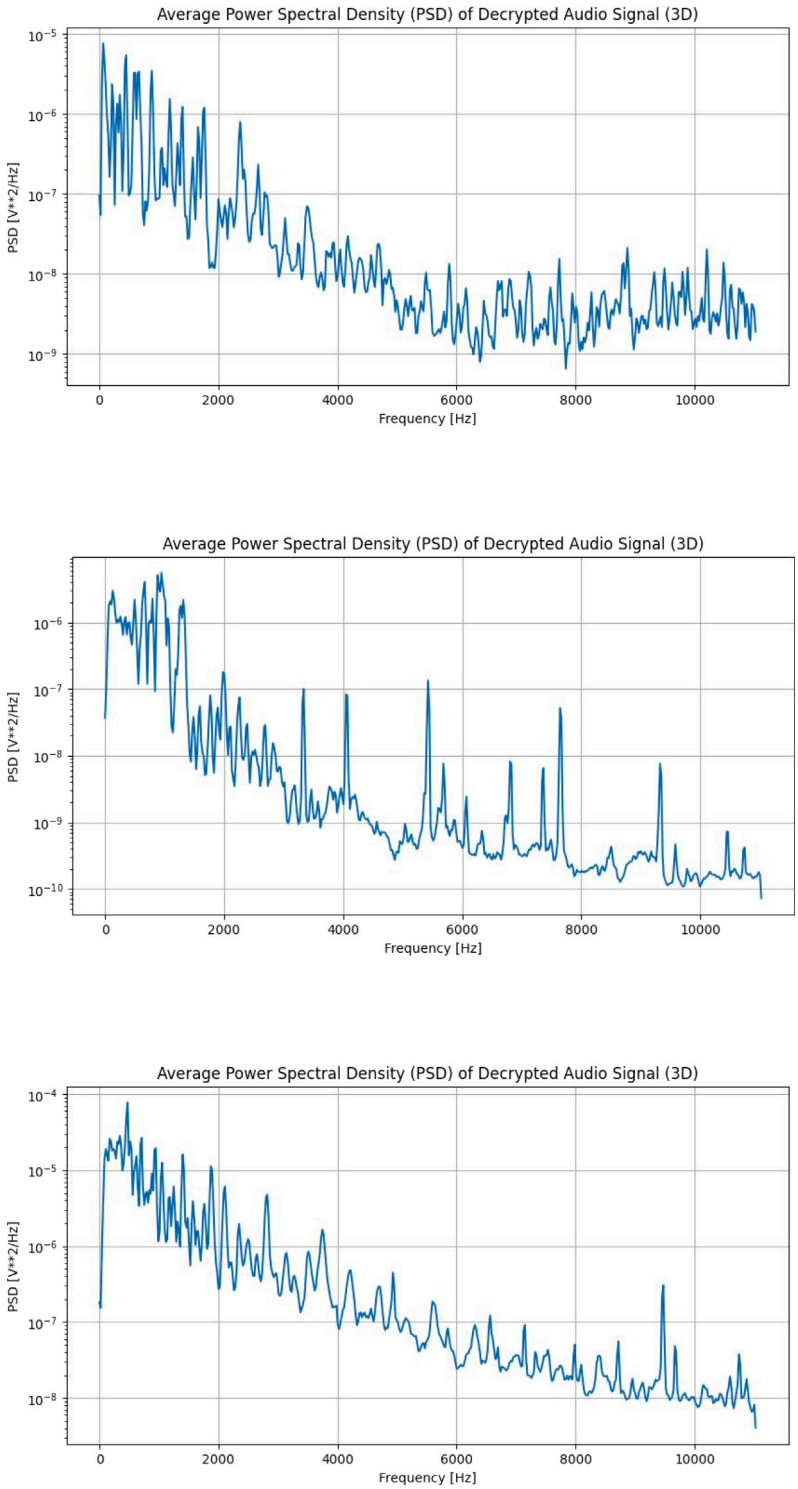

Fig. 12. Power Spectral Density (PSD) plot of the 3D hyperchaotic quadratic map. This plot illustrates the frequency content of the encrypted audio signal generated using the 3D hyperchaotic quadratic map-based encryption scheme.

