University of Baghdad
College of Engineering
JOURNAL OF ENGINEERING

Journal of Engineering

journal homepage: www.jcoeng.edu.iq

Volume 32 Number 4 April 2026

Audio Encryption Using Chaotic Systems with Direct Byte-Level Processing

Nagham Malik Abd Ali *, **Tarik Zeyad Ismaeel**

Department of Electrical Engineering, College of Engineering, University of Baghdad, Baghdad, Iraq

ABSTRACT

To protect digital audio transmissions from unauthorized access and modification, this paper proposes a voice encryption scheme based on chaotic systems. The proposed approach combines multiple chaotic maps into a cryptographic scheme that is applied at the byte level. The input sound is first divided into four equal-length parts. The Rossler system, Lorenz system, Henon map, and Baker map are chaotic systems used to encode each fragment. Four segments are combined, and subsequently, a logistic map is applied to the encoded audio to introduce a flipping step, ensuring a strong spread and confusion throughout the entire signal. During the decoding phase, XOR processes and switching are systematically reversed using saved keys, restoring the original audio. The encoded and retrieved audio is evaluated using several tests to ensure the success of the encoding and retrieval process, such as the signal-to-noise ratio (SNR) test, autocorrelation, mean square error (MSE), histogram analysis, and spectrogram comparison. The results demonstrate that the proposed system is highly secure against attackers and possesses a powerful diffusion and confusion mechanism, enhancing speech communication in the field of communications. Hence, the system is suitable for multimedia applications that require an elevated level of confidentiality, including the transmission of sensitive data, digital rights protection, and military communications.

Keywords: Encryption, Decryption, Audio, Chaotic system.

1. INTRODUCTION

The issue of protecting digital multimedia information has garnered a lot of attention in the recent past due to the increased use of cloud storage technology and communication networks. Initially, the development of chaos cryptography targeted text and image encryption due to the ability to manipulate the information using permutation and diffusion processes. Basic mathematical analysis of the controlled Baker map and the behavior of the two-dimensional chaos laid the foundation for the development of chaos cryptography

*Corresponding author
Peer review under the responsibility of University of Baghdad.
https://doi.org/10.31026/j.eng.2026.04.06

Article received: 01/10/2025
Article revised: 12/03/2026
Article accepted: 22/03/2026
Article published: 01/04/2026

systems **(Kuperin and Pyatkin, 2005).** Later, general models and reviews on chaos cryptography explained the use of chaotic systems for encrypting information due to the sensitivity of the systems to initial conditions, ergodicity, and the lack of periodicity in the systems **(Kocarev, 2011)**. On this basis, many image encryption methods using single and multiple chaotic maps with substitution and permutation networks have been developed. For example, Baker maps and logistic chaotic maps were used for improving diffusion and pixel scattering effects **(Sowthily and Brindha, 2018)**, and triple chaotic maps were used for improving statistical security in color image encryption **(Hosny et al., 2024)**. More recent research has proposed hybrid architectures that use special transforms, such as the Chirp Z-Transform, with logistic chaotic maps for improving statistical and differential attack resistances. **(Alaklabi et al., 2024)**. More advanced research has also proposed DNA-based image encryption and normalized exponential chaotic maps for improving security levels. **(Gill et al., 2025)** and algebraic and combinatory chaotic maps for designing nonlinear substitution modules **(Mohi et al., 2025)**. On the other hand, many research works were proposed for encrypting text and generic data using single and intertwined chaotic maps, which proved that chaotic maps can be used for encrypting data other than multimedia images. **(Gokavarapu and Kumari, 2015; Raghuvanshi et al., 2020; Mangi et al., 2023)**.

In the wider field of communication systems, chaotic systems have been studied as a method of ensuring secure transmission as opposed to protecting static data. Studies have shown the efficiency of chaotic synchronization in secure communication, such that alignment of the transmitter and receiver is possible without the need for key exchange **(Yau et al., 2012; Chang et al., 2015)**. Other studies have been directed at performance analysis in communication systems, where the dual chaotic map was combined with space-time code and embedding methods to enhance bit error rate (BER) performance in noisy channels. **(Abdulameer et al., 2022)**.

Apart from the communication models, a lot of work has been done in generalizing the application of chaotic systems in cryptography. Various tests, such as NPCR, UACI, histogram tests, and NIST randomness tests, have been done to measure the immunity to differential and statistical attacks **(Rastogi and Thakur, 2013; Alaklabi et al., 2024)**. Implementation of chaotic systems has also been done in the context of FPGA implementation for image and multimedia encryption to provide real-time solutions **(Mansor, 2016)**. This shows that the chaotic system is a very good platform for the design of a secure encryption model.

More advanced studies involved speech and audio encryption, where new issues are introduced because of the time and frequency properties of audio signals. Some initial literature reviews covered chaos-based speech encryption methods from basic one-dimensional logistic maps to more complex chaotic systems, focusing on digital accuracy and reconstruction error issues **(Mosa et al., 2011; Ambika and Radha, 2012)**. Later studies proposed hybrid models of speech encryption that incorporated chaotic maps with traditional cryptographic algorithms like Blowfish and AES to improve randomness and resistance to brute-force attacks **(Abd and Naser, 2018; Mohammed and Al-Mothafar, 2024)**. Other studies introduced chaos-based stream cipher algorithms and speech scramblers specifically for speech signals **(Ahmad et al., 2012; Hasan, 2016; Mohammed and Sadkhan, 2016)**.

To enhance security and quality of reconstruction, some research works have attempted to combine signal processing methods and chaos-based encryption. For instance, methods based on FFT and three-dimensional chaos maps have been suggested to improve spectral

properties and resistance to attacks **(Sathiyamurthi and Ramakrishnan, 2017; 2020)**. Multi-map architecture has also been used to design S-boxes and confusion layers in speech encryption systems **(Abdullah and Abduljaleel, 2021)**. Comparative analysis of scrambling and encryption of speech in terms of statistical and spectral analysis results has also been presented in some research works **(Sadkhan and Abbas, 2015)**.

