A Hybrid Chaotic Map and DNA Coding Approach for Secure Audio Encryption

Salah Taha Allawi[1] and May Mowaffaq AL-Taee[2]
[1]Department of Computer Science, College of Science, Mustansiriyah University, 10052 Baghdad, Iraq
[2]Legal Department, Ministry of Higher Education and Scientific Research, 10011 Baghdad, Iraq
Salah.taha@uomustansiriyah.edu.iq, may.m.altaie@gmail.com

Keywords: Speech Encryption, Chaotic Maps, Hybrid Chaotic Key, DNA Coding, Statistical Attacks.

Abstract: Speech signal security has become a critical requirement in modern communication systems because of the rapid growth of multimedia transmission over open networks. This study proposes a new speech encryption technique that combines DNA encoding and chaotic maps, divided into two phases. In the first phase, 3 chaotic maps (Tent, Logistic, and Sine) are used to generate 3 keys, and then these keys are combined to generate a hybrid key resistant to statistical attacks. In the second phase, the audio file is prepared by applying normalization and quantization operations. To enhance the encryption strength, DNA coding techniques are used to change speech samples and a hybrid key into DNA sequences before applying the encryption process. To evaluate the proposed method, two widely used speech databases, namely RAVDESS and TIMIT, were used. The results show excellent security performance, achieving NPCR values of 100% for both datasets. The results show UACI values of 33.27% for RAVDESS and 31.57% for TIMITDIC. These results confirm that the proposed hybrid chaos-and-DNA approach provides a high level of security and robustness.

1 INTRODUCTION

Because of the faster growth of the internet, sharing and transferring various types of multimedia have become easier. However, this sharing has raised various information security concerns. To protect multimedia information, several methods have been introduced, including watermarking, steganography, and encryption [1]-[3]. Encryption is an important method because it ensures the security of both professional and personal contacts and prevents unauthorized access to private recordings or chats transmitted through social media platforms [4].

Traditional encryption techniques, which are used to encrypt text or images, may not be the best choice for protecting voice data because they have strict time requirements and limits on the quality and latency. These requirements have led many researchers to suggest new encryption techniques that use mathematical complexity to achieve high levels of security while protecting signal integrity [5], [6]. Chaotic encryption algorithms have attracted a lot of attention in different areas because they offer several benefits, such as being very sensitive to initial points and settings, not repeating patterns, randomness, and providing speed, security, and complexity [7], [8]. However, relying solely on chaotic systems for speech encryption is insufficient; therefore, advanced technologies are needed to enhance speech security. DNA technology is one such method used to improve the security of chaotic speech [9]. In recent research, the use of DNA coding in encryption methods has opened up a new field in secure signal processing. DNA-based coding converts digital data into sequences that look like biological nucleotides. This method makes it difficult to decrypt the encrypted message. DNA coding has been commonly used in data and image encryption; its application with audio and speech signals has also achieved excellent results, especially when combined with chaotic maps to create encryption methods [6]. The major contributions from this research paper:

1) Introduce a hybrid speech encryption system combining chaotic maps (Logistic, Tent, and Sine) to generate a secure hybrid key.
2) The system integrates chaotic mapping with DNA-based encryption to improve scrambling and propagatio.
3) The system is resistant to various statistical attacks.

The remainder of this paper includes Section 2, which displays many related works. Meanwhile,

Section 3 explains chaotic maps and DNA encoding. The proposed method is presented in Section 4. Section 5 displays the results of the conducted experiments. Section 6 presents a summary of the judgments and several recommendations for future work.

2 RELATED WORK

This part reviews a selection of previous work that has been presented in the field of audio file encryption.

In 2023, the authors in [2] proposed a novel approach to encrypt audio using the chaotic logistic map. Initially, to break the correlation between the audio samples, a permutation mechanism is applied to rearrange the positions of these samples. Secondly, a complicated hyper-chaotic system creates a key that is used to mix up the audio, which helps cover the quiet parts of speech, protecting important information and ensuring the encryption works well. To confirm the security and effectiveness of this method, various quality checks were performed, such as entropy, key space, and correlation coefficient. The results show that the system works well, with an NSCR of 99.63 and a large key space of 2^{420}.

