 http://dx.doi.org/10.14500/aro.11869

A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators

Ameer K. Jawad, Gholamreza Karimi†, and Mazdak Radmalekshahi

Department of Electrical Engineering, Faculty of Electrical and Computer Engineering,
Razi University, Kermanshah, Iran

***Abstract*—Improved speech encryption is needed for digital voice communications. Data security requires advanced encryption against cyberattacks. Traditional encryption may not be able to handle advanced threats or large datasets. This study uses chaotic system features to create a secure and adaptive digital audio encryption algorithm and enhances public audio encryption. Three hyperchaotic systems allow digital audio signal randomized encryption. The first system generates chaotic random integer numbers as keys, the second selects non-sequential indices to increase unpredictability, and the third randomly samples the digital audio signal and encrypts it through XOR operations with selected key, making it harder for intruders to learn the encryption pattern. The proposed system uses Diffie-Hellman key exchange for key agreement. We have tested and proven the efficiency of the proposed algorithm. The encrypted audio signals, achieving a Peak Signal-to-Noise Ratio (PSNR) of around −20 dB, exhibit high distortion, spectral complexity, very low correlation (round to zero), high entropy, and minimal time delay compared to other articles, making them resistant to decryption attempts by attackers. The system has a large key space of 1345 bits, and its randomized nature and extensive key space protect sensitive audio data in public communication channels, even with minor changes to hyper-chaos generators. The proposed algorithm represents a significant advancement in the field of digital audio encryption. The researchers have utilized chaotic systems to create a strong and flexible encryption system. This algorithm is suitable for military and medical communications that require a high level of audio data security.**

***Index Terms*—Audio encryption, Chaotic sequences, Hyperchaotic systems, Key space, Randomized encryption.**

I. Introduction

Digital audio systems are popular for their technical and practical benefits. Effective recording, storage, signal processing, and quality are available (Nguyen, et al., 2005). Digital audio works well with new technology, enabling interoperability. Its portability and storage enable high-quality, lossless data transfer over communication networks and efficient file storage on digital media. Due to these benefits, digital audio systems are preferable for communications, audio recording, and file storage. Digital speech encryption encrypts speech for privacy and security (Abdullah, et al., 2022; Hussein, Khashan and Jawad, 2020). Cryptographic methods render audio signals or speech data incomprehensible to unauthorized listeners. Only authorized recipients with decryption keys can decipher encrypted speech. Speech encryption uses digital signal processing, symmetric or asymmetric encryption, and secure key management (Dai, et al., 2022). Symmetric encryption uses a shared secret key for encryption and decryption (Ibrahim and Mohammed, 2022; Kumar Shrivasta, Bhatnagar and Pangaria, 2013), while asymmetric encryption involves a pair of public and private keys. The encrypted speech data are transmitted over secure channels or networks to prevent interception and eavesdropping. Encryption protects sensitive information exchanged during audio calls, conference calls, audio messages, or other verbal communication (Hassan, Al-Adhami and Mahdi, 2022).

A. Chaos-Based Audio Encryption

Audio encryption based on chaos utilizes chaotic systems and their properties to encrypt speech signals. Chaos theory studies complex and unpredictable behavior arising from simple non-linear dynamical systems (Nien, et al., 2007). Chaotic systems exhibit sensitivity to initial conditions (Ene, Pop and Lapadat, 2022), non-periodic behavior (Hasan, Mosleh and Abdulhameed, 2021), and deterministic randomness. In speech encryption based on chaos, chaotic systems generate encryption keys or transform the speech signal itself. The chaotic properties of the system introduce randomness and complexity, making it difficult for unauthorized individuals to decipher the encrypted speech (Sathiyamurthi, et al., 2018; Tolba, et al., 2018). Chaotic maps or flows, such as the logistic map or Lorenz system, generate pseudo-random numbers that can be encrypted using a chaotic encryption algorithm. These systems are ideal for encryption due to their randomness and starting condition sensitivity, and can withstand cryptographic attacks and cryptanalysis (Abdullah, Hreshee and Jawad, 2015; Mahdi, Jawad and Hreshee, 2016).

ARO-The Scientific Journal of Koya University
Vol. XII, No. 2 (2024), Article ID: ARO.11869. 12 pages
DOI: 10.14500/aro.11869
Received: 15 October 2024; Accepted: 11 December 2024
Regular research paper; Published: 21 December 2024
†Corresponding author's e-mail: ghkarimi@razi.ac.ir

B. The Primary Objective of this Article

The main aim of this research is to develop a secure and efficient audio encryption algorithm capable of protecting sensitive audio data transmitted over public channels. We intend to propose a solution that provides enhanced security and performance by examining the shortcomings of current techniques and exploiting the advantages of hyperchaotic systems.

C. The Specific Contributions of this Study Include

- A novel audio encryption algorithm based on three hyperchaotic Rabinovich systems
- A detailed analysis of the security and performance of the proposed algorithm
- A comparison of the proposed algorithm with existing techniques and future research directions.

By addressing these issues, this research contributes to the advancement of audio encryption techniques and enhances the security of digital audio communication systems.

D. Limitations

While the proposed algorithm offers significant improvements in security and efficiency, it is important to acknowledge its limitations. The computational complexity of the algorithm may increase with larger audio files. In addition, the security of the system relies on the secrecy of the initial conditions and parameters of the hyperchaotic systems. Because cryptographic algorithms use symmetric encryption, key management remains challenging and has limitations.

E. The Main Contributions

This study introduces a novel audio encryption system that utilizes three hyperchaotic systems based on the Rabinovich system to enhance the security of public communication channels. The proposed algorithm uses three hyperchaotic systems or one with different initial values and parameters. The first chaotic system generates chaotic random integer numbers (CRINs) between 0 and 65535 (2^{16}), the second selects a random index from the sequence of the first system, and the third selects digital audio samples (DAS) from the digitized audio signal. XOR the third chaotic selector selects DAS and CRIN bit by bit. Unlike traditional systems, the proposed encryption system uses random DAS numbers instead of sequential ones.

F. Paper Structures and Sections

The article is organized as follows: Starting with the abstract and section one for introduction, the literature review in the second section, and then defining chaotic systems and their types, especially the hyper-chaotic Rabinovich system in the third section, and then the encryption algorithm is explained in full steps in the fourth section. The fifth section describes the subjective and objective measurements used in the evaluation of cryptography are described. The sixth section contains the simulation results of encryption, decryption, and calculating the key space reached in this paper. The seventh section of the paper deals with the final conclusions.

II. Literature Review

There are many methods for audio signal encryption: Time domain scrambling (TDS), frequency domain scrambling, Two-Dimensional Scrambling Based on Time and Frequency (2DS), and Chaotic Masking (Abdullah, Hreshee and Jawad, 2016). In (Hreshee, Abdullah and Jawad, 2018; Jawad, Abdullah and Hreshee, 2018), a secure communication system that is based on two levels of encryption, namely chaotic scrambling and chaotic masking, was proposed. In (Ouannas, et al., 2021), a secure communication method combines chaotic modulation, recursive encryption, and chaotic masking using backstepping control rules, synchronizing two hyperchaotic Lorenz systems with encrypted states, and recursive encryption techniques. In (Yousif, 2023), a comparison of the performance of the RSA and El-Gamal algorithms for the encryption and decryption of speech data were presented. In (Ameen and Hreshee, 2023), the security of encrypted audio based on elliptic curves and hybrid chaotic maps was investigated in the context of 5G networks. In (Qasim, 2023), a new audio encryption algorithm that is based on a hyper-chaotic system was proposed. In (Tomita, Okumura and Okamoto, 2023), a chaos-based radio encryption modulation system using LabVIEW, program-defined radio, and Universal Software Radio Peripheral demonstrated effectiveness in binary phase-shift keying and information-theoretic and computational security. In (Ilyas, et al., 2022), the reconfigurable 4D Lorenz Hyperchaotic-based IoT device security core platform was proposed to secure real-time communication between embedded systems linked to networks using IoT standards. It is built using VHSIC Hardware Description Language architecture. In (Samimi, Majidi and Khorashadizadeh, 2020), a safe communication system based on chaotic synchronization, an intelligent controller with a brain-based emotional learning architecture is presented. Emotional learning is applied to assess uncertainty and provide the correct information to the receiver. In (Gao, et al., 2022), the TDS can be hidden with the help of a suggested system that uses two optical dispersion components and an electro-optic self-feedback phase modulation loop. In (Giap, Nguyen and Huang, 2021), a linear synchronization control strategy was implemented by converting Lorenz chaotic system-based secure communication into Takagi-Sugeno fuzzy systems. (Zhang, et al., 2022) suggested that modified projective difference function synchronization (CMPDFS) of CVCSs might provide a safe communication method for wireless sensor networks while also addressing amplitude concerns. (Abdullah, et al., 2022; Abdullah, Hreshee and Jawad, 2015; Mahdi, Jawad and Hreshee, 2016) presented speech encryption based on chaotic masking by the Lorenz system and multiple methods to reduce the noise effect on the recovered speech signal at the receiver side. (Hussein, Khashan and Jawad, 2020) presented two stages of chaotic

