

Optimized Digital Audio Scheme Using 4D Lorenz Hyperchaotic System, FAN Transform, and ABC Optimization

Zahraa Dawood Salman Al-Gburi¹ 

¹Department of Computer Engineering Techniques, Bilad Alrafidain University, 32001, Diyala, Iraq
dr.zahraadawod@bauc14.edu.iq

Abstract

A significant amount of data is transmitted globally in audio format, making audio security increasingly important. Audio encryption is thus essential for protecting sensitive data from unauthorized access and modern security threats. This research proposes a hybrid encryption framework that combines the Fast Approximation of Nonlinear (FAN) Transform with the Artificial Bee Colony (ABC) optimization algorithm. Initially, the input signal is converted into a 256×256 two-dimensional matrix and normalized to prepare it for encryption. Finally, the Artificial Bee Colony algorithm is utilized to perform an additional scrambling phase, searching for an optimal permutation that minimizes the correlation between adjacent signal elements. The novelty of the proposed scheme lies in jointly integrating these four components into a single encryption pipeline; the FAN transform, coupled with the 4D Lorenz hyperchaotic system, provides high-complexity spatial permutation. This multilayered encryption approach ensures high security by combining chaos theory, bio-inspired computing, and evolutionary optimization. Experimental results indicate an average value for correlation coefficient of 0.000002, several Pixels Change Rate (NPCR) of 99.59%, a Unified Average Changing Intensity (UACI) of 26.06%, a Peak Signal-to-Noise Ratio (PSNR) of 10.30874, a Mean Squared Error (MSE) of 6069.17, a Signal-to-Noise Ratio (SNR) of 3.673422, the entropy of 7.996856 and the Log-Likelihood Ratio (LLR) of 4.9577.

Keywords: Audio Encryption, FAN transform, Lorenz hyperchaotic system, DNA Encoding, ABC optimizer.

Article history: Received: 23 Jun 2026, Accepted: 2 Sep 2026, Published: Next Issue.

This article is open-access under the CC BY 4.0 license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The demand for strong data security has grown dramatically with the rapid development of mobile devices and multimedia technologies. Audio, video, and image data have become integral to modern communication. Audio plays a particularly important role in multimedia systems. Audio data is susceptible to leaks if not encrypted properly, which could threaten user privacy and have dire consequences. Therefore, audio encryption has become an increasingly active research area [1], [2].

Modern encryption techniques are based on two basic principles: confusion and diffusion. Confusion is the property of the encryption process that obscures

the relationship between the secret key and the ciphertext. Diffusion is the property of the encryption process that spreads the statistical characteristics of the plaintext over the ciphertext to hide them.

In recent years, chaos theory has proven effective in providing confusion and diffusion for cryptographic systems [3]. Chaotic maps present a dynamic, highly nonlinear behavior and extreme sensitivity to initial conditions and control parameters: even slight perturbations in initial values yield drastically different trajectories, providing a high degree of unpredictability. This property improves the randomness needed for cryptographic applications, and chaotic maps have been widely used in audio encryption schemes accordingly [4], [5], [6].

Due to its natural parallelism, large data storage capacity, and low power consumption, DNA cryptography has also become a promising method for information security. These properties enable DNA-based encryption to be computationally more efficient than conventional methods such as DES and AES. DNA computing was first introduced in 1994, and since then, it has been combined with chaotic maps to design highly secure hybrid encryption schemes, which have been extensively investigated in image encryption [7].

Nevertheless, audio data differs from text or still images when it comes to security. Audio files are significantly larger and often must be processed in real time, for example, in video conferencing. Conventional encryption techniques developed for text data are inefficient for large amounts of audio data and increase processing time and storage overhead. Thus, it is necessary to balance encryption strength with processing efficiency. More importantly, some encryption methods introduce noise or distortion, which lowers audio quality, so preserving both security and fidelity is a main focus in multimedia security research [8], [9], [10], [11].