In the same year, the authors in [10] proposed a new method to encrypt audio files. These methods are dependent on generating new chaotic maps. Firstly, the Sine and Logistic maps are used to create a Sine-logistic map (SLIM). Secondly, using the Sine and Cubic maps to create a Sine-cubic integrated map (SCIM). To generate (Key A) and (Key B), SLIM and SCIM are used, respectively. The speech signal is compressed, and then, using Key A, the shifting operation is run on it. Finally, the XOR operation was applied between Key B and the compressed-shifted speech signal, and then the audio file was sent over a common channel. Three audio files were used to test the system, yielding an average NSCR of 99.58 and a UACI sampling rate of 33.65.

In addition, the authors in [11] introduced a novel approach for encrypting audio using a Chaotic Chebyshev map. To extract the integer and fractional components, the entered audio files are first preprocessed. The integer components are normalized to the range [0, 255]. Secondly, the integer parts of the entered audio files are mixed and spread out by repeatedly chaotically applying the Chebyshev map using values derived from the original data. A post-processing step is ultimately conducted on the dispersed audio samples. Three audio files were used to evaluate the system, yielding an average NSCR of 99.74 and a large key space of 2^{159} across the samples.

In 2025, the authors in [4] proposed a method based on the Tent and Logistic maps for secure audio encryption. Random permutation of the audio data using the Tent, and then a random key equivalent to the length of the audio file is created using a 1D Logistic. To create the encrypted audio, the XOR operation is performed on the audio file and the random key. Two classes of audio files are used to test the proposed system, which achieves an NSCR of 100 and a key space of 2^{616}.

In addition, the authors in [9] suggested novel encryption approach based on DNA encoding and a chaotic map, comprising a data preparation and a data encryption stage. The speech signal is divided into four equal parts at the beginning. Then, confusion and diffusion are used, followed by DNA encoding. The components are then combined to create the encrypted signal. After that, a random key is first created using a Sine map and then is encoded using DNA codes. Finally, encryption is applied using a (DNA XOR) operation between the file data and the random key to produce the encrypted file. Four audio files were selected randomly from the TIMIT dataset as test samples. The results show that the system works well, with an NSCR of 100 and a UACI of 33.12.

Table 1 presents several previous methods, briefly detailing the methodologies used and the results of each study.

By examining Table 1, it is clear that the proposed methods are simple, and the design is clear, but they suffer from using a limited set of evaluation criteria and failing to employ fundamental criteria for testing method quality. In addition, they rely on a few test samples.

The proposed method fixes the problems of earlier techniques by using three random chaotic keys, adding DNA coding to the data encoding process, and following accepted testing standards. Diverse datasets were employed to show the robustness and efficacy of this strategy.

Table 1: Explain the previous work and the results achieved in each study.

Ref.	Method	Number of samples	Result
Ref. [2]	chaotic logistic map	8 audio files	NSCR = 99.63 key space 2^{420}
Ref. [10]	3 chaotic map (Logistic, Sine, Cubic)	3 audio files	NSCR = 99.58
Ref. [11]	chaotic Chebyshev map	3 audio files	NSCR = 99.74 key space 2^{159}
Ref. [4]	Tent, 1D logistic maps	2 groups of audio files	NSCR = 100 key space 2^{616}
Ref. [9]	DNA coding, chaotic map	4 audio files	NSCR = 100 key space 2^{698}

3 METHODOLOGY

Using multiple chaotic maps makes the data harder to understand and spread out, increases the number of keys, and strengthens the encryption system. The proposed method uses three chaotic maps (logistic, Tent, and Sine) because of their sensitivity to slight variations in initial values and ability to generate high-quality pseudo-random sequences.

3.1 Chaotic Systems

Chaos theory is characterized by its high sensitivity to control parameters and initial conditions. Cryptographic features such as diffusion and confusion link its unpredictable, random results [12].

3.1.1 D Logistic Map

It is one of the most widely used chaotic systems because of its relatively simple mathematical structure. [13]. Equation (1) shows the mathematical form.

$$P_{i+1} = \mu_1 P_i (1 - P_i). \quad (1)$$

here (μ_1) is the control parameter in the scope 0-4, (P_0) is the seed value 0-1, (i) is the count of loops, and (P_{i+1}) is the next value.