masking based on Lorenz and Rossler systems and proposed a noise reduction scheme based on an analog-to-digital converter. In (Abdelfatah, 2020), self-adaptive scrambling, multi-chaotic maps, dynamic DNA encoding, and cipher feedback encryption are four independent audio encryption approaches used in the same framework to provide the described safe audio encryption. In (Pirdawood, Kareem and Zahir, 2023), the Laplace transformation is used in the framework that has been proposed for the purpose of audio encryption. In (Barua and Kabir, 2022), encryption and decryption of audio by changing properties and noise reduction was proposed. In (Sajaa and Al-Mothafar, 2024), it was proposed to perform an evaluation of the Rijndael algorithm for audio encryption using brute force attack is carried out.

III. Chaos and Hyper Chaos Definition and Types

Chaos signals are non-periodic, dynamic, and random signals originating from non-linear processes, controlled by ordinary differential equations (ODE) in an interactive system. These signals fluctuate in a limited, non-periodic, random-like manner, resulting in two-state variable motions or trajectories that are easily uncorrelated (Abdullah, et al., 2022; Abdullah, Hreshee and Jawad, 2015; Khalid, et al., 2019). Chaos can be classified into chaotic maps and chaotic flows, with chaotic maps being evolution functions that behave in some way. Discrete-time maps, such as Logistic, Duffing, and Henon maps, are typical representations of discrete maps. Chaotic-Flow systems, such as the Lorenz, Rössler, and Chua systems, are well-known chaotic flow systems with differential equations (Hussein, Khashan and Jawad, 2020; Mahdi, Jawad and Hreshee, 2016).

Hyper-Chaos is an autonomous continuous-time system (a part of chaotic flows) with at least four dimensions and two positive Lyapunov exponents (Alsaabri and Hreshee, 2021; Shakir, Mehdi and Hattab, 2023). The Les for the Rabinovich system is (9.712, 1.457, −4.445, and −15.724), which indicates that it is a hyper-chaotic system. As a result, it gains from increased randomness and unpredictability, which is crucial in communication security. Fig. 1 shows a time series for all vectors and non-uniform 3D attractors of the studied HCRS. The following equations comprise the HCRS (Alsaabri and Hreshee, 2021):

$$\left.\begin{aligned} \dot{x} &= ry - ax + yz \\ \dot{y} &= rx - by - xz \\ \dot{z} &= -dz + xy + w^2 \\ \dot{w} &= xy + cw \end{aligned}\right\} \quad (1)$$

Where (x, y, z, and w) are the state vectors, (r, a, b, c, and d) are the control parameters.

The HCRS is susceptible to slight changes in the control parameters or initial conditions, resulting in a significant difference in the system's behavior. Fig. 2 illustrates the concept by showing the waveform in the time domain of the x(t) state after changing X_0 and parameter C by 10^{-15}.

IV. The Proposed Encryption and Decryption System

The proposed system (Fig. 3) uses three hyperchaotic systems to encrypt a digital audio signal. The system works as follows:

1. The first chaotic system generates a sequence of CRINs between 0 and (2^{16}–1). These numbers are then used to encrypt the digital audio signal.

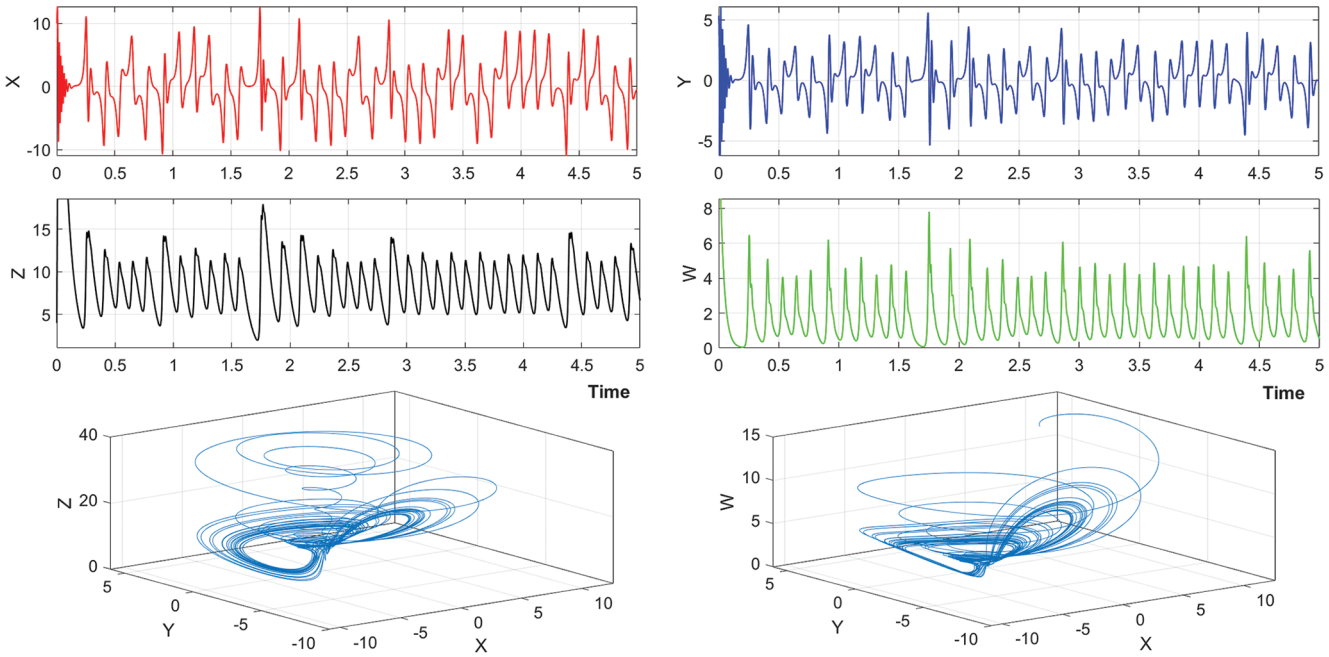

Fig. 1. Time series (X, Y, Z, and W) vectors and 3D attractors (X, Y, and Z), (X, Y, and W) for the HRCS.

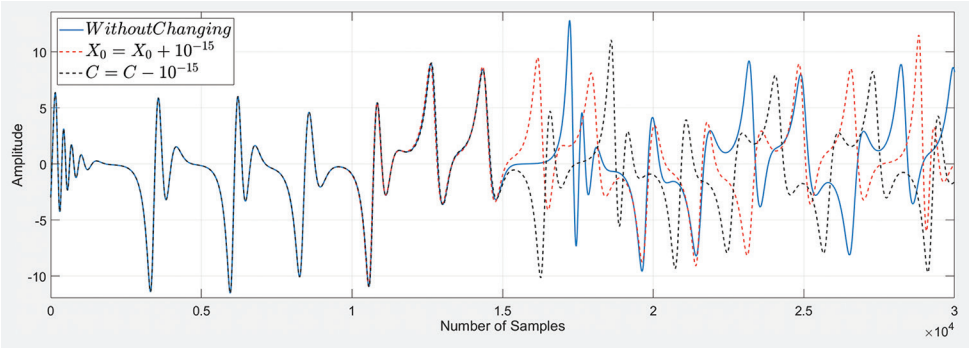

Fig. 2. Sensitivity to any slight change in initial values and control parameters.