To address these issues, this paper proposes an audio encryption scheme based on the FAN transform, DNA coding, and Artificial Bee Colony (ABC) optimization. First, the audio signal is permuted using the FAN transform and the Lorenz hyperchaotic system to provide the first level of scrambling. Then, the DNA matrix built on the permuted signal is XORed with the key DNA matrix obtained from the chaotic sequence to achieve diffusion. Finally, the scrambling is improved using a correlation-based objective function with the help of the ABC optimization algorithm. The objective function minimizes the correlation between the samples toward zero, resulting in the encrypted audio output. The major contributions of this work are summarized below:

- (a) The FAN transforms and the Lorenz hyperchaotic system are combined in a first-stage scrambling scheme that improves randomness and overall encryption strength by strengthening confusion and diffusion beyond what simple sample-level scrambling can accomplish.
- (b) A DNA-based encoding stage that increases computational speed and storage/transmission efficiency by using a logistic map to generate the key sequence and an XOR operation to carry out the core diffusion step.
- (c) The ABC optimization algorithm is used in a second stage of scrambling to create a more secure ciphered audio signal by minimizing inter-sample correlation toward zero.

The paper is organized as follows: Section 2 reviews related work. Section 3 describes the DNA encoding method. Section 4 introduces the chaotic systems. Section 5 describes the FAN transform. Section 6 introduces the Artificial Bee Colony algorithm. Section 7 describes how the audio is encrypted, and Section 8 describes how the audio is decrypted. Section 9 shows simulation experiments and security analysis. Section 10 compares the proposed scheme with related work. Section 11 concludes the study.

2. Related Work

Several chaos-based encryption algorithms have been proposed over the past 20 years. In recent years, research has focused more on audio encryption, using sophisticated chaotic and hybrid techniques to increase security beyond what traditional ciphers can offer.

In this study, Jawad et al. [13] proposed an audio encryption algorithm based on three hyperchaotic Rabinovich generators, chaotic integer keys, non-sequential index selection, and XOR operations, with secure key exchange via Diffie-Hellman. The scheme exhibited high entropy, near-zero correlation, and a large key space, making it suitable for sensitive applications such as military or medical communications. However, the scheme is limited to basic metrics, lacks testing against advanced cryptanalytic attacks, and does not address practical concerns such as real-time performance and robustness in noisy channels.

Abdallah and Meshoul proposed a multi-layer audio encryption system that combines audio with active hiding signals and employs fusion, substitution, and permutation based on sample values. The evaluations demonstrate good performance and robustness in noisy environments. Nevertheless, the study is constrained by simulation-based assessment

and limited comparison with recent chaotic hybrid schemes [3].

Regarding the Mordell elliptic curves, symmetric permutation groups, and chaotic maps, Aziz et al. presented a noise-tolerant real-time audio encryption framework focused on modular scalability, low computational overhead, and robustness against noise. The scope of security analysis remains narrow, as resistance to advanced cryptographic attacks was not fully explored [10].

Naskar et al. demonstrated an audio encryption method that achieved near-zero correlation and high sample change rates by using channel shuffling, logistic chaotic maps, and DNA encoding. The scheme was not tested for resilience against differential or brute-force attacks, or for practicality in large-scale or real-time use [19].

A hybrid encryption scheme based on elliptic curve cryptography and chaotic maps has been suggested for audio transmission in GFDM modulators by Ameen and Hreshee [8], which is secure and fast in encryption/decryption. However, the study was based only on simulation. It did not evaluate energy consumption, latency, or compare the cryptography methods used with other cryptography methods. Also, the audio encryption scheme was introduced to improve statistical randomness and resistance to differential attacks by combining double DNA encoding with two chaotic maps for dynamic diffusion. However, the method was only validated on a small dataset, so its generalizability across various audio formats was not investigated.

Although computational efficiency and robustness under noisy or lossy channels remain unaddressed, Zghair et al. developed a speech scrambling approach that combined a seven-dimensional hyperchaotic system with DCT to achieve a large keyspace and strong security, outperforming recent methods in simulation [27].

Fu et al. [10] proposed a new hyperchaotic system with specialized circuit realization and feedback control. They applied it to audio encryption with strong statistical efficiency. The work focuses more on circuit-level validation than on large-scale cryptanalytic testing, leaving broader security evaluation for future studies.

To improve security and predictability, Abdullah and Abduljaleel proposed a three-stage speech encryption method that uses DNA coding, multi-chaotic maps, and S-box substitution [18]. The method's performance under various communication conditions and its resistance to sophisticated cryptanalytic attacks have not yet been investigated.

The study did not address real-time performance, computational complexity, or scalability to larger datasets [16]. Khaleel and Abduljaleel developed a speech encryption method that combines quantum chaotic maps with k-means clustering for creating standard keys using two-stage bit- and block-level scrambling.