However, a number of research gaps are still observable in existing literature. Most of the literature works have not focused on byte-level audio encryption while maintaining a precision of sixteen bits after several iterations of permutation and XOR. Secondly, very few works have focused on distributed encryption models where different portions of the audio signal are encrypted using different chaotic maps before combining them using a common encryption layer. Finally, very few works have focused on a holistic assessment framework that integrates the assessment of the audio signal in the frequency domain using spectral analysis, histogram analysis, reconstruction metrics such as MSE and SNR, temporal analysis using autocorrelation analysis, and security analysis using NPCR, UACI, and NIST standards in a single assessment framework **(Abdulameer et al., 2022; Alaklabi et al., 2024; Hosny et al., 2024)**.

Based on the above-identified gaps in the existing literature, the proposed research work focuses on a byte-level audio encryption technique that maintains 16-bit storage accuracy with the help of a distributed encryption approach using multiple chaotic systems. The audio signal is split into four parts, each encrypted with a different type of chaotic system (Rössler, Henon, Lorenz, and Baker-like), followed by a global layer based on the logistic map applied to the entire byte sequence. The entire approach is validated with the help of an exhaustive experimental setup based on criteria established in the previous research works.

2. CHAOTIC SYSTEMS USED

2.1 Chaotic Logistic Map

One of the well-known chaotic functions that has been researched for use in cryptography is the logistic map. The logistic function can be written as follows:

$$x_{n+1} = r * x_n(1 - x_n) \tag{1}$$

where x_n accepts values between 0 and 1, and parameter r is a positive constant that accepts values up to 4. Its value establishes and investigates the logistic map's behavior. The iterations turn chaotic at r = 3.57 **(Pareek et al., 2006; Mokhnache et al., 2022). Fig. 1** shows the behavior of the logistic map.

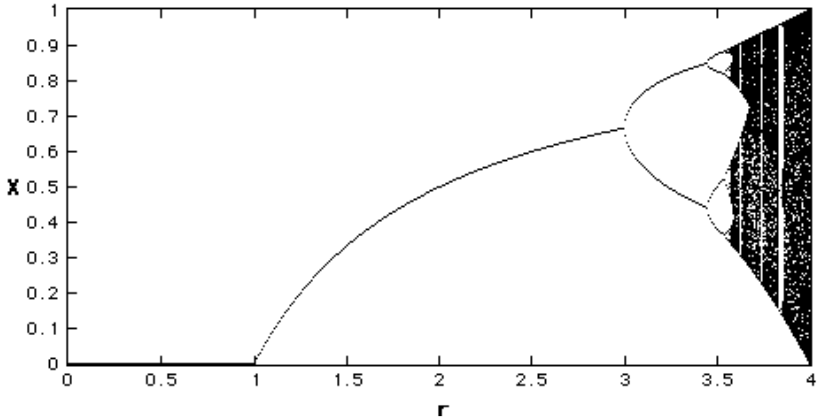

Figure 1. Logistic map bifurcation diagram **(Pareek et al., 2006)**

2.2 Lorenz System

The following three first-order differential equations govern the Lorenz system and simulate the Lorenz attractor's long-term evolution. **(Mansor, 2016):**

$$x^{\cdot} = \delta(y - n) \quad (2)$$
$$y^{\cdot} = -xz + \rho x - y \quad (3)$$
$$z^{\cdot} = xy - \beta z \quad (4)$$

where x, y, and z are the state vectors of the system, and β, ρ, and δ refer to the system parameters **(Mansor, 2016).** Because of the sensitivity to the initial conditions and to the parameters, the Lorenz system must satisfy the following conditions. **(Mansor, 2016):**
1) β, ρ, and δ are greater than zero.
2) δ must be greater than β.
3) ρ is greater than ρ_c, where ρ_c is the critical value of $\rho = \delta(\delta+\beta+3)/(\delta-\beta-1)$ **(Willsey et al., 2011). Fig. 2** shows Lorenz system trajectory.

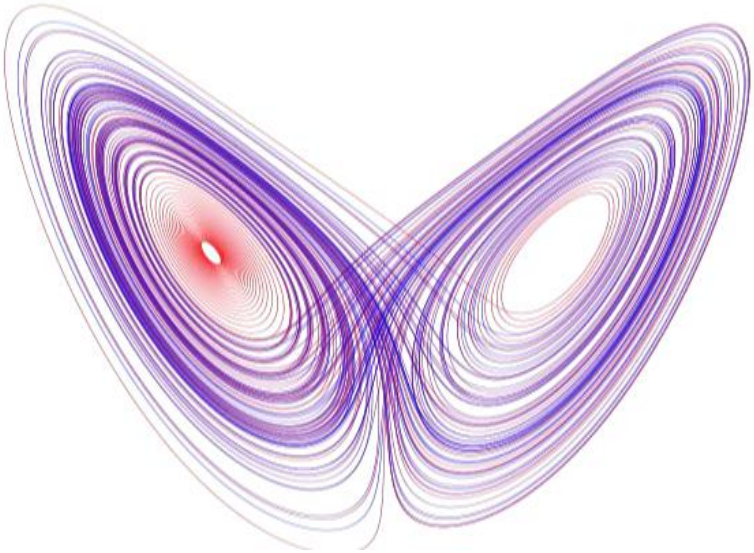

Figure 2. Lorenz system trajectory **(Willsey et al., 2011; Mansor, 2016)**

2.3 Henon Map

The two-dimensional Henon map was defined by the French physicist Michel Henon. The following is how a Henon map converts a point (x_n, y_n) into **(Hosny et al., 2024):**

$$x_{n+1} = 1 - a(x_n)^2 + y_n \quad (5)$$
$$y_{n+1} = bx_n \quad (6)$$

The map is guaranteed to be chaotic when the control parameters are a = 0.3 and b = 1.4 **(Mursi et al., 2014; Hosny et al., 2024).** The Henon chaotic map has near-optimal randomization qualities, is computationally efficient, and can produce confusion and a flat histogram. The Lyapunov exponent, random behavior, and uniform non-variation of the density variable are some of its notable features. The Henon map is strongly advised for cryptography applications due to these characteristics **(Hosny et al., 2024).**