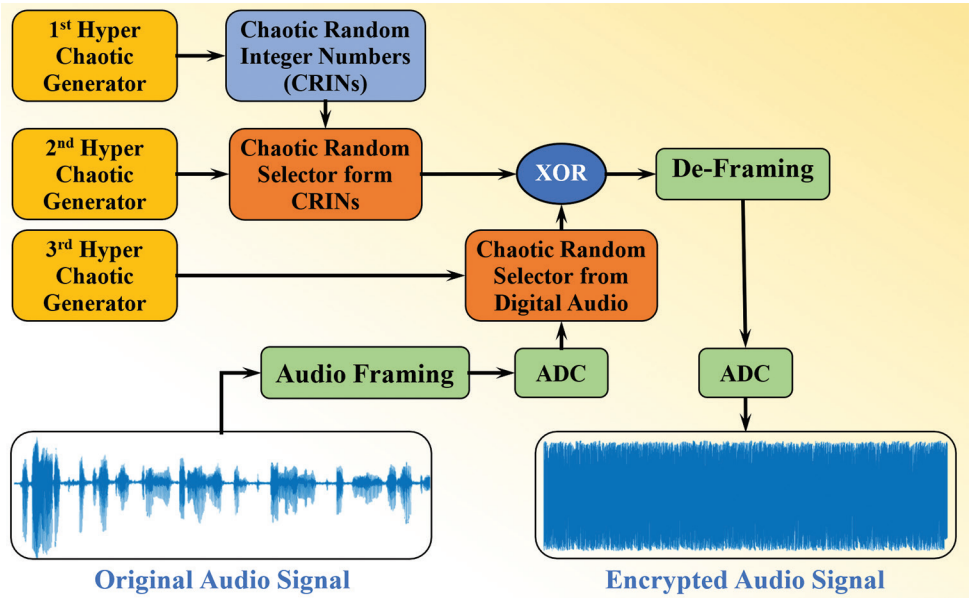

Fig. 3. Block diagram of the proposed audio encryption model.

2. The second chaotic system selects a random index from the sequence of CRINs generated by the first system to ensure that the CRINs used to mask the audio signal are not used in a predictable order.
3. The third chaotic system selects a random sample from the digital audio signal. This sample is then XORed with the CRIN chosen by the second system. This XOR operation encrypts the audio signal.

The proposed scrambling algorithm is described in the following steps:

Step 1. Initialization

This step establishes the three hyperchaotic systems' initial conditions and parameters. These initial conditions and parameters greatly affect chaotic dynamics and random numbers. Different initial conditions and parameters produce different chaotic sequences, improving system security.

Step 2. Generating chaotic signals

The simplest numerical method used to solve the ODE of the Rabinovitch system is the Euler method (Sathiyamurthi, et al., 2018; Xu and Cao, 2020), as shown in the following Equation:

$$y_{n+1} = y_n + hf(x) \quad (2)$$

Where h represents a step size, usually a small value such as 0.001. Generating (X, Y, Z, and W) by the Euler method solving the Rabinovitch system given in (1), as shown in the following equations:

$$\begin{aligned} x_{n+1} &= x_n + h(ry_n - ax_n + yz_n) \\ y_{n+1} &= y_n + h(rx_n - by_n - x_n z_n) \\ z_{n+1} &= z_n + h(-dz_n + x_n y_n + w_n^2) \\ w_{n+1} &= w_n + h(x_n y_n + cw_n) \end{aligned} \quad (3)$$

Where (n) and (n + 1) are the present and the next state. This Equation will generate a number with a high correlation between adjacent chaotic samples.

Step 3. Addressing correlation and generating CRINs

This step addresses the high correlation between adjacent chaotic samples (CS), which can weaken the randomness of the generated sequence. Multiplying by a large number and taking the remainder helps decorate the sequence but might limit the possible values obtained. This step converts the continuous chaotic signal into a sequence of "Chaotic Random Integer Numbers" (CRINs) (Fig. 4) suitable for masking the audio samples. Modulo operation ensures the CRINs remain within a specific range (0–65535 in this case), allowing for efficient

http://dx.doi.org/10.14500/aro.11869

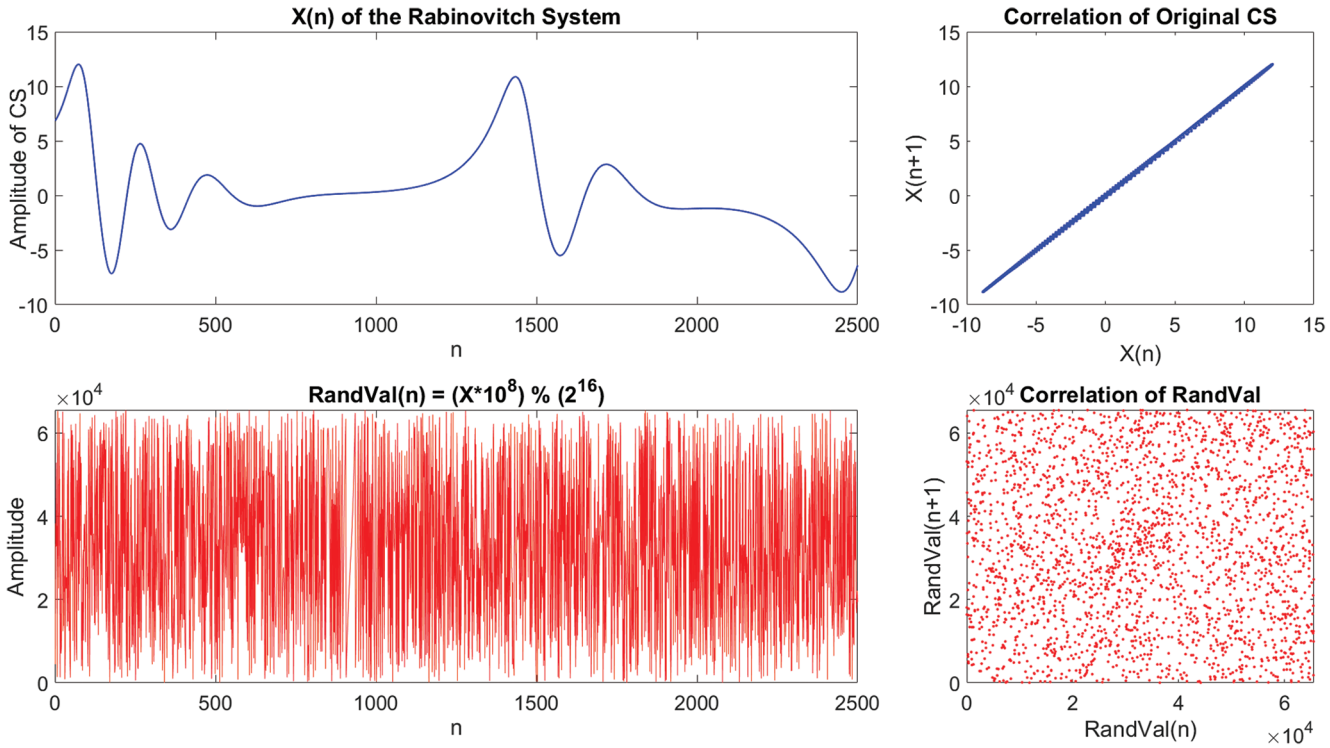

Fig. 4. The correlation between chaotic samples for original and random chaotic signals.

manipulation during encryption, as shown in the following equation:

$$RandVal = mod(x(n)*10^{8}), 2^{16}) \quad (4)$$

$$CRIN = round(RandVal) \quad (5)$$

Where: CS is Chaotic Sequences, and *CRIN* is a "Chaotic Random Integer Numbers" generated based on hyperchaotic signals.

Step 4. Sorting and indexing

Sorting the results from the second and third hyperchaotic systems introduces non-linearity and randomness into the selection process. Assigning new indices based on the sorted order further obfuscates the relationship between the original chaotic sequence and the selected indices (Fig. 5). In step 4, we have n = 12 in our sequence. Thus, the new index representation is in Table I.

Step 5. Audio encryption

To encrypt audio, a DAS (Digital Audio Sample) based on a chaotic selection from the second and third systems XORs the CRINs from the first hyperchaotic system. The XOR operation encrypts audio data by masking it with random values, as shown in equation (6). After converting the digital encryption samples back to analog, we de-frame the encrypted frames to create an encrypted audio signal.

$$\text{Encrypted} = \text{CRIN}(\text{CRS}_1) \otimes \text{DAS}(\text{CRS}_2) \quad (6)$$

Where CRS_1 & CRS_2: Chaotic Random Selectors from the second and third HCRSs.