In this study, Guo et al. presented a cautious vortex-like chaotic system with tunable parameters for audio cryptography, with strong ergodicity and a large parameter space. Nevertheless, the study does not benchmark performance against DNA-based or optimization-assisted encryption schemes, thereby limiting direct comparison with hybrid methods such as the one outlined here.

All of these studies show consistent advancements in chaos- and DNA-based audio encryption, but common drawbacks remain: most schemes rely on a single propagation or scrambling mechanism, there is little cryptanalytic testing, and there is no optimization-driven refinement of the scrambled output. In this particular work, we bridge these gaps by integrating permutation based on the FAN transform, DNA-based diffusion, and ABC-enhanced scrambling under one umbrella.

3. Methodology

This section presents the methodology underlying the proposed audio encryption scheme. It first introduces the foundational concepts required by the design, namely DNA encoding and the chaotic systems used for key generation, before detailing the FAN transform and the Artificial Bee Colony (ABC) optimization algorithm employed for signal scrambling. These components are then integrated into the complete encryption procedure, followed by a description of the corresponding decryption process.

3.1 DND Encoding

There are four nucleotides in the DNA of living organisms. Cytosine (C), adenine (A), guanine (G), and thymine (T). These are the building blocks of DNA. The complementary base pairing rules, where adenine pairs with thymine and cytosine pairs with guanine, make it possible for these nucleotides to be binary encoded as 10, 00, 11, and 01, respectively. This gives a total of eight possible coding schemes. In audio encryption, each audio sample is first converted to a binary sequence and then encoded with four DNA nucleotides. Table 1 summarizes the specific mapping for encryption and decryption on audio data. The encryption process uses a DNA-based XOR operation, which is logically analogous to the conventional binary XOR [1].

3.2 DND Encoding

Chaotic systems are a class of nonlinear dynamical systems that exhibit high sensitivity to initial conditions and control parameters. Minor changes in the starting values can result in significantly different behaviors. Two examples of chaotic systems are presented below [20].

3.2.1 Lorenz hyperchaotic system

This section presents a new four-dimensional chaotic system derived from the classic Lorenz-Haken model. By extending the original system into four dimensions, the resulting chaotic system exhibits increased complexity and unpredictability. These enhanced characteristics improve its suitability for secure communication and encryption applications. The system is described by the following equations:[21], [22].

$$\begin{aligned} \frac{dx}{dt} &= A * (Y - X) + W, \quad \frac{dy}{dt} = C * X - Y - X * Z, \\ \frac{dx}{dt} &= X * Y - B * Z, \quad \frac{dw}{dt} = -Y * Z + R * W \end{aligned} \quad (1)$$

Where the parameters $C = 28$, $A = 10$, $R = -1$, $B = 8/3$, and the values for $[X, Y, Z, W] = 1$.

3.3 Logistic map chaotic system

The Logistic map is a mathematical function defined by a nonlinear recurrence relation that generates two-dimensional, non-periodic chaotic sequences. The following equation represents it [23]:

$$P_{n+1} = U \times P_n \times (1 - P_n) \quad (2)$$

where the value of P is between 0 and 1, and the optimal range for U is between 3.57 and 4.

3.4 FAN Transform

A transformation must be a one-to-one mapping to ensure that an inverse exists, allowing the original data to be recovered. In image processing, such mappings rearrange pixel positions using positive integer coordinates. The Arnold transform is a well-known example, but many other coordinate transformations can achieve similar effects. If the modulus operation in the Arnold transform is removed and applied to a larger image, the result remains linear and invertible, with no repeated positions in the smaller region. This makes it suitable for both compression and encryption. In a previous study, the FAN transform was introduced and used for scrambling because of its strong reversibility and unique mapping properties. This transform continues to be explored for its potential in secure multimedia applications [24], [25]. The following equation defines the FAN transform.

$$\frac{K_1}{K_2} = \frac{1}{Y_{I,J}} \frac{X[I,J]}{X[I,J] * Y[I,J] + 1} \times \frac{I}{J} \bmod \frac{m}{n} + \frac{1}{1} \quad (3)$$

Here, k_1 and k_2 represent the indices of the new position in the scrambled matrix, denoted as $P[k_1, k_2]$. The variables i and j refer to the row and column indices of the matrices X and Y , respectively. At the same time, $m=256$ and $n=256$ define the matrix dimensions.