CRediT authorship contribution statement

Thejas Haridas: Writing – review & editing, Writing – original draft, Visualization, Validation, Investigation, Formal analysis, Data curation, Conceptualization. **Upasana S.D.:** Writing – review & editing, Writing – original draft, Visualization, Software, Methodology, Formal analysis, Data curation, Conceptualization. **Vyshnavi G.:** Writing – review & editing, Writing – original draft, Visualization, Methodology, Formal analysis. **Malavika S. Krishnan:** Writing – review & editing, Visualization, Formal analysis. **Sishu Shankar Muni:** Writing –

review & editing, Visualization, Supervision, Resources, Project administration, Methodology, Investigation, Formal analysis, Data curation, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The data that support the findings of this study are available within the article.

Acknowledgments

We express our gratitude to Bharath V Nair and Vismaya V S for insightful discussions and for making figure corrections.

References

[1] F.Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, CRC Press, 2017.
[2] Q. Lawande, B. Ivan, S. Dhodapkar, Chaos based cryptography: a new approach to secure communications, BARC Newslett. 258 (258) (2005).
[3] J. Banks, J. Brooks, G. Cairns, G. Davis, P. Stacey, On Devaney's definition of chaos, Am. Math. Mon. 99 (4) (1992) 332–334.
[4] G. Qi, G. Chen, S. Du, Z. Chen, Z. Yuan, Analysis of a new chaotic system, Phys. A 352 (2–4) (2005) 295–308.
[5] W. Ditto, T. Munakata, Principles and applications of chaotic systems, Commun. ACM 38 (11) (1995) 96–102.
[6] W.A. Brock, D.A. Hsieh, B.D. LeBaron, Nonlinear Dynamics, Chaos, and Instability: Statistical Theory and Economic Evidence, MIT Press, 1991.
[7] A. Akgul, S. Kacar, I. Pehlivan, B. Aricioglu, Chaos-based encryption of multimedia data and design of security analysis interface as an educational tool, Comput. Appl. Eng. Educ. 26 (5) (2018) 1336–1349.
[8] L.S. Storch, J.M. Pringle, K.E. Alexander, D.O. Jones, Revisiting the logistic map: a closer look at the dynamics of a classic chaotic population model with ecologically realistic spatial structure and dispersal, Theor. Popul. Biol. 114 (2017) 10–18.
[9] J. Lü, G. Chen, D. Cheng, A new chaotic system and beyond: the generalized Lorenz-like system, Int. J. Bifurcation Chaos 14 (05) (2004) 1507–1537.
[10] F.R. Marotto, Chaotic behavior in the Hénon mapping, Comm. Math. Phys. 68 (1979) 187–194.
[11] M.F. Abd Elzaher, M. Shalaby, Two-level chaotic system versus non-autonomous modulation in the context of chaotic voice encryption, in: 2021 International Telecommunications Conference, ITC-Egypt, IEEE, 2021, pp. 1–6.
[12] S.A. Al Nahian, Z. Hosen, P. Ahmed, An elementary study of chaotic behaviors in 1-D maps, J. Appl. Math. Phys. 7 (5) (2019) 1149–1173.
[13] R.B. Naik, U. Singh, A review on applications of chaotic maps in pseudo-random number generators and encryption, Ann. Data Sci. 11 (1) (2024) 25–50.
[14] W.S. Sayed, A.G. Radwan, A.A. Rezk, H.A. Fahmy, et al., Finite precision logistic map between computational efficiency and accuracy with encryption applications, Complexity 2017 (2017).
[15] M. Agarwal, Arvind, R. Ratan, Analysis of Bao-Zhou-Chen-Liu's hybrid chaotic system, in: Soft Computing: Theories and Applications: Proceedings of SoCTA 2022, Springer, 2023, pp. 303–315.
[16] H. Li, Z. Hua, H. Bao, L. Zhu, M. Chen, B. Bao, Two-dimensional memristive hyperchaotic maps and application in secure communication, IEEE Trans. Ind. Electron. 68 (10) (2020) 9931–9940.
[17] W. Li, W. Yan, R. Zhang, C. Wang, Q. Ding, A new 3D discrete hyperchaotic system and its application in secure transmission, Int. J. Bifurcation Chaos 29 (14) (2019) 1950206.
[18] H.A. Abdallah, S. Meshoul, A multilayered audio signal encryption approach for secure voice communication, Electronics 12 (1) (2022) 2.
[19] A.D. Algarni, N.F. Soliman, H.A. Abdallah, F.E. Abd El-Samie, Encryption of ECG signals for telemedicine applications, Multimedia Tools Appl. 80 (2021) 10679–10703.
[20] A. Flores-Vergara, E.E. García-Guerrero, E. Inzunza-González, O.R. López-Bonilla, E. Rodríguez-Orozco, J.R. Cárdenas-Valdez, E. Tlelo-Cuautle, Implementing a chaotic cryptosystem in a 64-bit embedded system by using multiple-precision arithmetic, Nonlinear Dynam. 96 (2019) 497–516.
[21] D. Trujillo-Toledo, O. López-Bonilla, E. García-Guerrero, E. Tlelo-Cuautle, D. López-Mancilla, O. Guillén-Fernández, E. Inzunza-González, Real-time RGB image encryption for IoT applications using enhanced sequences from chaotic maps, Chaos Solitons Fractals 153 (2021) 111506.
[22] E. Rodríguez-Orozco, E.E. García-Guerrero, E. Inzunza-Gonzalez, O.R. López-Bonilla, A. Flores-Vergara, J.R. Cárdenas-Valdez, E. Tlelo-Cuautle, FPGA-based chaotic cryptosystem by using voice recognition as access key, Electronics 7 (12) (2018) 414.