Step 6. Audio decryption

Finally, on the receiver side, employing identical keys as those used in the transmitter (the same initial values and parameters) and obtaining similar results (*CRINs*, CRS_1, and CRS_2) from three HCRSs, the following equation governs the decryption process:

$$\text{Decrypted}(\text{CRS}_2) = \text{CRIN}(\text{CRS}_1) \otimes \text{Encrypted} \quad (7)$$

V. The assessment of Audio Encryption Involves Both Subjective and Objective Testing

The proposed audio encryption scheme will undergo rigorous statistical tests and visual comparisons to assess its security and overall performance. Key metrics include mean squared error (MSE), PSNR, signal-to-noise ratio (SNR), correlation, entropy, number of pixels with a change in intensity, and unified average changed intensity. Visual comparisons include waveform, histogram, correlation, and FFT plots.

A. Correlation and Histogram Plots

The correlation figure represents the relationship between the Audio Sample (t) and Audio Sample (t + 1) by scattering plot. A high relationship and correlation between the adjacent audio samples is in the clear or original audio. While, for encrypted audio, the relationship and correlation are neglected. The proposed system will change the audio sample values, changing the histogram of the encrypted audio, increasing the encryption strength of the proposed method (Tan and Zhou, 2010; Vaseghi, et al., 2021).

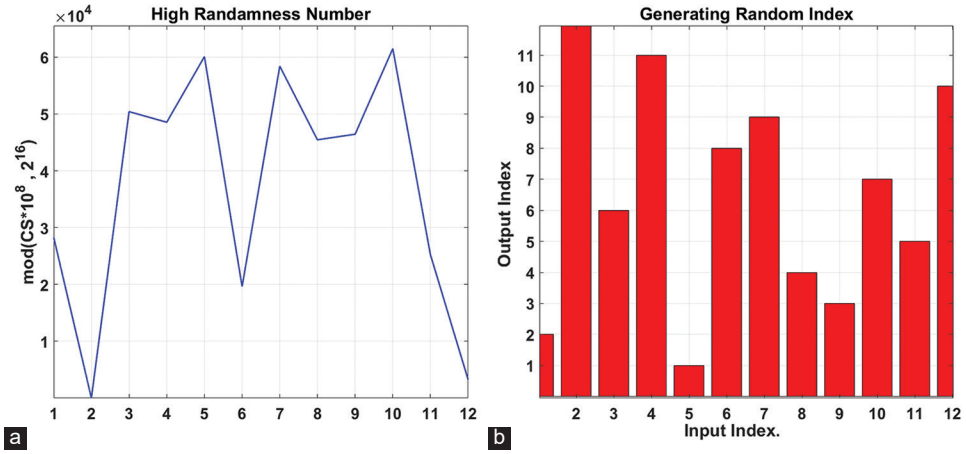

Fig. 5. (a) A high randomness numbers. (b) Generate random locations (steps 4 and 5).

TABLE I
THE OUTPUT RANDOM INDICES USED AS A CHAOTIC RANDOM SELECTOR

Output index	2	12	6	11	1	8	9	4	3	7	5	10

B. PSNR and MSE

The fundamental goal of every cryptographic method is to maximize the difference between ciphered and original data to withstand differential and statistical assaults. The MSE and the PSNR determine the difference between the original and recovered or ciphered audio signals. The mathematical description of MSE and PSNR can be found in equations (8) and (9). (Abood, et al., 2023; Belagali and Udupi, 2023; Hanif, et al., 2020; Majid Msallam and Fayez Aldoghan, 2023):

$$MSE = \frac{\sum_i |x_i - y_i|}{N_{AS}} \tag{8}$$

$$PSNR_{dB} = 10\log\left(\frac{65535^2}{MSE}\right) \tag{9}$$

Where x and y are the original and the encrypted or decrypted audio signal, N_{AS} the number of audio samples.

C. Signal-to-Noise Ratio

The reconstructed signal exhibits greater quality and less distortion than the original signal, indicating potentially skewed or inaccurate data, necessitating subjective metrics (Elkamchouchi, Salama and Abouelseoud, 2020; Hreshee, Abdullah and Jawad, 2018). The formula of SNR is:

$$\mathrm{SNR_{Db}} = 10\log10\left(\frac{\sum x^2}{\sum (x-y)^2}\right) \tag{10}$$

Where x is the original audio signal and y is the audio signal that was encrypted or decrypted.

D. Correlation Coefficients

The correlation coefficient is used to obtain the similarity between two audio signals.

$$Corr. = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}((x_i - E(x)))^2}\sqrt{\sum_{i=1}^{N}((y_i - E(y)))^2}} \tag{11}$$

Where $E(x) = \frac{1}{N}\sum_{i=1}^{N} x(i)$, x and y are the audio sample values of the original and the encrypted audio signal, respectively. When it's 0, the audio signals are different (the original and the encrypted audio signals). If it's 1, the encryption fails to obscure the original audio signal's features (Min, Ting and Yu-jie, 2013).

E. Entropy

Information entropy analysis measures randomness and encryption quality by comparing the Entropy of original and cipher audio signals, calculated using a specific method.

$$E = \sum_{i=0}^{2^n-1}\left[p(i) * log_2\left(\frac{1}{p(i)}\right)\right] \tag{12}$$

Where p(i) is the bit-valued I probability, for audio signals with 65536 audio levels (0–65535), the maximum Entropy equals 16, and it's considered optimum randomness. Practical audio signal entropy is lower than maximal Entropy (Ahmad and Ahmed, 2010).

F. Root Mean Square (RMS) and Crest Factor (CF) Value

Calculating the average audio source amplitude or input signal standard deviation with a mean of zero yields the RMS value (Abdelfatah, 2020; Rahman, et al., 2020). CF is a waveform parameter calculated by dividing peak values by effective value (Abdelfatah, 2020). A higher CF indicates signal peaks, while a 0 Db ratio indicates no peaks. Information is presented:

$$CF = 20\log_{10}\frac{|V_{Peak}|}{V_{RMS}} \tag{13}$$

G. The Audio Signals that are used to evaluate the Proposed System

There are two types of audio signals that are used to evaluate the proposed system; the standard audio signal (audio signal (1) in Fig. 6) is used in these papers: (Abdullah, et al., 2022; Abdullah, Hreshee and Jawad, 2015; 2016; Hreshee, Abdullah and Jawad, 2018; Hussein, Khashan and Jawad, 2020; Mahdi, Jawad and Hreshee,

http://dx.doi.org/10.14500/aro.11869

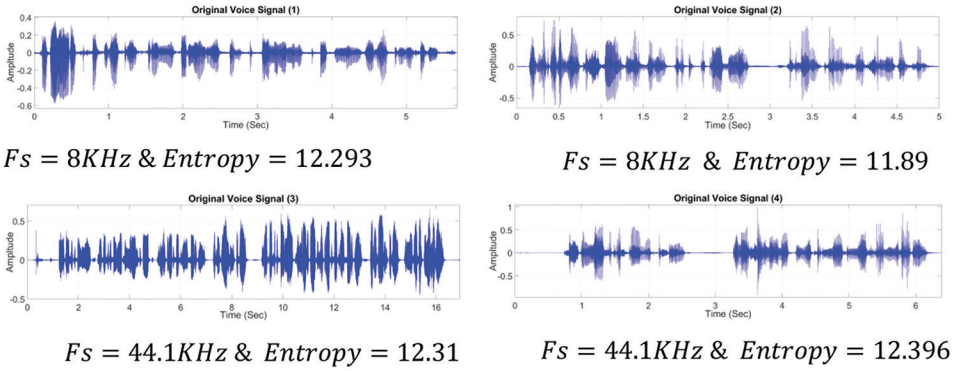

Fig. 6. Time series of the original audio signals.

2016), and recorded immediately with varying lengths (5, 16.6, and 6.5 s) and frequency sampling (8 kHz to 44.1 kHz), respectively, as audio signals (2, 3, and 4 in Fig. 6). The comparison table uses the results from the audio signal (1).

VI. Simulation Results and Discussions

A. Encryption Results

The following Table II provides an illustration of the encryption results of the four audio signals based on the proposed algorithm.