3.1.2 Tent Map

At certain values of its control parameter, this fundamental dynamical system exhibits chaotic behavior [14]. Equation (2) shows the mathematical form.

$$N_{r+1} = \begin{cases} \mu_2 N_r & if\ N_r < 0.5 \\ \mu_2 (1 - N_r) & if\ N_r \geq 0.5 \end{cases}. \quad (2)$$

Where μ_2 is a parameter in the scope 0-2, (N_0) is the seed in scope 0-1, (N_{r+1}) is the next value, and (r) the number of loops.

3.1.3 Sine Map

It is a continuation map with a 1D structure that creates serial numbers exhibiting chaotic behavior [15]. Equation (3) shows the mathematical form.

$$K_{j+1} = \mu_3 . sin(\pi K_j). \quad (3)$$

Where:

- (μ_3) is a control parameter 0-1;
- (K_0) is the seed value 0-1;
- (K_{j+1}) is the next value;
- (j) is the number of loops.

3.2 DNA Sequences

DNA includes four bases: guanine (G.), thymine (T.), cytosine (C.), and adenine (A.), where (A.) pairs with (T.) and (G.) pairs with (C.). Likewise, in a binary system, 0 and 1 are complementary, with 00 relating to 11 and 10 relating to 01. There are 24 encoding groups; we used only 8 of them, as shown in Table 2 [16], [17].

Table 2: DNA encoding rules (8 rules).

Rul. No.	00	10	01	11
R.1	A.	C.	G.	T.
R.2	A.	G.	C.	T.
R.3	T.	C.	G.	A.
R.4	T.	G.	C.	A.
R.5	C.	A.	T.	G.
R.6	G.	A.	T.	C.
R.7	C.	T.	A.	G.
R.8	G.	T.	A.	C.

3.3 Audio Datasets

This work uses two well-known dataset used in audio research (TIMIT, RAVDESS).

3.3.1 TIMIT Dataset

It is one of the most popular datasets designed for phonological and speech recognition research. It was compiled from 630 speakers from 8 different regions of the United States, with each speaker contributing 10 sentences, for 6300 sentences [18].

3.3.2 RAVDESS Dataset

It is one of the most popular datasets designed for speech emotion recognition research and human-computer interaction. This dataset was compiled based on the participation of 12 men and 12 women in eight emotional states. Each participant performed two sentences, resulting in 1,440 audio recordings [19].

4 PROPOSED METHOD

The proposed method comprises two phases: encryption and decryption, as illustrated below.

4.1 Encryption Phase

This stage includes audio preparation, hybrid key generation, and the encryption process. Figure 1 shows the general diagram of the proposed method (encryption phase). Algorithm 1 explains the major steps of the proposed method (encryption phase).

Data preparation begins with data input (an audio file), followed by standardization and normalization of the audio file data. Next, the data is encoded using DNA coding rules. Hybrid chaotic key (HCK) generation begins by generating three random keys using (Logistic, Tent, and Sine). The seed values and control parameters used to generate the keys are $P_0 = 0.5$, $\mu 1 = 3.99$, $N_0 = 0.4$, $\mu 2 = 1.99$, $K_0 = 0.6$, $\mu 3 = 0.99$. These three keys are then combined to create the hybrid encryption key. The hybrid key is then encoded using DNA coding rules. Equation 4 is used to generate the hybrid chaotic key.

$$HCk = (x + y + z)\ mod\ 1. \quad (4)$$

Where:

- (x) represents the key generated by the Logistic map,
- (y) represents the key generated by the Tent map,
- (z) represents the key generated by the Sine map.