3.5 Artificial Bees Colony (ABC) Algorithm

The Artificial Bee Colony (ABC) algorithm is an optimization method inspired by the foraging behavior of honey bees. It was proposed to solve complex numerical and combinatorial optimization problems efficiently. In ABC, the population of artificial bees is divided into three groups: employed bees, onlooker bees, and scout bees. Employed bees explore the neighborhood of their current food sources (candidate solutions) and share information about the quality (fitness) of these sources with onlooker bees through a waggle dance. Onlooker bees choose food sources to exploit based on probabilistic information shared by other bees, favoring higher quality solutions. Scout bees search for new random food sources when the fitness of current sources is too low to survive, enhancing the algorithm's ability to explore the search space. It starts from a set of random solutions. It iteratively updates a set of neighboring solutions by assessing their fitness and selecting the best candidates. This iterative process balances exploration (via scouts and diverse search) and

exploitation (via neighborhood searches and onlooker selection). This allows the algorithm to escape local optima and consistently converge toward the global optimum. ABC has been successfully applied to function optimization, engineering design, scheduling, and routing problems and is valued for its ease of use, flexibility, and effectiveness in complex problems [26].

3.6 Audio Signal Encryption Method

This method is considered to be one of the most efficient strategies in audio encryption. It addresses traditional problems by proposing novel methods such as the FAN Transform, DNA coding, and the Artificial Bee Colony (ABC) optimization method. The FAN Transform is combined with the Lozenges 4D hyperchaotic system to obtain a robust and efficient permutation of audio signals. Then, each part of the audio signal is replaced with DNA coding. Next, the audio signal location is scrambled using the correlation between audio samples with the ABC optimization method. The signals are encrypted so they look like random noise, increasing security; Fig. 1 shows the general framework of the proposed method. The steps of the system are explained as follows:

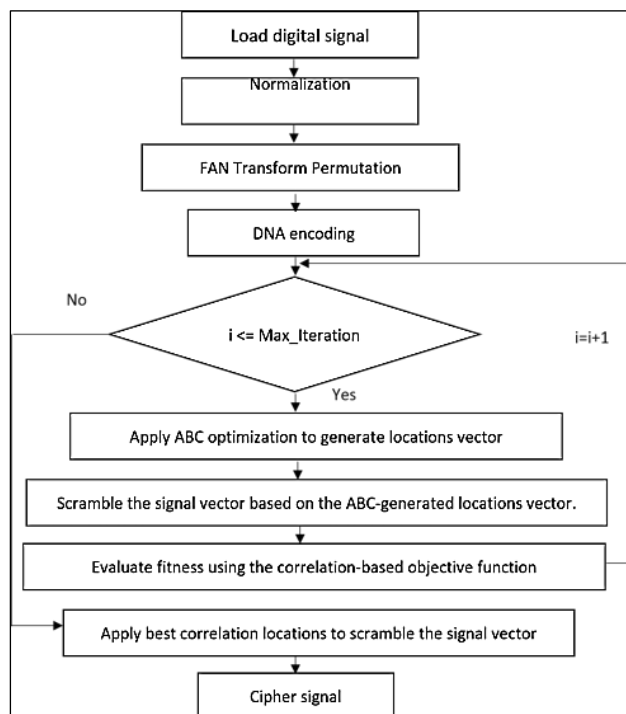


Fig. 1 Illustration of the system architecture for the proposed audio encryption method.

Step 1. The Digital Signal Loading

The sound signal is first input and read as audio samples. During preprocessing, these samples are converted into a vector containing 65,536 elements, to be converted into a 2D matrix. This vector is then reshaped into a 256 by 256 matrix.

Step 2. Normalization

Normalize the signal matrix to the range [0, 255] to facilitate processing during the DNA encoding phase. This is achieved using the following equation: Here, the signal value denotes the original signal value. The resulting normalized signal is the value scaled to the range [0, 255].

Step 3. FAN Transform Permutation

In this step, the signal locations within the matrix are modified using the FAN transform and the Lorenz hyperchaotic system. First, two arrays, X and Y, each of size 256×256, are generated using the Lorenz hyperchaotic system, as shown in equation (1). Both arrays are ensured to be unique, with no repeating elements. The process is then continued for all indices i and j; equation 3 is applied to arrays X and Y to alter the position of each element in the digital signal matrix.