According to Table II, The proposed encryption algorithm introduces high distortion to the signal, resulting in low-quality encrypted audio signals with PSNR values of −19.942 Db or less and SNR values of −39.26 Db, significantly different from the original audio signal. Furthermore, from Table II, The encrypted audio signal significantly differs from the original, making it difficult for eavesdroppers to recover without the encryption key. The Entropy values above 14.74–15.936 indicate that the encrypted signal is unpredictable, making it difficult for eavesdroppers to analyze and decrypt without the encryption key. The proposed algorithm can scramble and encrypt the audio signal, making it unintelligible to eavesdroppers. Furthermore, from Table II, The encryption algorithm is practical for real-time audio communication, with a mean delay of 5 MS for 1 s of encryption at 8,000 Hz and 18.5 MS at 44,100 Hz. The encrypted audio signals have RMS and CF values of 0.57 and 1.73, respectively, indicating no statistical correlation between the original and encrypted signals. The analysis visually compares the characteristics of original and encrypted audio signals, showing waveforms, correlation plots, histograms, frequency domain representation, and color-coded illustrations of energy across frequencies over time exclusively for an encrypted signal.

From Figs. 7 and 8 the encrypted audio signals display negligible correlation between adjacent samples, contributing significantly to the system's security. Histogram plots, revealing a flat distribution, underscore the randomness, and unpredictability introduced through encryption; this intentional obfuscation of signal patterns enhances resistance against cryptographic attacks. The FFT plots demonstrate a wide frequency range in the encrypted audio signals. This spectral complexity enhances the difficulty of signal analysis and attack, fortifying the encryption process against adversaries aiming to exploit specific frequency patterns or weaknesses.

TABLE II
The Objective Encryption Results of the Four Audio Signals

Audio	$PSNR_{Db}$	SNR_{Db}	Corr.	Entropy	RMS	CF	Delay
Audio1	−21.137	−40.105	−0.0014	14.737	0.5776	1.7312	0.021 Sec
Audio2	−19.942	−39.262	−0.0075	14.743	0.5780	1.7301	0.020 Sec
Audio3	−20.009	−39.654	0.0008	15.821	0.5767	1.7341	0.083 Sec
Audio4	−20.851	−40.105	−0.0020	15.936	0.5769	1.7335	0.323 Sec

B. Decryption Results

The following Table III provides an illustration of the encryption results of the four audio signals based on the proposed algorithm.

From Table III, The proposed encryption algorithm effectively recovers the original audio signal from the encrypted signal without distortion or noise, with minimal decryption delay. The decrypted signal's quality is close to the original, with a MSE value of zero and a PSNR value of 94.5 Db, indicating accurate recovery and no significant alteration in the signal's statistical properties.

The graphical encryption (subjective) results from Figs. 9 and 10 showed that the time plots showed the audio signal's amplitude over time, and the decrypted audio signal was similar to the original. FFT plots revealed a similar spectrum to the original audio signal, with highly correlated correlation plots over time. The amplitude of the audio signal at time (t) is similar to time (t + 1), with points clustered around a line with a slope of 1. Decrypted audio signal histogram plots were typically bell-shaped, with most samples clustered around the mean value.

C. Key Sensitivity and Space

Key sensitivity refers to the difficulty in decrypting an encrypted signal if there is a change between encryption and decryption keys. Secure cryptosystems require large sensitivity; meaning only one key factor remains unchanged.

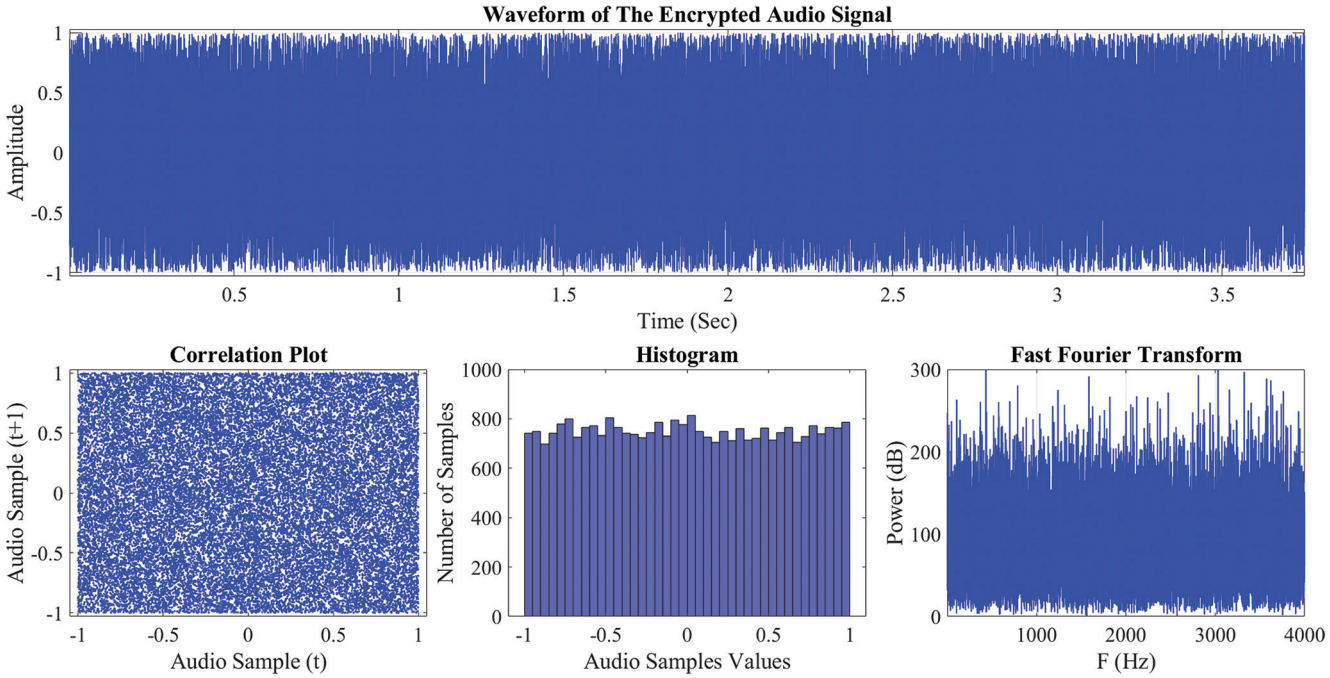

Fig. 7. Subjective encryption results for the 1st audio signal.

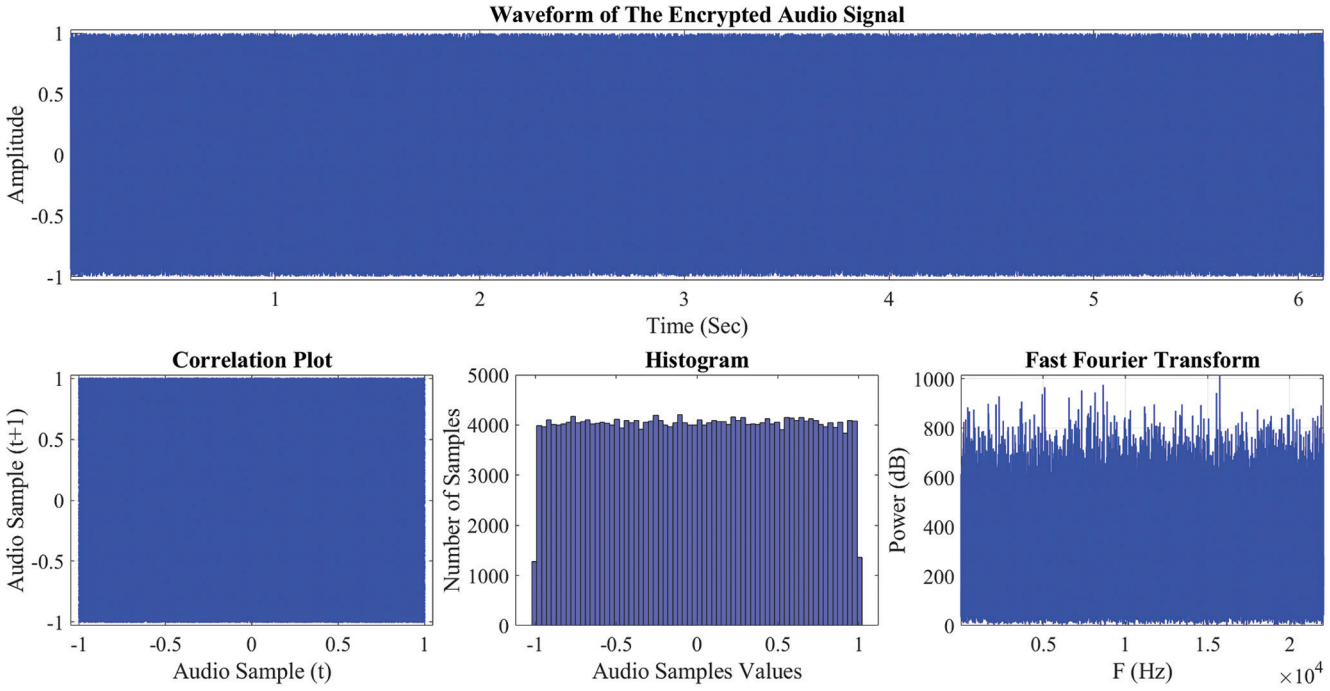

Fig. 8. Subjective encryption results for the 3rd audio signal.