2.4 Rosslor System

The number of second-order nonlinear terms in this system is different from that in the Lorenz system, which includes two nonlinear second-order terms, ab and ac. With a, b, and c representing the system parameters, the differential equations of the system are as follows:

$$x^{\cdot} = -(y + z) \quad (7)$$
$$y^{\cdot} = x + ay \quad (8)$$
$$z^{\cdot} = b + z(x - c) \quad (9)$$

When a=0.2, b=0.2, and c=5.7, the Rossler system attractor behaves as a chaotic attractor. Additionally, it is a bifurcation parameter, meaning that it is the parameter that causes the system to approach a fixed point, periodic system, or chaotic system. The system corresponds to b=2, c=4. As can be seen from the previous equations, xz is the only second-order nonlinear term. **(Mansor, 2016).**

2.5 Baker's Map

Baker's map is one solution to the most basic mathematical model for examining mixing and chaos in two dimensions. This map provides a mathematical description of a baker's kneading action: the dough is stretched, chopped, stacked, and squeezed to distribute the components uniformly. Baker's map is represented by the equation below. **(Kuperin and Pyatkin, 2005):**

$$f(x,y) = \begin{cases} (2x, y/2) & 0 \le x < 1/2 \\ (2x, y/2\ , y/2\ + 1/2) & 1/2 \le x \le 1 \end{cases} \quad (10)$$

In this case,

- x: stands for the horizontal coordinate at the initial location.
- y: Denotes the original point's perpendicular coordinate.
- After applying the Baker map to the point (x,y), the resulting coordinate is f(x,y).

3. METHODOLOGY

3.1 Preprocessing

i. Read the audio WAV.
ii. Convert to mono if necessary.
iii. Normalize and save the normalization scale (mx) for rescaling during recovery.

3.2 Segmentation

i. Divide the sample vector into S consecutive segments, such as S = 4.
ii. Convert samples to 16-bit signed integers (int16) using integer conversion. Use a reversible typecast to transform each int16 into two bytes (uint8). Lossless invertibility requires this.

3.3 Segment-Level Encryption

- Segment 1: The Rossler chaotic system is used for encryption in the first section. Three parameters define the Rossler system in Eqs. (7) to (9): a = 0.2, b = 0.2, and c = 5.7.

as well as initial conditions for the state variables x_0, y_0, and z_0, which are selected at random from a narrow positive range. To eliminate the initial bias, a transient discard of 200 iterations and a time step dt=0.01 are also used. To create permutation indices, the generated trajectory is first sorted using its real-valued outputs. Next, the sequence is quantized into 8-bit values to create a keystream. The segment is thus encrypted by applying an XOR operation with the quantified keystream after rearranging the audio bytes using the permutation indices. To ensure that even slight changes in the key result in entirely different permutations and keystreams, a lightweight key-scheduling mechanism further alters the initial seeds across segments. By combining positional scrambling and numerical diffusion, this dual mechanism improves security while preserving computational efficiency.

- Segment 2: The Henon map is used in the second section. The Hénon system is parameterized Eqs. (5) and (6) in this implementation by a=1.5 and b=0.3, where x_0 has random initial conditions, and y_n are eliminated from the initial state using a transient discard of 500 iterations. Permutation-only encryption is used in this stage, in contrast to Segment 1. A deterministic permutation order is derived by processing two correlated sequences produced by the iterative dynamics of the Henon map. This order reshuffles the audio signal's byte positions without changing their values. This step aims to weaken resistance to statistical analysis by upsetting the data's initial spatial arrangement and lowering local correlations. The scheme's unpredictability and cryptographic strength are greatly increased by the fact that even slight changes in the secret key parameters produce completely different permutation patterns because of the Hénon map's extreme sensitivity to initial conditions.

- Segment 3: The Lorenz system is used in the third section. The Lorenz parameters that are used in Eqs. (2) to (4) are σ = 10, β = 8/3, and ρ = 28, with initial conditions for x_0, y_0, and z_0 chosen at random. y_0 and z_0. To get rid of short-term correlations, a transient discard of 200 iterations and a numerical integration step of dt = 0.01 are used. The Rossler-based method and the Lorenz trajectory are processed similarly. After sorting the real-valued outputs, a permutation index vector is created and used to rearrange the audio bytes. To achieve diffusion, the same sequence is quantized into an 8-bit keystream and then XORed with the permuted bytes. The signal's structural and statistical characteristics are obscured by this dual operation. Because the Lorenz system is chaotic, even slight variations in parameters or seeds result in radically different keystreams and permutations. This feature greatly improves the encryption's resistance to differential analysis and brute-force attacks, and the combination of XOR and permutation keeps implementation efficiency high.

- Segment 4: At segment 4, a Baker transformation is applied, which is theoretically based on Baker's map that is used in dynamical systems. Here, the byte stream is split into fixed partitions, and each of them is processed with local permutation operations. The execution employed the following parameters: eight partitions exist. Shuffle mode is implemented by reversing the byte order of every partition. The stream of bytes is partitioned first into eight roughly equal pieces with calculated partition boundaries. In every partition, the indices are reversed to produce a local permutation. The local permutations form a global permutation of the whole sequence of bytes when they are concatenated. Apart from its computational efficacy, this partitioned shuffling process adds another layer of positional scrambling over the more intricate chaotic maps utilized

in the course of the previous sections. All these steps are crucial in further destabilizing the sequential nature of the audio data, even though it does not entail diffusion (i.e., no XOR operation). Use of multiple partitions makes the cipher more resistant to statistical analysis. Furthermore, the ability to enable and disable shuffle operations within partitions offers flexibility in balancing efficiency and complexity.

3.4 Global Stage (Logistic Map: Permutation + Diffusion)

At the end of each of the four segments, their ciphertext byte streams are concatenated into a single long stream. The logistic map provides further encryption to the global stage. In the code, the logistic map in Eq. (1) is initialized with the following parameters:
• Control parameter r=3.99,
• Initial state $x_0 \in (0.05,0.95)$, randomly selected,
• A transient discard of 1000 iterations to remove initialization bias.

The logistic sequence is applied in two complementary operations:

1. Permutation: The created chaotic sequence is ordered to obtain a permutation index, which is utilized to reorder the concatenated ciphertext bytes.
2. Diffusion (XOR): The identical sequence is quantized to 8-bit integers to obtain a keystream, and then it is XORed with the permuted byte stream.