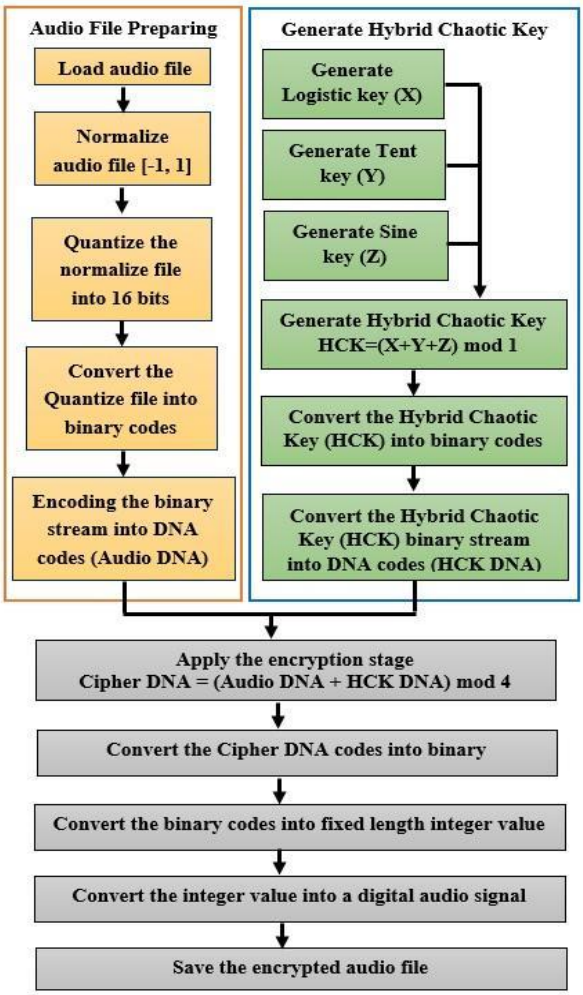

Figure 1: General diagram of the proposed method.

The encryption process involves combining the hybrid encryption key with the encrypted data. Finally, the encrypted data is converted from DNA codes to binary codes, then to healthy values, and finally to an audio signal, which is stored as an encrypted audio file and transmitted to the recipient. Equation (5) is used to create the encrypted audio file (CA).

$$CA = (Audio\ DNA + Key\ DNA)\ mod\ 4 \quad (5)$$

Where (Audio DNA) represents the audio file data encoded using DNA codes, and (Key DNA) represents the hybrid key data after it has been encoded using DNA codes.

```
1)      Input: Original audio file
2)      Output: Cipher audio file
3)      Input the original audio file.
4)      Normalize the audio signal range
[-1, 1].
5)      Converting the normalized audio
signal to binary code and then changing
it to DNA codes (Audio DNA).
6)      To produce a key (x), use a
Logistic map.
7)      To produce a key (y), use a Tent
map
8)      To produce a key of (z), use a
Sine map.
9)      Generate hybrid chaotic key (HCK =
(x + y + z) mod 1)
10)     Converting the hybrid chaotic key
to binary code and then changing it to
DNA codes (HCK DNA).
11)     Apply encryption stage to generate
the Cipher DNA sequence (Cipher DNA =
(Audio DNA + HCK DNA) mod 4).
12)     Convert the Cipher DNA codes to
binary.
13)     Convert the binary codes into
fixed-length integer values.
14)     Convert the integer values into a
digital audio signal (PCM format).
15)     Save the encrypted audio file.
```

Algorithm 1: The general steps of the suggested method.

4.2 Decryption Phase

This stage includes three steps: data preparation, generating a hybrid key, and decryption. Data preparation begins by inputting the encrypted audio file; the data is changed to binary and then encoded using DNA coding (Audio DNA). Generate the hybrid chaotic key: three 1D chaotic maps (Tent, Logistic, and Sine) were used to generate three chaotic keys. These keys are combined to create the hybrid key and then encrypted using DNA coding (key DNA). Decryption processing is performed by subtracting the hybrid chaotic key from the audio data. The plain audio (*PA*) file was converted into binary form. Finally, the binary data is converted to integer values and then converted back into an audio file. Equation (6) is used to decrypt the audio file.

$$PA = (Audio\ DNA - Key\ DNA)\ mod\ 4. \quad (6)$$

Where (*PA*) is the decrypted audio file data, (*Audio DNA*) is the audio file data that was encoded with DNA codes, and (*Key DNA*) is the hybrid chaotic key data that was encoded with DNA codes.