TABLE III
THE OBJECTIVE DECRYPTION RESULTS OF THE FOUR AUDIO SIGNALS

Audio	$PSNR_{Db}$	SNR_{Db}	Corr.	Entropy	RMS	CF	Delay
Audio1	93.717	79.541	1	12.293	0.0850	8.1785	0.018 Sec
Audio2	94.116	75.652	1	11.89	0.0882	8.3798	0.017 Sec
Audio3	96.684	74.472	1	12.31	0.0775	12.901	0.071 Sec
Audio4	93.001	73.748	1	12.396	0.0713	0.0713	0.323 Sec

Even a small change in the initial condition of a key, such as 1×10^{-15}, cannot retrieve information from an attacker.

From Table IV and Fig. 11 notice that when we make a minimal change in any parameter or initial value in the 1st, 2nd, or 3rd HCS generators, the attacker cannot retrieve the audio initially stored. The key space of the proposed scheme used in this paper mainly depends on the five parameters

http://dx.doi.org/10.14500/aro.11869

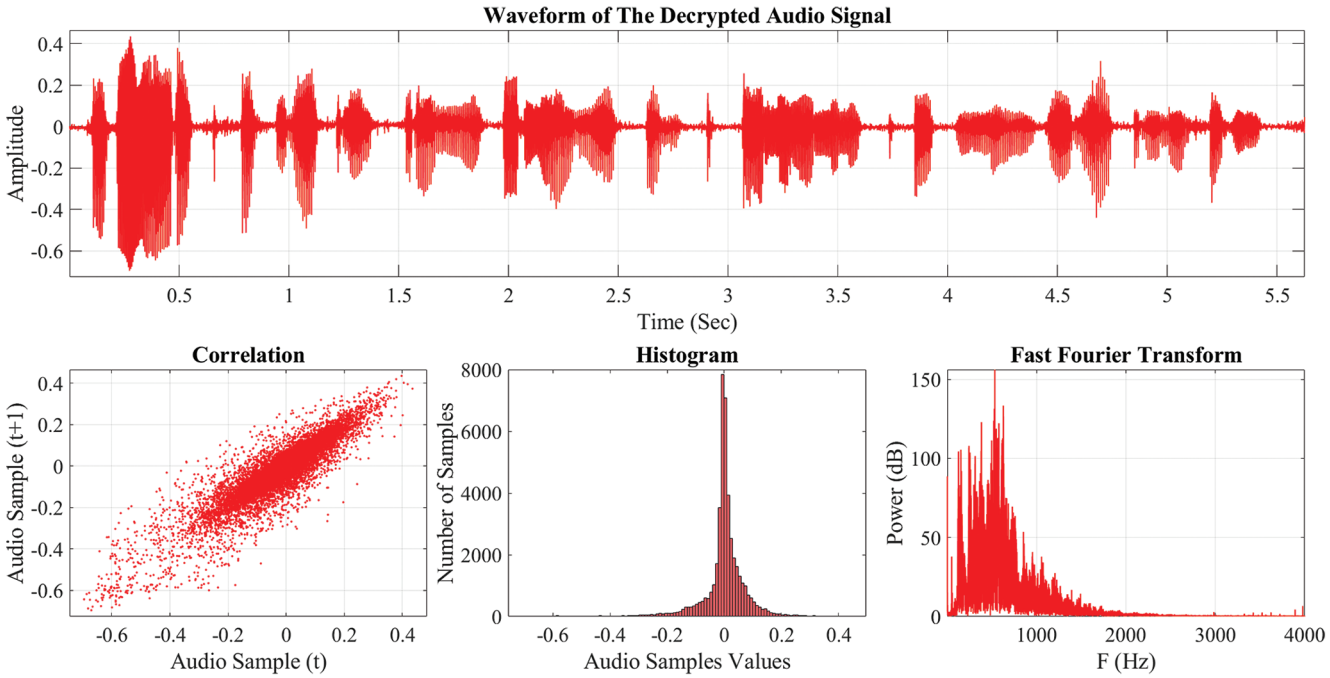

Fig. 9. Subjective decryption results for the 1st audio signal.

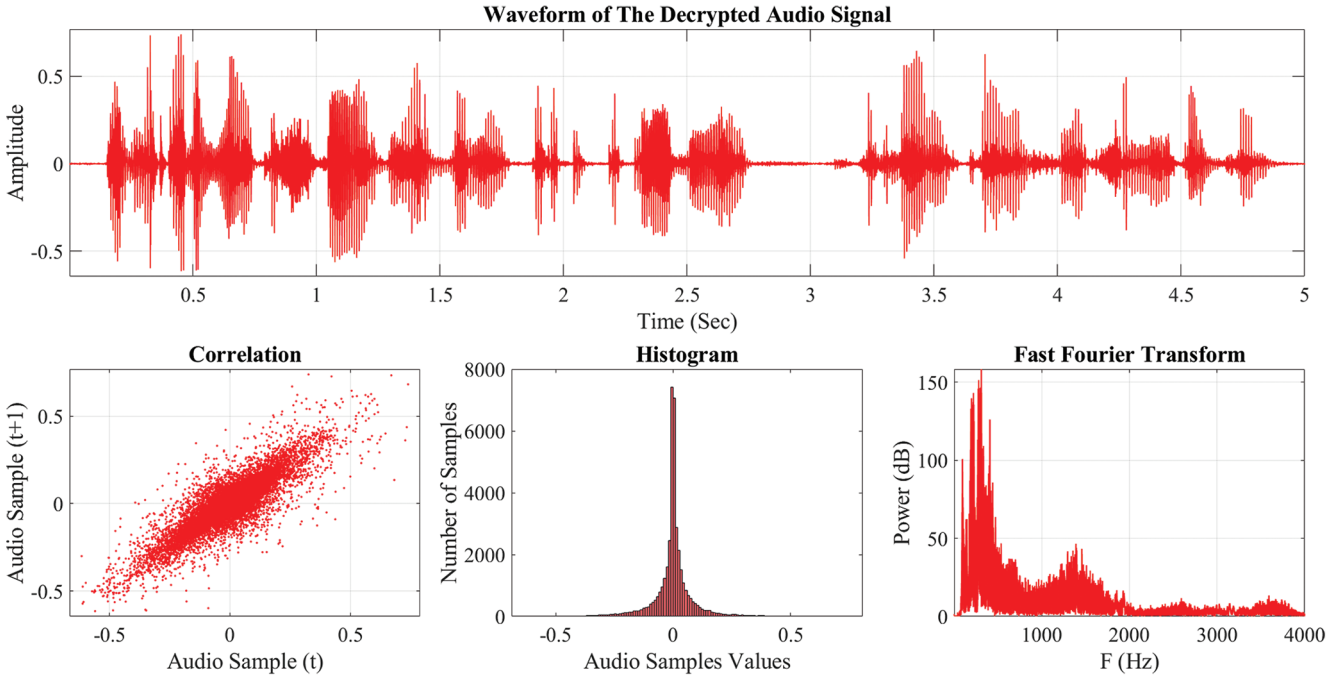

Fig. 10. Subjective encryption results for the 2nd audio signal.