[23] D. Murillo-Escobar, M.Á. Murillo-Escobar, C. Cruz-Hernández, A. Arellano-Delgado, R.M. López-Gutiérrez, Pseudorandom number generator based on novel 2D Hénon-Sine hyperchaotic map with microcontroller implementation, Nonlinear Dynam. 111 (7) (2023) 6773–6789.
[24] V.K. Tamba, V.-T. Pham, A.A. Shukur, G. Grassi, S. Momani, Oscillator without equilibrium and linear terms: Dynamics and application, Alex. Eng. J. 97 (2024) 376–384.
[25] A. Gokyildirim, U.E. Kocamaz, Y. Uyaroglu, H. Calgan, A novel five-term 3D chaotic system with cubic nonlinearity and its microcontroller-based secure communication implementation, AEU-Int. J. Electron. Commun. 160 (2023) 154497.
[26] Y.-B. Huang, P.-W. Xie, J.-B. Gao, Q.-Y. Zhang, A robust chaotic map and its application to speech encryption in dual frequency domain, Int. J. Bifurcation Chaos 33 (08) (2023) 2350096.
[27] M.A. Mohamed, T. Bonny, A. Sambas, S. Vaidyanathan, W.A. Nassan, S. Zhang, K. Obaideen, M. Mamat, M. Nawawi, M. Kamal, A speech cryptosystem using the new chaotic system with a capsule-shaped equilibrium curve, Comput. Mater. Contin. 75 (3) (2023).
[28] S.A. Gebereselassie, B.K. Roy, Speech encryption algorithm based on two newly designed chaotic maps, Franklin Open 5 (2023) 100055.
[29] A. Akgül, S. Kaçar, İ. Pehlivan, An audio data encryption with single and double dimension discrete-time chaotic systems, Tojsat 5 (3) (2015) 14–23.
[30] G. Li, Y. Pu, B. Yang, J. Zhao, Synchronization between different hyper chaotic systems and dimensions of cellular neural network and its design in audio encryption, Cluster Comput. 22 (Suppl 3) (2019) 7423–7434.
[31] A.A. Shukur, M.A. AlFallooji, V.-T. Pham, Asymmetrical novel hyperchaotic system with two exponential functions and an application to image encryption, Nonlinear Eng. 13 (1) (2024) 20220362.
[32] K. Iskakova, M.M. Alam, S. Ahmad, S. Saifullah, A. Akgül, G. Yılmaz, Dynamical study of a novel 4D hyperchaotic system: An integer and fractional order analysis, Math. Comput. Simulation 208 (2023) 219–245.
[33] N.R. Babu, M. Kalpana, P. Balasubramaniam, A novel audio encryption approach via finite-time synchronization of fractional order hyperchaotic system, Multimedia Tools Appl. 80 (2021) 18043–18067.
[34] S. Gao, J. Liu, H.H.-C. Iu, U. Erkan, S. Zhou, R. Wu, X. Tang, Development of a video encryption algorithm for critical areas using 2d extended schaffer function map and neural networks, Appl. Math. Model. (2024).
[35] S. Gao, H.H.-C. Iu, M. Wang, D. Jiang, A.A.A. El-Latif, R. Wu, X. Tang, Design, hardware implementation, and application in video encryption of the 2-D memristive cubic map, IEEE Internet Things J. 11 (12) (2024) 21807–21815, http://dx.doi.org/10.1109/JIOT.2024.3376572.
[36] S. Gao, H.H.-C. Iu, J. Mou, U. Erkan, J. Liu, R. Wu, X. Tang, Temporal action segmentation for video encryption, Chaos Solitons Fractals 183 (2024) 114958.
[37] S. Gao, R. Wu, X. Wang, J. Liu, Q. Li, X. Tang, EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory, Inform. Sci. 621 (2023) 766–781.
[38] A.A. Neamah, A.A. Shukur, A novel conservative chaotic system involved in hyperbolic functions and its application to design an efficient colour image encryption scheme, Symmetry 15 (8) (2023) 1511.
[39] H. Bao, Z. Hua, H. Li, M. Chen, B. Bao, Discrete memristor hyperchaotic maps, IEEE Trans. Circuits Syst. I. Regul. Pap. 68 (11) (2021) 4534–4544, http://dx.doi.org/10.1109/TCSI.2021.3082895.
[40] B.V. Nair, V.V. S, S.S. Muni, A. Durdu, Deep learning and chaos: A combined approach to image encryption and decryption, 2024, http://dx.doi.org/10.48550/ARXIV.2406.16792, arXiv URL https://arxiv.org/abs/2406.16792.
[41] S.S. Muni, Ergodic and resonant torus doubling bifurcation in a three-dimensional quadratic map, Nonlinear Dynam. 112 (6) (2024) 4651–4661, http://dx.doi.org/10.1007/s11071-024-09284-6.
[42] S.S. Muni, Pathways to hyperchaos in a three-dimensional quadratic map, Eur. Phys. J. Plus 139 (7) (2024) http://dx.doi.org/10.1140/epjp/s13360-024-05438-y.
[43] A.S. Abo-Taleb, M. Nabil, M. Shalaby, S. Elramly, An enhanced SHA3-based hashing method: A side-channel attack countermeasure, in: Proceedings of the 8th International Conference on Software and Information Engineering, 2019, pp. 145–150.
[44] M. Singh, D. Garg, Choosing best hashing strategies and hash functions, in: 2009 IEEE International Advance Computing Conference, IEEE, 2009, pp. 50–55.
[45] G. Rilling, P. Flandrin, P. Goncalves, et al., On empirical mode decomposition and its algorithms, in: IEEE-EURASIP Workshop on Nonlinear Signal and Image Processing, Vol. 3, Grado: IEEE, 2003, pp. 8–11.
[46] N. Ahmed, T. Natarajan, K.R. Rao, Discrete cosine transform, IEEE Trans. Comput. 100 (1) (1974) 90–93.