5 RESULT AND DISUSSION

To evaluate the proposed method, two datasets (TIMIT and RAVDESS) were chosen. A selection of 40 audio files was chosen from the RAVDESS dataset; these groups comprise 6 speech emotions (angry, disgust, fear, happy, sad, and surprised), representing audio files for men and women. Each file is 3 seconds long; the audio is in PCM WAV format, 16-bit, single-channel, and 48000 Hz. A selection of 25 audio files representing different speech emotion was chosen from the TIMIT dataset for men and women. Each file is a few seconds long; the audio is in PCM WAV format, 16-bit, single-channel, and 16000 Hz. Figure 2 displays the sound wave and visual representation of an audio file from the RAVDESS dataset (Happy sample audio) before and after it has been encrypted using the suggested method.

To determine the efficiency of the proposed method, a series of tests was conducted.

5.1 Number of Sample Change Rate (NSCR)

It is used to measure an encryption system's resistance to differential attacks. The closer the NSCR values are to 100%, the more it shows that the proposed encryption system produces an encrypted audio file resistant to differential attacks [11]. Equation 7 is used to compute the correlation coefficient.

5.2 Unified Average Changing Intensity (UACI)

It is used to calculate the mean intensity of changes between the encrypted and original speech. The value 33.3% is considered the theoretical ideal value for the UACI [20]. Equation (8) is used to compute the correlation coefficient.

$$NSCR = \sum_i \frac{DV(i)}{T} \times 100, \quad (7)$$

$$DV(i) = \{0 \ \ if \ \ D_1(i) = D_2(i)\ 1 \ \ if \ \ D_1(i) \neq D_2(i),$$

$$UACI = \sum_i \frac{|D_1(i) - D_2(i)|}{65535} \times 100. \quad (8)$$

Where $D_1(i)$ represents the original speech signal, $D_2(i)$ the encrypted speech signal, and $DV(i)$ the sample value at position i. (T) is the count number of audio samples.

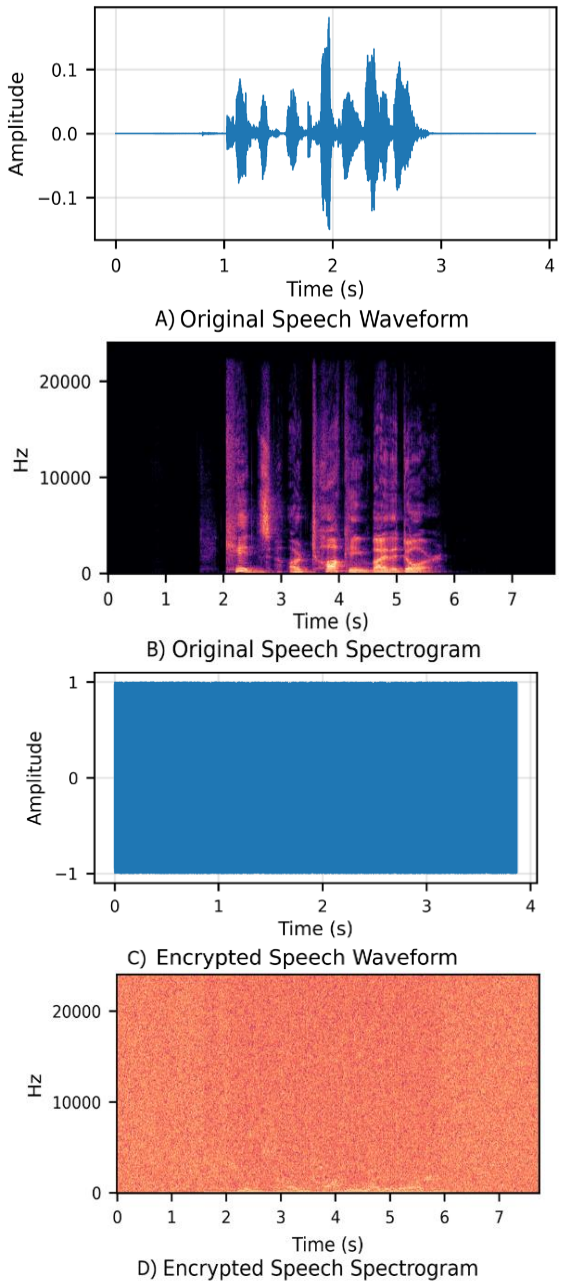

Figure 2: Sound waveform of an audio file from the RAVEDESS dataset: (A) Original speech waveform, (B) Original speech spectrogram, (C) Encrypted speech waveform, and (D) Encrypted speech spectrogram.