TABLE IV
THE DECRYPTION RESULTS WHEN CHANGING ONE PARAMETER OR INITIAL CONDITION

Change one key	$PSNR_{Db}$	SNR_{Db}	Corr.	Ent.	RMS	CF
$\Delta y1=+10^{-15}$	−20.851	−40.105	0.00043	15.935	0.5771	1.7329
$\Delta r1=-10^{-15}$	−20.854	−40.108	−0.00007	15.941	0.5776	1.7312
$\Delta c2=+10^{-15}$	−20.853	−40.107	0.0004	15.936	0.5769	1.7333
$\Delta x2=-10^{-15}$	−20.848	−40.102	0.00055	15.935	0.5774	1.7320
$\Delta w2=+10^{-15}$	−20.850	−40.105	0.00116	15.935	0.5775	1.7316
$\Delta a3=+10^{-15}$	16.246	−3.008	0.00051	12.396	0.0713	9.1777
$\Delta z3=+10^{-15}$	16.243	−3.011	−0.00031	12.399	0.0714	9.1778

[r, a, b, c, and d] and four initial conditions (x_0, y_0, z_0 & w_0). There are nine coefficients used in the system. The key space of this article is at least.

$$Keys\ for\ one\ HCS = \prod_{1}^{11} \frac{1}{10^{-15}} = \left(\frac{1}{10^{-15}}\right)^{9} = 10^{135} \quad (14)$$

$$All\ Keys\ for\ three\ HCS = (10^{135})^{3} = 10^{405} \quad (15)$$

$$All\ Keys\ in\ Bits\ Representation = 2^{1345} = 1345\ bits \quad (16)$$

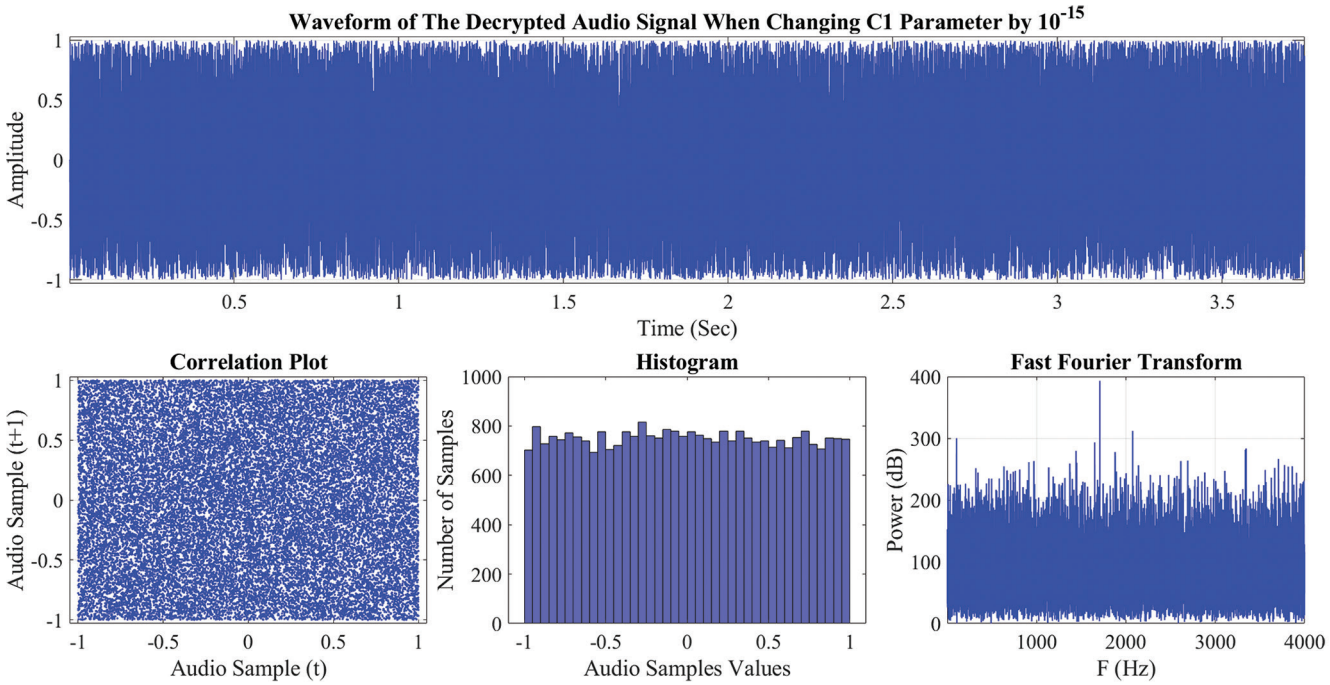

Fig. 11. Decrypted by changing the ©-parameter of the 1st HCS by 10^{-15}.

TABLE V
COMPARING THE PROPOSED STUDY WITH PREVIOUS ARTICLES

Scheme	Key space	$PSNR_{Db}$	SNR_{Db}	Corr.	Entropy	Delay (Sec)
(Ameen and Hreshee, 2023)	510 bits	0.914	−27.81	-	15.911	-
(Ameen and Hreshee, 2022)	500 bits	7.7596	−19.394	−0.0148	13.727	0.022
(Hassan, Al-Adhami and Mahdi, 2022)	512 bits	12.881	7.020	0.4703	-	0.050
El-Gamal (Yousif, 2023)	-	-	−35.56	0.0200	-	0.0175
RSA (Yousif, 2023)	-	-	−38.80	0.032	-	0.0814
(Qasim, 2023)	420 bits	-	-	0.0167	7.9918	0.0687
(Abdelfatah, 2020)	928 bits	4.25	−38.02	0.0005	-	0.0370
Our	1345 bits	−20.84	−40.097	−0.0009	15.936	0.0210

Compare the key space of this article with the algorithms, as illustrated in Table V.

Table V shows that the suggested strategy has the greatest key space (1345 bits) and the strongest brute-force resistance. The proposal has the lowest PSNR (−20.84 Db) and the greatest negative SNR (−40.097 Db).

VII. Conclusions

Three hyperchaotic systems randomly encrypt digital audio signals, increasing security and reducing predictability. The system's random selection and CRIN generation make it hard for intruders to guess next. Eavesdroppers cannot understand the audio signal because the algorithm scrambles and encrypts it. The proposed algorithm distorts encryption, highlighting the encryption strength-signal fidelity trade-off. The algorithm intentionally distorts audio for security. Correlation, histogram, and FFT plots show the algorithm's effectiveness. Decryption yields the original audio signal with zero MSE, minimal distortion, and high PSNR values around 96 Db. Decrypted audio signal correlation plots show a high correlation with themselves over time, ensuring accurate signal recovery. Success in decryption and signal restoration is shown by bell-shaped histogram plots. These visual verifications prove decryption works. This encryption system is suitable for real-time audio communication due to its low delay and consistent graphical encryption results. It is promising for secure communication environments that prioritize efficiency and security. The researcher's recommendation for future work is to use artificial intelligence such as convolutional neural networks for chaotic behavior testing before the encryption process.

References

Abdelfatah, R.I., 2020. Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. *IEEE Access*, 8, pp.69894-69907.

Abdullah, H.N., Hreshee, S.H., and Jawad, A.K., 2015. Design of efficient noise reduction scheme for secure speech masked by chaotic signals. *Journal of American Science*, 11(7), pp.49-55.

Abdullah, H.N., Hreshee, S.H., and Jawad, A.K., 2016. *Noise Reduction of Chaotic Masking System Using Repetition Method*. Available from: https://www.researchgate.net/publication/291356303 [Last accessed on 2024 Oct 10].

Abdullah, H.N., Hreshee, S.S., Karimi, G., and Jawad, A.K., 2022. Performance Improvement of Chaotic Masking System Using Power Control Method. In: *International Middle Eastern Simulation and Modelling Conference 2022, MESM 2022*, pp.19-23.

Abood, E.W., Hussien, Z.A., Kawi, H.A., Abduljabbar, Z.A., Nyangaresi, V.O., Ma, J., Al Sibahee, M.A., and Ali Kalafy, S.A., 2023. Provably secure and efficient audio compression based on compressive sensing. *International Journal of Electrical and Computer Engineering*, 13(1), pp.335-346.

Ahmad, J., and Ahmed, F., 2010. Efficiency analysis and security evaluation of image encryption schemes. *Computing*, 23(4), p.25.

Alsaabri, H.H., and Hreshee, S.S., 2021. Robust Image Encryption Based on Double Hyper Chaotic Rabinovich System. In: 7th *International Conference on Contemporary Information Technology and Mathematics, ICCITM 2021*, pp.146-152.

Ameen, M.J.M., and Hreshee, S.S., 2022. Securing physical layer of 5G wireless network system over GFDM using linear precoding algorithm for massive MIMO and hyperchaotic QR-decomposition. *International Journal of Intelligent Engineering and Systems*, 15(5), pp.579-591.

Ameen, M.J.M., and Hreshee, S.S., 2023. Security analysis of encrypted audio based on elliptic curve and hybrid chaotic maps within GFDM modulator in 5G networks. *Bulletin of Electrical Engineering and Informatics*, 12(6), pp.3467-3479.