This last step guarantees that even when an opponent has succeeded in acquiring partial knowledge about an intermediate segment, future global transformation would render direct reconstruction of plaintext impossible. Sensitivity to initial conditions of the logistic map also guarantees that variations in the secret seed or control parameter by a small amount generate entirely different permutations and keystreams, thus enlarging the effective key space. This architecture trades computational performance against cryptographic resilience through the balance between XOR operations and limited permutation with chaotic dynamical randomness.

3.5 Storage

The encrypted audio data are stored in a standalone binary file, and the corresponding key-related parameters are held separately under a matching identifier to facilitate linkage with recovery data; the key file must be protected using an appropriate key-management mechanism. **Fig. 3** demonstrates the methodology of audio coding using chaotic systems.

3.6 Decryption Process

The decryption procedure is designed as the inverse of the encryption pipeline, relying on the same keys, chaotic map parameter, iterations, and key material saved during encryption.

1. Retrieving the encrypted byte stream together with the key file, which stores the initial seeds, chaotic map parameters, the number of discarded iterations, and any auxiliary permutation tables or XOR keystreams required for deterministic recovery.
2. Global Decoding Phase, where the logistic map is reinitialized using the stored parameters. The corresponding permutation vectors and XOR keystreams are regenerated. The inverse operations are then applied in sequence, where the XOR diffusion is reversed, followed by the inverse permutation to restore the original byte order across all segments.