5.3 Mean Square Error (MSE)

It is used to evaluate the decryption quality of any decrypted audio file. A closer value to 0 shows perfect decryption, meaning that the decrypted and original audio files are similar [20], [21]. Equation (9) is used to compute the correlation coefficient.

5.4 Peak Signal Noise Ratio (PSNR)

It is used to calculate the level of distortion between the original and the deciphered signal. A low PSNR value between the encoded and original speech shows significant distortion, while a high PSNR value shows accurate restoration of the original sound [20], [21]. Equation 10 is used to compute the correlation coefficient.

5.5 SNR

It is used to analyze the encrypted audio file. The encryption quality is better when the SNR is more negative [20]. Equation 11 is used to compute the SNR.

$$MSE = \frac{1}{N}\sum_{i} (A_1(i) - A_2(i))^2, \quad (9)$$

$$PSNR = 10 \times log_{10}\left(\frac{MA^2}{MSE}\right), \quad (10)$$

$$SNR = \frac{AU_{signal}}{AU_{noise}}. \quad (11)$$

Where:

- (MA) represents the largest potential value of an audio file;
- (AU_{signal}) represent the original speech signal;
- (AU_{noise}) represent the noise that added to the original speech signal.

5.6 Shannon Entropy

It is used in audio encryption research to evaluate how close the encrypted signal is to a random sequence. A value nearest to 16 bits shows a high resistance to statistical attacks [22].

5.7 Key Space Analysis

High-level encryption methods are needed to make it more difficult for attackers to search the key space and to lengthen the time required to decrypt the key. Among these methods is the use of chaotic maps because of their big sensitivity to initial conditions and control settings. The hybrid chaotic key used in this method includes six control parameters. According to the IEEE 754 standard, the important number in a double-precision floating-point key is 52 bits. Therefore, the hybrid chaotic key space size used

in this method is $(2^{52})^6 = 2^{312}$, which is larger than 2^{128} and large enough to resist brute-force attacks.

5.8 Correlation

It is used to measure the linear connection between the encrypted and original signals. The encryption result is better when the correlation coefficient is lower [10], [23].

Table 3 shows the average results of a set of tests on 40 audio files (RAVDESS dataset) and 25 audio files (TIMIT dataset) after applying the proposed method.

To confirm the high sensitivity of keys to any change in the initial values used in key generation, which leads to different results than using the original data, an experiment was conducted to change one initial parameter for finding the random logistic map (m1 = 3.99 to 3.90). The results (MSE = 0.8613, SNR = -2.25 dB, and Percentage Difference = 99.9989%) obtained from comparing the sample encoded with the original data and the sample encoded with the modified data prove that any change in any of the parameters leads to a change in the result. Tables 4 and 5 compare the proposed method's test dataset results with those of other studies.

Table 3: Average set of test results on 40 audio files (RAVDESS dataset) and 25 audio files (TIMIT dataset).

Test type	RAVDESS	TIMIT
Size Audio File	341.48 KB	101.96 KB
Encryption Time	1018.80 MS	289.11
NSCR	100	100
AUCI	33.27	31.57
Entropy (Encryption) 16 bit	15.226	14.671
Entropy (Decryption) 16 bit	6.951	9.323
PSNR (Encryption)	3.022	3.322
PSNR (Decryption)	80.1805	79.3304
SNR (Encryption)	-38.8395	-33.0268
SNR (Decryption)	38.083	40.518
correlation (Encryption)	-0.1578	-0.2045
correlation (Decryption)	0.9999	0.9999

Table 4: The results compared (NCSR and UACI) the proposed method with those of other methods.