Step 4. DNA encoding process

The digital signal is first converted to binary, with each value represented by 8 bits. These bits are then grouped into pairs of 2 bits. Each 2-bit group is mapped to a DNA nucleotide based on a selected DNA encoding rule. There are 8 possible encoding rules, each defining a unique mapping between 2-bit combinations and DNA bases. For example, one such rule maps (00 → A), (01 → C), (10 → G), and (11 → T). Therefore, the DNA representation is DNA_seq, the result of converting the digital signal depending on the chosen encoding rule.

Generate the key to be used in DNA-based encryption by first using the Logistic Map to produce a sequence of chaotic numbers IDX in the range [1, 4]. Then, convert each number into its corresponding DNA code using the vector D = [A, C, G, T], where each number in the sequence represents an index in the vector D. The DNA code is obtained by mapping each number to its corresponding nucleotide based on this vector. Where KE represents the encrypted key, and IDX denotes the sequence of chaotic numbers in the range [1, 4], generated using the Logistic Map as defined by Equation (2).

Once the data is converted into DNA format, an XOR operation is performed between two DNA sequences of equal length: KE (the encrypted key) and the DNA_seq (DNA-encoded digital signal) using DNA-specific XOR rules.

Where Encrypted_DNA represents the result obtained after performing the XOR operation

Step 8: Scrambling with ABC Phase

The strength of the encryption process depends heavily on the ABC. The ABC method searches multiple position vectors to find the one that yields the minimum correlation value, representing a highly randomized framework, given the result obtained from the DNA-based encryption. This optimal vector is then used to shuffle the elements of the input matrix. This scrambles the initial layout. The ABC optimization motivated this strategic permutation, which aims at improving the signal positions by minimizing statistical correlation. The end product of this transformation is a one-dimensional array, which is the encrypted audio signal. The detailed procedure is shown as follows:

1. Flatten the 2D audio signal into a one-dimensional vector
2. Generate the initial population for the ABC optimization F , where each individual has the same size as the audio signal with a size 1 by 65,536.
3. Each solution (population) is sorted in ascending order, and the resulting indices are used to guide the scrambling of the audio signal as shown the following equation.
4. The scrambled indices derived from the population are applied to the digital signal to produce the scrambled vector .
5. The fitness value is computed using an objective function that evaluates the correlation between the original audio signal and the ABC-encrypted signal (ABC_Audio).
6. The ABC optimization algorithm is employed to update the population F , thereby generating new candidate solution positions
7. Iterate steps 2 through 5 for a total of 30 iterations
8. In the final step, the encrypted audio signal vector (Encrypted_DNA) is scrambled using the optimal solution, identified as the one with

the lowest correlation value from step 4, as per the scrambling procedure in step 3, to generate the final encrypted audio signal.

In the decryption phase, the initial values of the Lorenz hyperchaotic system and Logistic map must be transmitted to regenerate the same keys used during the encryption process, including the key employed for DNA encoding. Additionally, the scrambling position sequence used by the ABC algorithm must also be sent to enable proper decryption. Decryption is essentially the reverse of the encryption process. First, the scrambling operation performed by the ABC algorithm is reversed. Then, the DNA sequence is decoded using the same encryption key received from the sender. After that, the permutation process is inverted using the FAN transform in conjunction with the Lorenz hyperchaotic system. Finally, the normalization step is reversed to recover the original signal.

4. Simulation Results and Discussion

In this section, we present and discuss the test results for evaluating the performance of the proposed method. When you receive the encrypted signal, the spoken words are unintelligible. The original information has been completely obscured. The following measures are used to assess the quality and efficiency of the encryption processes.

4.1 Key space analysis

The initial values x , y , and z of a continuous chaotic system controlled by nonlinear differential equations are used by the system. With a valid precision of $10^{(-14)}$ for each initial condition, the resulting key space is about 10^{42} , which is about 2^{139} in binary. The key space must be larger than 2^{100} to resist exhaustive search attacks. The proposed method provides a key space large enough to make brute-force attacks impractical. This increases the security a lot, as attackers will not be able to discover the key in a reasonable period of time, thus making the encryption robust. This makes the key space at the receiver side very large and thus resistant to brute-force attacks.

4.2 Histogram analysis

The histogram examination is a powerful tool for the evaluation of the distribution of data in many fields involving encrypted data. When encrypting audio, the encrypted signal must have a uniform distribution

histogram, i.e., the digits should be evenly spread and should not expose any obvious patterns. The randomness means that the original audio features have been well concealed. The histograms of the original (plain) audio and the encrypted (cipher) audio show a distinct contrast, as shown in Fig. 2, the two channels of the cipher audio exhibit a nearly flat, uniform distribution. The results show that the encryption method has successfully masked the original audio data, and it is quite robust to statistical and differential attacks. Thus, the histogram examination strongly supports the robustness and effectiveness of the proposed encryption techniques.