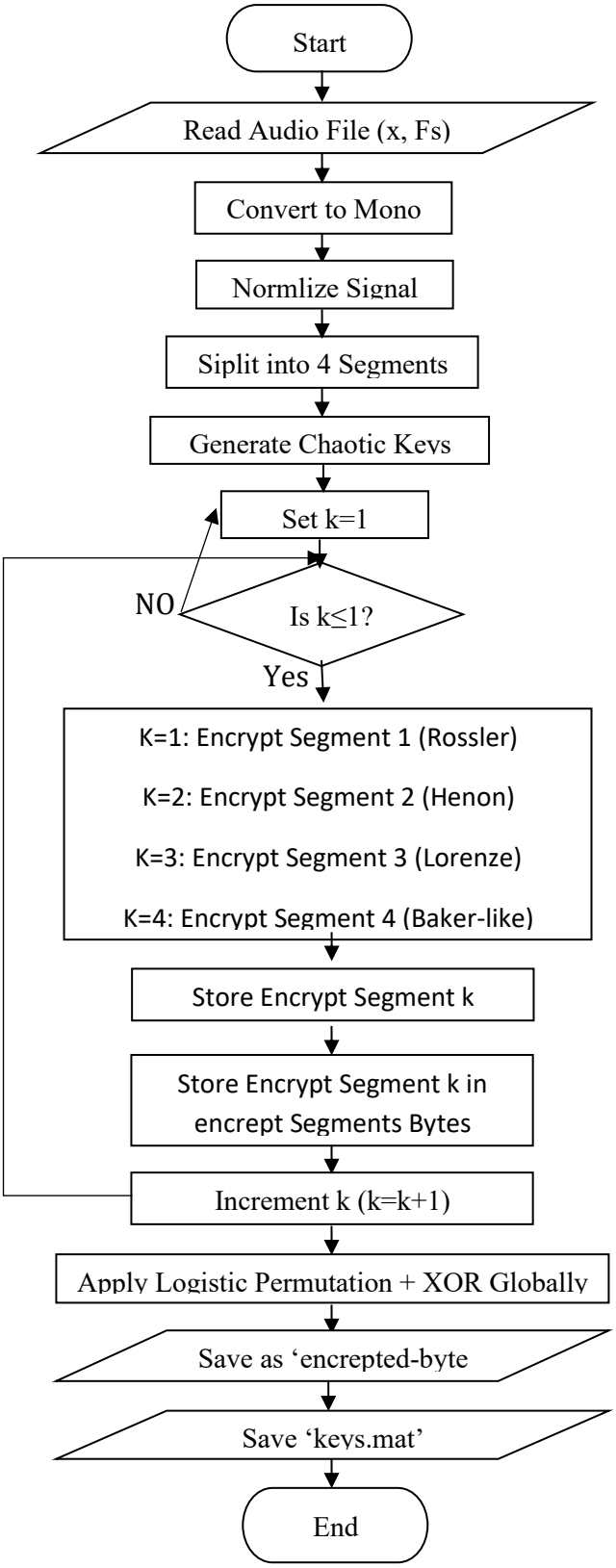

Figure 3. Flowchart of the encrypted stage

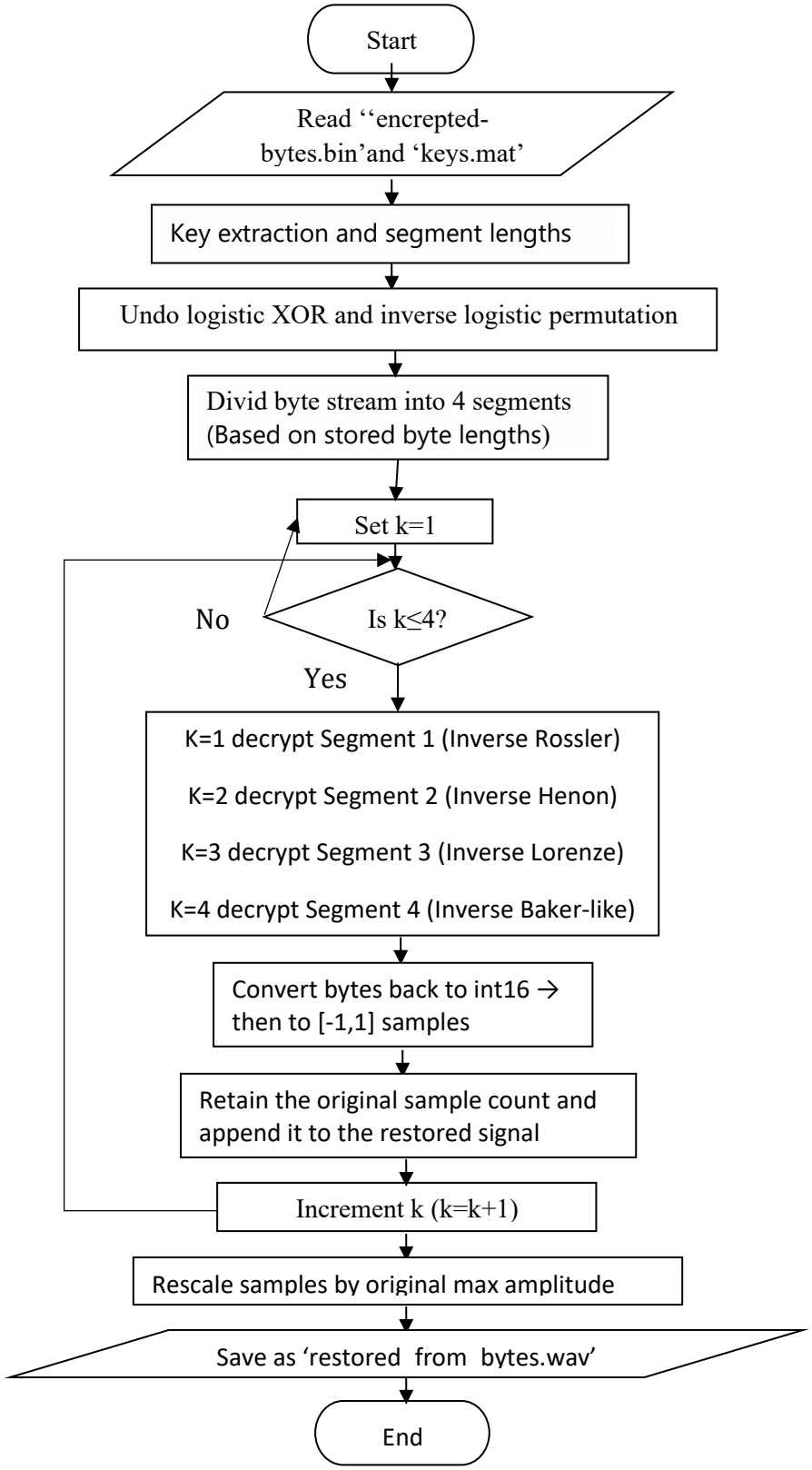

Figure 4. Flowchart of the decrypted stage

3. Segments decoding phase: Each segment is processed independently.

- Segment 1: In the reverse Rossler system, the same pseudo-random sequences are reproduced, and the inverse operations are applied by undoing the local EX-OR diffusion and then reversing the permutation of bytes.
- Segments 2: Reverse Henon map, the deterministic permutation orders are regenerated and inverted to recover the original structure of the data.
- Segment 3: Reverse Lorenz system, the Lorenz system reconstructs the chaotic sequence required for both permutation and diffusion. The inverse EX-OR and inverse permutation operations are carried out sequentially to restore the original segment data.
- Segment 4: Reverse Baker-like, the partition-based permutation order used during encryption is reconstructed and inverted to recover the correct arrangement of bytes.

Finally, the four decrypted segments are merged, converted back from byte representation to audio samples, and scaled using the original parameters. This ensures that the recovered audio waveform is an exact reconstruction of the original signal, assuming the encrypted data and key material remain preserved and secure. **Fig. 4** illustrates the methodology for decoding and audio recovery.

3.7 Pseudo-Code

Input: Audio signal S of length N
Output: Encrypted bytes file and decrypted audio S'
Step 1: Load the audio.

- Read audio signal
- Convert to mono
- Normalize samples to [-1,1]
- Split the audio signal into 4 segments

Step 2: Generate chaos keys.

- Rossler system
- Henon map
- Lorenz system
- Baker-like map
- Global logistic map (permute + XOR)

Step 3: Encryption
For each segment:

1. Convert segment samples to int16 → then to bytes (uint8)
2. Apply segment-specific chaos encryption:
    - Segment 1: Rossler system
    - Segment 2: Henon map
    - Segment 3: Lorenz system
    - Segment 4: Baker-like map
3. Merge segments and apply global encryption

- Concatenate all encrypted segment bytes
- Apply logistic map: permute + XOR

4. Save the bytes file as encrypted_bytes.bin and (keys.mat).

Step 4: Decryption

1. Load encrypted_bytes.bin and keys.mat
2. Undo global logistic encryption: XOR + inverse permutation

3. Divide bytes back into original segments
4. For each segment, reverse segment-specific encryption:
   - Segment 1: Inverse Rossler system (inverse XOR + inverse permutation)
   - Segment 2: Inverse Henon map (inverse permutation)
   - Segment 3: Inverse Lorenz system (inverse XOR + inverse permutation)
   - Segment 4: Inverse Baker-like (inverse partition permutation)
5. Convert bytes back to int16 → then to [-1,1] samples
6. Save the original number of samples

Step 6: Recover audio

1. Rescale samples by original max amplitude
2. Save as restored_from_bytes.wav

4. RESULTS AND DISCUSSION

All the experiments performed using the suggested encryption algorithm were executed on a home machine with the following specifications: Processor (Intel Xeon CPU E3-1505M v5 at a base clock speed of 2.81 GHz), and RAM (16 GB). The process, encryption and decryption functions, and time and statistical testing were performed for the software module on Windows 10 using MATLAB R2024a. **Tables 1 to 4**, **Figs. 3 and 4** below show the results of the tests performed:

4.1 SNR Test

The value of SNR test results for four samples of speech is shown in **Table 1 (AlSaad and Hato, 2014; Bushra et al., 2025).**

Table 1. SNR Test

No.	Speech sample in wav	Duration in second	SNR in dB	
			Encryption	Decryption
1	Audio1	5	-12.87	66.37
2	Audio2	4	-13.32	72.32
3	Audio3	3	-14.06	66.82
4	Audio4	1	-13.31	70.73
5	Audio5	23	-10.65	74.82
6	Audio6	60	-14.05	75.00

4.2 MSE Test

The value of the MSE test results for four samples of speech is shown in **Table 2 (Chicco et al., 2021; Alrifaee and Ismaeel, 2022).**

Table 2. MSE Test

No.	Speech sample in wav	Duration in second	MSE	
			encryption	Decryption
1	Audio1	5	0.028801	0.000000
2	Audio2	4	0.127266	0.000000
3	Audio3	3	0.042572	0.000000
4	Audio4	1	0.089751	0.000000
5	Audio5	23	0.083200	0.000000
6	Audio6	60	0.346755	0.000000

4.3 Entropy

The value of entropy test results for four samples of speech is shown in **Table 3 (Anjana *et al.*, 2022; Mohi *et al.*, 2025)**.