[47] A. Ayenu-Prah, N. Attoh-Okine, A criterion for selecting relevant intrinsic mode functions in empirical mode decomposition, Adv. Adapt. Data Anal. 2 (01) (2010) 1–24.
[48] S. Gao, H.H.-C. Iu, M. Wang, D. Jiang, A.A. Abd El-Latif, R. Wu, X. Tang, Design, hardware implementation, and application in video encryption of the 2D memristive cubic map, IEEE Internet Things J. (2024).
[49] A. Maity, B.C. Dhara, An audio encryption scheme based on empirical mode decomposition and 2D cosine logistic map, IEEE Lat. Am. Trans. 22 (4) (2024) 267–275.
[50] P. Yadav, M. Dutta, 3-level security based spread spectrum image steganography with enhanced peak signal to noise ratio, in: 2017 Fourth International Conference on Image Information Processing, ICIIP, IEEE, 2017, pp. 1–5.
[51] O.A. Imran, S.F. Yousif, I.S. Hameed, W.N.A.-D. Abed, A.T. Hammid, Implementation of El-Gamal algorithm for speech signals encryption and decryption, Procedia Comput. Sci. 167 (2020) 1028–1037.
[52] F. Farsana, K. Gopakumar, Speech encryption algorithm based on nonorthogonal quantum state with hyperchaotic keystreams, Adv. Math. Phys. 2020 (1) (2020) 8050934.
[53] N. Sasikaladevi, K. Geetha, K. Venkata Srinivas, A multi-tier security system (SAIL) for protecting audio signals from malicious exploits, Int. J. Speech Technol. 21 (2018) 319–332.
[54] I. Ahmed, A. Khan, N. Ahmad, NasruMinallah, H. Ali, Speech signal recovery using block sparse bayesian learning, Arab. J. Sci. Eng. 45 (3) (2020) 1567–1579.
[55] R. Saidi, N. Cherrid, T. Bentahar, H. Mayache, A. Bentahar, Number of pixel change rate and unified average changing intensity for sensitivity analysis of encrypted inSAR interferogram, Ingénierie des Systèmes d Inf. 25 (5) (2020) 601–607.
[56] M. Demirtaş, A lossless audio encryption method based on Chebyshev map, Orclever Proc. Res. Dev. 2 (1) (2023) 28–38.