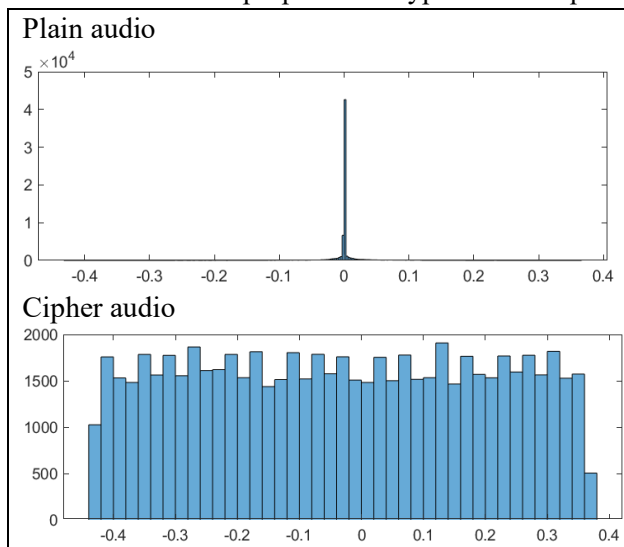


Fig. 2 The histograms of the original (plain) audio and the encrypted (cipher) audio

4.3 Spectrogram Analysis

A spectrum is a graphical representation of the variation of frequency content of an audio signal over time, obtained by applying the Short-Time Fourier Transform (STFT) to the time-domain samples. In a well encoded audio, the spectrogram shows a quite uniform distribution of the frequency components, which means that any patterns in the original signal have been removed. Fig. 3 shows the spectrogram of the encrypted audio, which has a uniform and balanced distribution of frequencies. It indicates that our encryption method can effectively conceal the original data and resist the attack based on frequency analysis. This uniformity confirms the robustness and success of the proposed encryption technique.

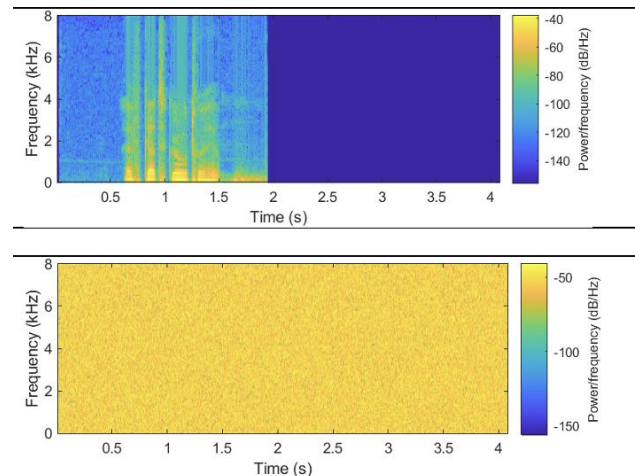


Fig. 3 The spectrogram of the encrypted audio demonstrates a consistent and balanced frequency distribution.

4.5 Correlation Analysis

A high degree of correlation is usually seen between consecutive samples in an unencrypted audio file. To improve the security of the audio encryption algorithm, the correlation coefficient should be reduced significantly. Decreasing the similarity of adjacent audio samples can help to protect against statistical attacks.

Where (x_i, y_i) are the amplitude levels of pairs of randomly selected audio samples, and L is the total number of pairs. where $E(y)$ and $E(x)$ are the mean values of the corresponding audio sample sets. Table 4 gives the correlation coefficient values calculated for the test audio files. In the original form of the audio files, the audio files have a high correlation among the sample pairs, but after encryption with the proposed algorithm, the correlation drops to near zero. This means that the algorithm is robust against statistical attacks. Besides, the correlation graphs show this behavior. The correlation of selected pairs of audio samples from the test file is shown in Fig. 4. The top row corresponds to the original signals, and the bottom row reflects the distribution after encryption. The original signals show strong clustering, indicating high correlation, while the encrypted signals exhibit a scattered distribution, signifying the loss of correlation and thus confirming the robustness of the encryption method.