Table 3. Entropy Test

No.	Speech sample in wav	Duration in second	Entropy	
			encryption	Decryption
1	Audio1	5	7.9972	4.6743
2	Audio2	4	7.9989	5.3939
3	Audio3	3	7.9977	5.1173
4	Audio4	1	7.9965	5.4172
5	Audio5	23	7.9981	6.1584
6	Audio6	60	7.9997	4.9028

4.4 Correlation Test

The value of correlation test results for four samples of speech is shown in **Table 4 (Mokhnache et al., 2022; Haseeb et al., 2023)**.

Table 4. Correlation Test

No.	Speech sample in wav	Duration in second	Correlation	
			Original vs encrypted	Original vs decrypted
1	Audio1	5	0.002390	1.000000
2	Audio2	4	0.003717	1.000000
3	Audio3	3	-0.002049	1.000000
4	Audio4	1	-0.003114	1.000000
5	Audio5	23	0.000913	1.000000
6	Audio6	60	-0.000470	1.000000

4.5 Spectrogram

The spectrogram for the speech sample in the three cases (original, encryption, and decryption) is demonstrated in **Fig. 5 (Mosa et al., 2011; Sathiyamurthi and Ramakrishnan, 2020).**

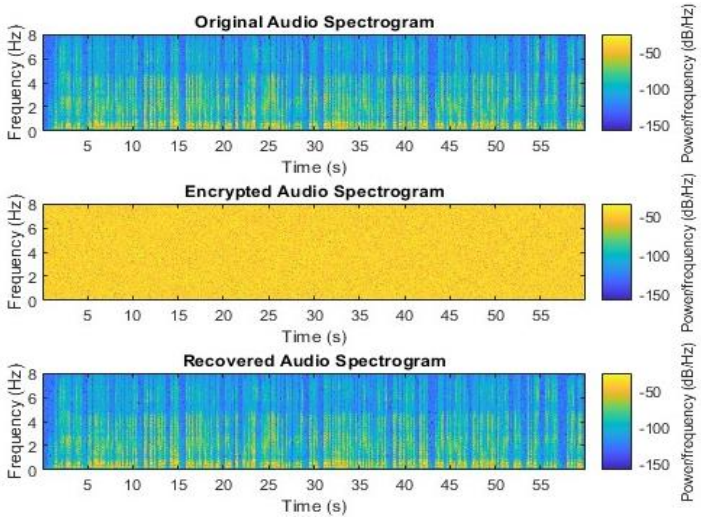

Figure 5. Spectrogram speech signal

4.6 Histogram

The histograms for the speech sample in the three cases (original, encryption, and decryption) are demonstrated in **Fig. 6 (Mosa et al., 2011; Sathiyamurthi and Ramakrishnan, 2020).**

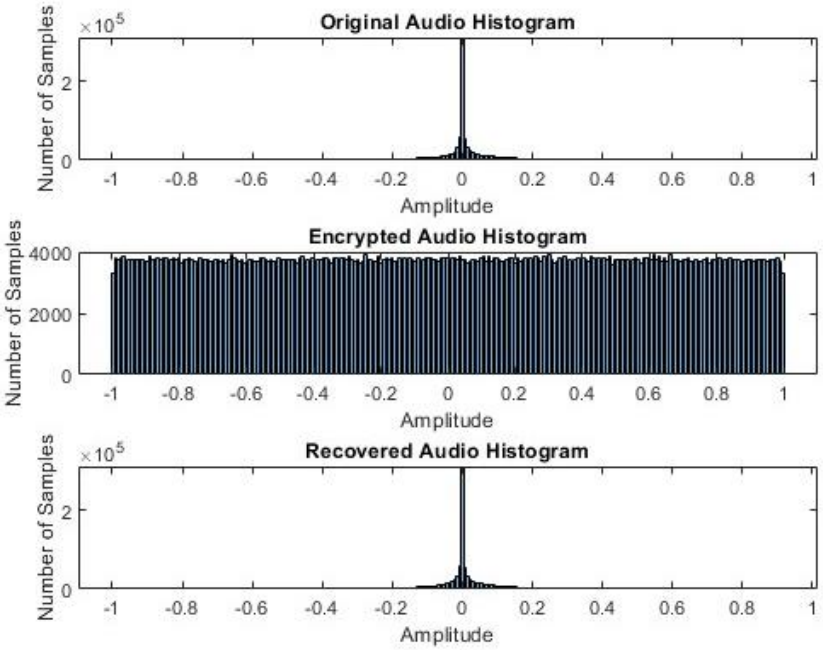

Figure 6. Histogram speech signal

The results showed that the system has a great ability to hide the statistical characteristics of the original signal, as the correlation coefficients between the original and encrypted signals reduced to values near zero, and the entropy value approached ideal randomness. The measurements also showed that the mean squared error (MSE) remained low ≈ 0.0000 (zero MSE indicates an exact sample-wise match (bit-exact)) while maintaining a high signal-to-noise ratio (SNR) after decryption, ranging between 66.37 and 70.73 dB, reflecting the audio quality after the encryption and decryption process.

5. CONCLUSIONS

This research presented a system for the encryption of audio signals based on a set of chaotic maps (Rossler, Henon, Lorenz, and Baker) as well as a logistic map to achieve a high level of randomness and complexity. The system showed better performance in terms of encryption strength and key sensitivity, despite increased computational complexity and execution time. Accordingly, the proposed approach constituted an effective step towards designing more secure systems to protect voice communications. In the future, it is possible to improve implementation efficiency to reduce the processing time and to study the possibility of integrating the system with real-time applications or embedded platforms with limited computing power.