Ref.	Number of audio samples	NSCR	UACI
Ref. [2]	8 audio files	99.63	-
Ref. [10]	3 audio files	99.58	33.65
Ref. [11]	3 audio files	99.74	-
Ref. [4]	2 groups of audio files	100	-
Ref. [9]	4 audio files	100	33.12
Our method	RAVDESS dataset 40 audio files	100	33.27
	TIMIT dataset 25 audio files	100	31.57

Table 5: The results compared (correlation test) the proposed method with those of other methods.

Ref.	Correlation		
	Encryption		Decryption
Ref. [2]	0.00008		-
Ref. [10]	-0.0484		0.9819
Ref. [11]	0.0029		0.8657
Ref. [4]	-0.0006		-
Ref. [9]	-0.0002		1
Our method	REVDESS dataset	-0.1578	0.9999
	TIMIT dataset	-0.2045	0.9999

6 CONCLUSIONS

With the faster development of the internet and the ability to share and transfer various types of data, including multimedia, many concerns have been raised regarding the security of this information transfer. Therefore, researchers are constantly striving to find modern methods to address these concerns and prevent unauthorized access to information and its potential manipulation. This paper suggests an audio encryption approach that mixes DNA sequences and chaotic systems across several phases. The audio file is first prepared and encoded using a DNA code. The second step is to use three chaotic maps (the Logistics Map, the Tent Map, and the Pocket Map) to generate a hybrid key. Finally, to generate an encrypted audio file, it applies the XOR operation between the hybrid key and the encoded audio file data. The proposed hybrid chaotic and DNA encryption scheme performs consistently across different speech datasets (RAVDESS, TIMIT). It achieves the highest NSCR (100%), exhibits a great level of randomness in the encrypted signals (approximately 15-16), and shows a notable difference compared to the original signals. Although RAVDESS has a slightly higher UACI and TIMITDIC has more original entropy, both datasets show that the encryption method offers powerful protection for audio, whether it's emotional or balanced in speech sounds.

REFERENCES

[1] T. Haridas, S. D. Upasana, G. Vyshnavi, M. S. Krishnan, and S. S. Muni, "Chaos-based audio encryption: Efficacy of 2D and 3D hyperchaotic systems," Franklin Open, vol. 8, no. September, 2024, doi: 10.1016/j.fraope.2024.100158.

[2] H. A. Qasim, "A new Audio Encryption Algorithm Based on Hyper-Chaotic System," Mustansiriyah J. Pure Appl. Sci., vol. 1, no. 3, pp. 85-94, 2023.

[3] M. Demirtaş, "A Sound Encryption Method Based on Feature Extraction and a Novel Chaotic Map," in 10th International Conference on Computer Technology Applications (May 2024), 2024, no. May, pp. 303-309, doi: 10.1145/3674558.3674602.

[4] I. A. Taqi and S. M. Hameed, "A Secure Audio Encryption Method Using Tent-Controlled Permutation and Logistic Map-Based Key Generation," Comput. Mater. Contin., vol. 85, no. 1, pp. 1653-1673, 2025, doi: 10.32604/cmc.2025.067524.

[5] S. S. Ahmed and S. A. Kadhim, "A Review on Chaotic Cryptosystems for Digital Speech Communication," J. Al-Ma'moon Coll., vol. 1, no. 39, pp. 182-201, 2023, doi: 10.36458/1253-000-039-011.

[6] A. Kumar and M. Dua, "Audio encryption using two chaotic map based dynamic diffusion and double DNA encoding," Appl. Acoust., vol. 203, 2023, doi: 10.1016/j.apacoust.2022.109196.

[7] Y. Huang, L. Wang, Z. Li, and Q. Zhang, "A new 3D robust chaotic mapping and its application to speech encryption," Chaos, Solitons & Fractals, vol. 184, no. July, 2024, doi: 10.1016/j.chaos.2024.115038.

[8] E. H. Haseeb, S. A. Kadhim, and A. S. Mahmood, "A Six-Dimensional Hyperchaotic Pseudorandom Sequence for Enhanced Voice Encryption," Inf. Syst. Eng., vol. 28, no. 4, pp. 1055-1062, 2023, doi: 10.18280/isi.280425.