Barua, N., and Kabir, A., 2022. Encryption and decryption of audio by changing properties and noise reduction. *International Journal of Innovative Science and Research Technology* 7(9), pp.805-809.

Belagali, P., and Udupi, V.R., 2023. Image steganography based on enhanced payload capacity using hybrid edge detection and least significant bit steganography. *Journal of Harbin Engineering University*, 44(8), pp.1952-1960.

Dai, W., Xu, X., Song, X., and Li, G., 2022. Audio encryption algorithm based on chen memristor chaotic system. *Symmetry*, 14(1), p.17.

Elkamchouchi, H., Salama, W.M., and Abouelseoud,Y., 2020. New video encryption schemes based on chaotic maps. *IET Image Processing*, 14(2), pp.397-406.

Ene, R.D., Pop, N., and Lapadat, M., 2022. Approximate closed-form solutions for the rabinovich system via the optimal auxiliary functions method. *Symmetry,* 14(10), p.2185.

Gao, Z., Su, B., Wu, S., Liao, L., Li, Z., Wang, Y., and Qin, Y., 2022. Security-enhanced chaotic optical communication based on external temporal self-feedback hardware encryption and decryption. *IEEE Photonics Journal*, 14(4), pp.1-8.

Giap, V.N., Nguyen, Q.D., and Huang, S.C., 2021. Synthetic adaptive fuzzy disturbance observer and sliding-mode control for chaos-based secure communication systems. *IEEE Access*, 9, pp.23907-23928.

Hanif, M., Ali Naqvi, R., Abbas, S., Khan, M.A., and Iqbal, N., 2020. A novel and efficient 3D multiple images encryption scheme based on chaotic systems and swapping operations. *IEEE Access*, 8, pp.123536-123555.

Hasan, F.S., Mosleh, M.F., and Abdulhameed, A.H., 2021. FPGA implementation of LDPC soft-decision decoders based DCSK for spread spectrum applications. *International Journal of Electrical and Computer Engineering,* 11(6), pp.4794-4809.

Hassan, N.F., Al-Adhami, A., and Mahdi, M.S., 2022. Digital speech files encryption based on hénon and gingerbread chaotic maps. *Iraqi Journal of Science*, 63(2), pp.830-842.

Hreshee, S.S., Abdullah, H.N., and Jawad, A.K., 2018. A high security communication system based on chaotic scrambling and chaotic masking. *International Journal on Communications Antenna and Propagation*, 8(3), pp.257-264.

Hussein, E.A.R., Khashan, M.K., and Jawad, A.K., 2020. A high security and noise immunity of speech based on double chaotic masking. *International Journal of Electrical and Computer Engineering,* 10(4), pp.4270-4278.

Ibrahim, M.K., and Mohammed, F.T., 2022. Image cryptography based on image processing technique and classification algorithm. *Journal of Algebraic Statistics*, 13(2), pp.989-1001.

Ilyas, B., Raouf, S.M., Abdelkader, S., Camel, T., Said, S., and Lei, H., 2022. An efficient and reliable chaos-based iot security core for UDP/IP wireless communication. *IEEE Access*, 10, pp.49625-49656.

Jawad, A.K., Abdullah, H.N., and Hreshee, S.S., 2018. Secure Speech Communication System based on Scrambling and Masking by Chaotic Maps. In: *IEEE, International Conference on Advances in Sustainable Engineering and Applications, ICASEA 2018 - Proceedings*, pp.7-12.

Khalid, M., Hussein, E.A., and Jawad, A.K., 2019. Digital image encryption based on random seguences and XOR operation. *Journal of Engineering and Applied Sciences,* 14(8), pp.10331-10334.

Kumar Shrivasta, V., Bhatnagar, A., and Pangaria, M., 2013. Enhancement of security in international data encryption algorithm (Idea) by increasing its key length. *International Journal of Advanced Research in Computer and Communication Engineering*, 2, pp.3869-3871.

Mahdi, A., Jawad, A.K., and Hreshee, S.S., 2016. Digital chaotic scrambling of voice based on duffing map. *Communications Engineering Journal*, 1(2), pp.16-21.

Majid Msallam, M., and Aldoghan, F., 2023. Multistage encryption for text using steganography and cryptography. *Journal of Technique*, 5(1), pp.38-43.

Min, L., Ting, L., and Yu-Jie, H., 2013. Arnold Transform Based Image Scrambling Method. In: 3rd *International Conference on Multimedia Technology (ICMT-13)*, Atlantis Press, pp.1302-1309.

Nguyen, K., Adams, R., Sweetland, K., and Chen, H., 2005. A 106-DB SNR hybrid oversampling analog-to-digital converter for digital audio. *IEEE Journal of Solid-State Circuits*, 40(12), pp.2408-2415.

Nien, H.H., Huang, C.K., Changchien, S.K., Shieh, H.W., Chen, C.T., and Tuan, Y.Y., 2007. Digital color image encoding and decoding using a novel chaotic random generator. *Chaos, Solitons and Fractals*, 32(3), pp.1070-1080.

Ouannas, A., Karouma, A., Grassi, G., Pham, V.T., and Luong, V.S., 2021. A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. *Alexandria Engineering Journal*, 60(1), pp.1873-1884.

Pirdawood, M.A., Kareem, S.R., and Zahir, D.C., 2023. Audio encryption framework using the laplace transformation. *Aro-the Scientific Journal of Koya University*, 11(2), pp.31-37.

Qasim, H.A., 2023. A new audio encryption algorithm based on hyper-chaotic system. *Mustansiriyah Journal of Pure and Applied Sciences*, 1(3), pp.85-94.

Rahman, S., Masood, F., Khan, W.U., Ullah, N., Khan, F.Q., Tsaramirsis, G., Jan, S., and Ashraf, M., 2020. A novel approach of image steganography for secure communication based on LSB substitution technique. *Computers, Materials and Continua*, 64(1), pp.31-61.

Sajaa, G.M., and Al-Mothafar, N.S., 2024. Evaluation of rijndael algorithm for audio encryption by brute force attack. *Journal of Engineering*, 30(1), pp.128-141.

Samimi, M., Majidi, M.H., and Khorashadizadeh, S., 2020. Secure communication based on chaos synchronization using brain emotional learning. *AEU - International Journal of Electronics and Communications*, 127, p.153424.

Sathiyamurthi, P., Ramakrishnan, S., Shobika, S., Subashri, N., and Prakavi, M., 2018. Speech and Audio Cryptography System Using Chaotic Mapping and Modified Euler's System. In: *IEEE, International Conference on Inventive Communication and Computational Technologies, ICICCT 2018* (Icicct), pp.606-611.

Shakir, H.R., Mehdi, S.A., and Hattab, A.A., 2023. A new four-dimensional hyper-chaotic system for image encryption. *International Journal of Electrical and Computer Engineering* 13(2), pp.1744-1756.

Tan, Y., and Zhou, W., 2010. Image Scrambling Degree Evaluation Algorithm based on Grey Relation Analysis. In: *Proceedings - 2010 International Conference on Computational and Information Sciences, ICCIS 2010*, pp.511-514.

Tolba, M.F., Sayed, W.S., Radwan, A.G., and Abd-El-Hafiz, S.K., 2018. Chaos-based Hardware Speech Encryption Scheme Using Modified Tent Map and Bit Permutation. In: *International Conference on Modern Circuits and Systems Technologies*, pp.1-4.

Tomita, K., Okumura, M., and Okamoto, E., 2023. Demonstration of chaos-based radio encryption modulation scheme through wired transmission experiments. *IEICE Transactions on Communications*, E106, pp.686-695

Vaseghi, B., Hashemi, S.S., Mobayen, S., and Fekih, A., 2021. Finite time chaos synchronization in time-delay channel and its application to satellite image encryption in OFDM communication systems. *IEEE Acces*, 9, pp.21332-21344.

Xu, W., and Cao, N., 2020. Hardware design of a kind of grid multi-scroll chaotic system based on a MSP430F169 chip. *Journal of Circuits, Systems and Computers*, 29(12), p.20501893.

Yousif, S.F., 2023. Performance comparison between RSA and El-gamal algorithms for speech data encryption and decryption. *Diyala Journal of Engineering Sciences*, 16, pp.123-137.

Zhang, F., Gao, R., Huang, Z., Jiang, C., Chen, Y., and Zhang, H., 2022. Complex modified projective difference function synchronization of coupled complex chaotic systems for secure communication in WSNs. *Mathematics*, 10(7), p.1202.