NOMENCLATURE

Symbol	Description	Symbol	Description
a,b, c	Rossler system parameters	*x, y, z*	state vectors
a, b	Henon system parameters	*x`, y`, z `*	Differential state variable of a chaotic system
R	Bifurcation parameter of the chaotic map	*β, ρ, δ*	Lorenze system parameters
x_n, y_n, x_{n+1} , y_{n+1}	Current and next value of the chaotic map state variable	ρ_c	Critical value of ρ

Acknowledgements

This work was supported by the Department of Electrical Engineering, College of Engineering, University of Baghdad.

Credit Authorship Contribution Statement

Nagham Malik Abd Ali: Writing (original draft), Software, Methodology, Validation, Investigation. Tariq Zeyad Ismaeel: Supervision, Conceptualization, Writing (review & editing), Validation.

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.

REFERENCES

Abd, M. and Naser, U., 2018. Speech encryption using chaotic map and Blowfish algorithms. *Journal of Basrah Researches (Science)*, 39(2A), pp. 68–76. https://doi.org/10.13140/RG.2.2.28316.13444.

Abdulameer, L.F., Sripati, U., and Kulkarni, M., 2022. BER performance improvement of dual chaotic maps based on STBC communication system. *Al-Khwarizmi Engineering Journal*, 18(4), pp. 32–44. https://doi.org/10.22153/kej.2022.10.001.

Abdullah, S.M. and Abduljaleel, I.Q., 2021. Speech encryption technique using S-box based on multi chaotic maps. *TEM Journal*, 10(3), pp. 1429–1434. https://doi.org/10.18421/TEM103-54.

Ahmad, M., Alam, B. and Farooq, O., 2012. Chaos-based mixed keystream generation for voice data encryption. International Journal on Cryptography and Information Security (IJCIS), 2(1), pp. 39–48.

Alaklabi, A., Munir, A., Hafeez, M.A., and Khattak, M.A.K., 2024. Z-crypt: Chirp z-transform-based image encryption leveraging chaotic logistic maps and substitution permutation network. *IEEE Access*, *12*, pp. 123401-123422. https://doi.org/10.1109/ACCESS.2024.3453171.

Alrifaee, Z.I.A. and Ismaeel, T.Z., 2022. Cryptography based on retina information. *Indonesian Journal of Electrical Engineering and Computer Science*, 28(3), pp. 1697–1708. https://doi.org/10.11591/ijeecs.v28.i3.pp1697-1708.

AlSaad, S.N. and Hato, E., 2014. A speech encryption based on chaotic maps. *International Journal of Computer Applications*, 93(4), pp. 19–28. https://doi.org/10.5120/16203-5488.

Ambika, D. and Radha, V., 2012. Secure speech communication: A review. *International Journal of Engineering Research of Application (IJERA)*, 2(5), pp. 1044–1049. https://www.ijera.com/papers/Vol2_issue5/FR2510441049.pdf.

Anjana, S., Yadav, A.K., Singh, P. and Singh, H., 2022. Audio and image encryption scheme based on QR decomposition and random modulus decomposition in Fresnel domain. *Optica Applicata*, 52(3), pp. 359-374. https://doi.org/10.37190/oa220303.

Bushra W., Hussein AL Zahawy, and Saad S. Hreshee, 2025. Two layers of audio security utilizing the international data encryption algorithm (IDEA) and Lorenz chaotic scrambler. *International Journal of Computational and Experimental Science and Engineering*, 11(3). https://doi.org/10.22399/ijcesen.2183.

Chang, W.D., Shih, S.P., and Chen, C.Y., 2015. Chaotic secure communication systems with an adaptive state observer. *Journal of Control Science and Engineering*, 2015, Article ID 471913. https://doi.org/10.1155/2015/471913.

Chicco, D., Warrens, M.J., and Jurman, G., 2021. The coefficient of determination, R-squared, is more informative than SMAPE, MAE, MAPE, MSE, and RMSE in regression analysis evaluation. *PeerJ Computer Science*, 7, pp. 1–24. https://doi.org/10.7717/PEERJ-CS.623.

Gill, H.S., Amjad, M., Faheem, M., Ur Rehman, A., Rana, U., Khan, A.R. and Bashir, R., 2025. A normalized exponential piecewise chaotic system (NEPCS) and DNA image cryptography using SHA-256. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3582318.

Gokavarapu, S., and Vani Kumari, S., 2015. A novel encryption using one-dimensional chaotic maps. *In Advances in Intelligent Systems and Computing*, *Springer Verlag*, pp. 193–203. https://doi.org/10.1007/978-3-319-13728-5_22.

Hasan, F.S., 2016. Speech encryption using fixed point chaos-based stream cipher (FPC-SC). *Eng. & Tech. Journal*, 34(11), pp. 2152–2166. https://doi.org/10.30684/etj.34.11A.19.

Haseeb, E.H., Kadhim, S.A., and Mahmood, A.S., 2023. A six-dimensional hyperchaotic pseudorandom sequence for enhanced voice encryption. *Ingénierie des Systèmes d'Information*, 28(4), pp. 1055–1062. https://doi.org/10.18280/isi.280425.

Hosny, K.M., Elnabawy, Y.M., Elshewey, A.M., Alhammad, S.M., Khafaga, D.S., and Salama, R., 2024. New method of colour image encryption using triple chaotic maps. *IET Image Processing*, *18*(12), pp. 3262-3276. https://doi.org/10.1049/ipr2.13171.

Kocarev, L., 2011. *Chaos-based cryptography: a brief overview. 1st ed*. Berlin: Springer-Verlag. https://doi.org/10.1007/978-3-642-20544-6.

Kuperin, Y.A. and Pyatkin, D.A., 2005. Two-dimensional chaos: The baker map under control. *Journal of Mathematical Sciences*. Kluwer Academic/Plenum, pp. 2798–2802. https://doi.org/10.1007/s10958-005-0234-8.

Mansor, A.J., 2016. *FPGA-Based Image Encryption Using Chaotic Systems*. PhD thesis, University of Technology, Iraq.

Mohammed, R.S., and Sadkhan, S.B., 2016. Speech scrambler based on proposed random chaotic maps. *In Proceedings of the Al-Sadiq International Conference on Multidisciplinary in IT and Communication Techniques Science and Applications (AIC-MITCSA 2016). IEEE*, pp. 154–159. https://doi.org/10.1109/AIC-MITCSA.2016.7759928.