[9] S. F. Yousif and H. A. Abdulkadhim, "Speech signal security scheme based on multiple chaotic maps with deoxyribonucleic acid coding algorithm," Int. J. Electron. Telecommun., vol. 71, no. 1, pp. 69-78, 2025, doi: 10.24425/ijet.2025.153546.

[10] S. A. Gebereselassie and B. K. Roy, "Speech encryption algorithm based on two newly designed chaotic maps," Franklin Open, vol. 5, no. November, p. 100055, 2023, doi: 10.1016/j.fraope.2023.100055.

[11] M. Demirtaş, "A Lossless Audio Encryption Method based on Chebyshev Map," in Orclever Proceddings of Research and Development, 2023, pp. 28-38, doi: 10.56038/oprd.v2i1.234.

[12] N. F. Hassan, A. Al-Adhami, and M. S. Mahdi, "Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps," Iraqi J. Sci., vol. 63, no. 2, pp. 830-842, 2022, doi: 10.24996/ijs.2022.63.2.36.

[13] M. S. Fadhil, A. K. Farhan, and M. N. Fadhil, "Designing Substitution Box Based on the 1D Logistic Map Chaotic System," IOP Conf. Ser. Mater. Sci. Eng., vol. 1076, no. 1, p. 012041, 2021, doi: 10.1088/1757-899X/1076/1/012041.

[14] P. Sathiyamurthi, J. Mohamed, and M. Suman, "A Novel Approach for Speech Encryption using Lorentz and Tent Chaotic map," UGC Care J., vol. 3, no. 3, pp. 249-256, 2020.

[15] W. Alexan, M. Gabr, E. Mamdouh, R. Elias, and A. Aboshousha, "Color Image Cryptosystem Based on Sine Chaotic Map, 4D Chen Hyperchaotic Map of Fractional-Order and Hybrid DNA Coding," IEEE Access, vol. 11, no. June, pp. 54928-54956, 2023, doi: 10.1109/ACCESS.2023.3282160.

[16] I. Qays and A. Hameed, "Hide Medical Images in a Speech Signal using DNA Coding and Fuzzy C-Means," in 2nd Annual International Conference on Information and Sciences, 2020, pp. 119-126, doi: 10.1109/AiCIS51645.2020.00029.

[17] S. T. Allawi, Y. M. Mohialden, and N. M. Hussien, "Protection of the Image Data by Using Chaotic Maps and DNA Sequence," Int. J. Intell. Eng. Syst., vol. 17, no. 4, pp. 451-462, 2024, doi: 10.22266/IJIES2024.0831.35.

[18] J. S. Garofolo, L. F. Lamel, W. M. Fisher, J. G. Fiscus, D. S. Pallett, and N. L. Dahlgren, "Darpa timit," 1990, doi: 10.35111/17gk-bn40.

[19] S. R. Livingstone and F. A. Russo, The Ryerson Audio-Visual Database of Emotional Speech and Song (RAVDESS): A Dynamic, Multimodal Set of Facial and Vocal Expressions in North American English, 2018, doi: 10.1371/journal.pone.0196391.

[20] P. Sathiyamurthi, T. Thrisith, J. Kamaleshwaran, and K. Tamil, "Chaotic Random Number Generation using Gauss and Standard Chaotic Maps for Secured Audio and Speech Communication," Int. J. Adv. Sci. Technol., vol. 29, no. 10, pp. 8144-8152, 2020.

[21] W. Dai, X. Xu, X. Song, and G. Li, "Audio Encryption Algorithm Based on Chen Memristor Chaotic System," Symmetry (Basel)., vol. 14, no. 17, pp. 1-19, 2022, doi: 10.3390/sym14010017.

[22] A. K. Jawad, G. Karimi, and M. Radmalekshahi, "A Novel Digital Audio Encryption Algorithm Using Three Hyperchaotic Rabinovich System Generators," Sci. J. Koya Univ., vol. 12, no. 2, pp. 234-245, 2024, doi: 10.14500/aro.11869.

[23] H. M. Elrefai, W. S. Sayed, and L. A. Said, "Hardware Implementation of a 2D Chaotic Map-Based Audio Encryption System Using S-Box," Electronics, vol. 13, pp. 1-13, 2024, doi: 10.3390/electronics13214254.