Mohammed, S.G. and Al-Mothafar, N.S., 2024. Evaluation of Rijndael algorithm for audio encryption by brute force attack. *Journal of Engineering*, 30(11), pp. 128–141. https://doi.org/10.31026/j.eng.2024.11.08.

Mohi Ud Din, S., Shah, T., Alblehai, F., Nooh, S., and Jamal, S.S., 2025. A combinatory approach of non-chain ring and Henon map for image encryption application. *Scientific Reports*, *15*(1), p.1781. https://doi.org/10.1038/s41598-025-85814-5.

Mokhnache, S., Daachi, M.E.H., Bekkouche, T. and Diffellah, N., 2022. A combined chaotic system for speech encryption. *Engineering, Technology & Applied Science Research*, *12*(3), pp. 8578-8583. https://doi.org/10.48084/etasr.5157.

Mosa, E., Messiha, N.W., Zahran, O. and Abd El-Samie, F.E., 2011. Chaotic encryption of speech signals. *International Journal of Speech Technology*, *14*(4), pp. 285-296. https://doi.org/10.1007/s10772-011-9103-7.

Mursi, M.F., Ahmed, H.E.H., Abd El-samie, F.E., and Abd El-aziem, A.H., 2014. Image encryption based on development of Hénon chaotic maps using fractional Fourier transform. *International Journal of Strategic Information Technology and Applications (IJSITA)*, *5*(3), pp. 62-77. https://doi.org/10.4018/ijsita.2014070105.

Pareek, N.K., Patidar, V., and Sud, K.K., 2006. Image encryption using chaotic logistic map. *Image and Vision Computing*, 24(9), pp. 926–934. https://doi.org/10.1016/j.imavis.2006.02.021.

Raghuvanshi, K.K., Kumar, Subodh, and Kumar, Sunil, 2020. A data encryption model based on intertwining logistic map. *Journal of Information Security and Applications*, 55, Article 102622. https://doi.org/10.1016/j.jisa.2020.102622.

Rastogi, S. and Thakur, S., 2013. Security analysis of multimedia data encryption technique using piecewise linear chaotic maps. *International Journal on Recent and Innovation Trends in Computing and Communication*, 1(5), pp. 458–461.

Sadkhan, S.B. and Abbas, N.A., 2015. Performance evaluation of speech scrambling methods based on statistical approach. *Atti della Fondazione Giorgio Ronchi*, 66(5), pp. 601–614.

Sathiyamurthi, P. and Ramakrishnan, S., 2017. Speech encryption using chaotic shift keying for secured speech communication. *Eurasip Journal on Audio, Speech, and Music Processing*, 2017(1), pp. 1–11. https://doi.org/10.1186/s13636-017-0118-0.

Sathiyamurthi, P. and Ramakrishnan, S., 2020. Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map. *Multimedia Tools and Applications*, 79(25–26), pp. 17817–17835. https://doi.org/10.1007/s11042-020-08729-5.

Sowthily, C. and Brindha, M., 2019. Image encryption using chaotic Baker's map and LSB steganography. *International Journal of Computational Intelligence and IoT*, pp. 1–6. https://ssrn.com/abstract=3355504.

Talib Mangi, H., Ali, S.A., and Jawad, M.J., 2023. Encrypting of text based on chaotic map. *Journal of University of Babylon for Pure and Applied Sciences (JUBPAS)*, 31(1). https://doi.org/10.19196/jubpas.v31i1.4526.

Willsey, M.S., Cuomo, K.M., and Oppenheim, A.V., 2011. Selecting the Lorenz parameters for wideband radar waveform generation. *International Journal of Bifurcation and Chaos*, 21(9), pp. 2539–2545. https://doi.org/10.1142/S0218127411029914.

Yau, H.T., Pu, Y.C. and Li, S.C., 2012. Application of a chaotic synchronization system to secure communication. *Information Technology and Control*, 41(3), pp. 274–282. https://doi.org/10.5755/j01.itc.41.3.1137.

تشفير الصوت باستخدام أنظمة فوضوية مع معالجة مباشرة على مستوى البايت

نغم مالك عبدعلي*، طارق زياد اسماعيل

قسم الهندسة الكهربائية، كلية الهندسة، جامعة بغداد، بغداد، العراق

الخلاصة

لحماية الإرسال السمعي الرقمي من النفاذ والتعديل غير المصرح به، تقترح هذه الورقة مخطط تشفير صوتي يعتمد على الأنظمة الفوضوية. يجمع النهج المقترح بين خرائط فوضوية متعددة في مخطط تشفير يتم تطبيقه على مستوى البايت. ينقسم صوت الإدخال أولا إلى أربعة أجزاء متساوية الطول. نظام روسلر ونظام لورينز وخريطة هينون وخريطة بيكر هي أنظمة فوضوية تستخدم لتشفير كل جزء. يتم الجمع بين أربعة أجزاء، وبالتالي، يتم استخدام خريطة لوجستية على الصوت المشفر لإضافة خطوة تقليب إضافية، مما يضمن انتشارا قويا وارتباكا على طول الإشارة بأكملها. أثناء مرحلة فك التشفير، يتم عكس عمليات XOR والتبديل بشكل منهجي باستخدام المفاتيح المحفوظة، مما يؤدي إلى استعادة الصوت الأصلي. يتم تقييم الصوت المشفر والاسترجاع باستخدام عدة اختبارات لضمان نجاح عملية التشفير والاسترجاع، مثل اختبار نسبة الإشارة إلى الضوضاء (SNR)، والارتباط التلقائي، ومتوسط الخطأ التربيعي (MSE))، وتحليل الرسم البياني، ومقارنة الطيف. أظهرت النتائج أن النظام المقترح آمن للغاية ضد المهاجمين ويمتلك آلية نشر وارتباك قوية لتحسين الاتصال الكلامي في مجال الاتصالات. ومن ثم، فإن النظام مناسب لتطبيقات الوسائط المتعددة التي تتطلب مستوى عال من السرية، بما في ذلك نقل البيانات الحساسة وحماية الحقوق الرقمية والاتصالات العسكرية.

الكلمات المفتاحية: التشفير، فك التشفير، الصوت، النظام الفوضوي.