4.6 Information Entropy Analysis

An effective way to gauge how random and unpredictable audio signals are is to use conventional

data entropy. The entropy value of around 8 (theoretical) means a very complex and random signal. Therefore, a good audio encryption algorithm should be near the entropy of 8. In the experiment, the audio files were used to calculate the entropy values, which are shown in Table 1. The results reveal that the encrypted audio signals have near-ideal entropy values of at least 7.99, indicating a high level of randomness. This large increase in entropy shows that there are no identifiable patterns in the encrypted audio, making statistical or pattern-based analysis very challenging for attackers. Therefore, the high entropy values justify the success of the proposed encryption method in securing the audio data against potential cryptanalytic attacks [14].

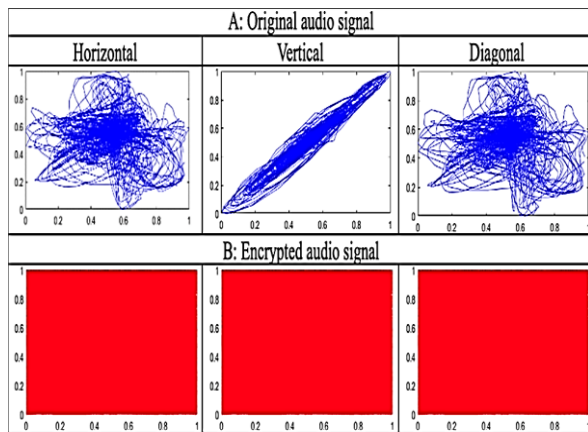


Fig. 4 Correlation between the samples in size 256 by 256 in (A) original audio file, (B) encrypted audio file

The correlations represent the two signals at any location of the cipher signal segments, and N_s denotes the length of the audio signals. The encryption scheme with a higher value of UACI and NPCR as compared to theoretical values is considered as stronger and more secure. The proposed scheme distorts the original signal by modifying a randomly picked sample. The UACI and NPCR are then calculated for different audio signals using the encrypted versions of both the original signal x and the modified audio x' , as shown in Table 1. The NPCR and UACI values consistently exceed the theoretical limits, according to the results. This shows strength against differential attacks. This robustness is due to the pseudo-randomness of the chaotic key stream and the diffusion. The attacker cannot infer any meaningful relationship between the

plaintext and ciphertext, which greatly enhances security.

Table 1: Results of NPCR and UACI analyses between two audio signals

Audio Samples	NPCR	UACI
sample-1	99.58496%	25.62799%
sample-2	99.58191%	25.24218%
sample-3	99.56207%	26.98850%
sample-4	99.58801%	25.99023%
sample-5	99.63379%	26.46939%

4.9 Signal-to-Noise Ratio (SNR)

The SNR is a metric for determining signal quality by measuring the ratio of signal power to noise power. Higher SNR values indicate that the signal component is stronger relative to the noise component. The SNR can be calculated as follows[14]:

$$SNR = 10 * \log_{10} \frac{\sum_{i=1}^{N_s} x_i^2}{\sum_{i=1}^{N_s} (x_i - y_i)^2} \quad (4)$$

Where x_i and y_i denote the i -th samples of the plain and encrypted audio signals, respectively, and N_s represents the total number of samples. The computed SNR values using the proposed method for the audio signal are presented in Table 3. In the context of encryption, a low value of SNR indicates that the encrypted signal is more distorted relative to the original, thereby revealing less meaningful information to an attacker. Table 3 shows that the proposed method produces consistently lower SNR values, confirming its strong resistance to statistical attacks.

4.10 Peak Signal to Noise Ratio (PSNR)

The Mean Squared Error (MSE) is determined by evaluating the average of the squared differences between the signal as follows.

$$MSE = \frac{1}{n} \sum_{i=1}^n (X[i] - Y[i])^2 \quad (5)$$

Let X denote the plain audio signal, while Y denotes the encrypted audio signal; the Peak Signal-to-Noise Ratio (PSNR) can be calculated. In this context, MAX represents the maximum amplitude of the audio signal. The Peak Signal-to-Noise Ratio (PSNR) analysis results. These values are relatively low, which is good for encryption. Low PSNR means

more noise in the encrypted signal and better defense against possible attacks.

4.12 Root Mean Square (RMS) & Crest Factor (CF) values

The Root Mean Square (RMS) value represents the average amplitude level of an audio signal. When the input signal has a zero mean, the RMS is equivalent to the standard deviation [14].

The Crest Factor (CF) describes the relationship between the highest amplitude of a waveform and its root mean square (RMS) value. It serves as an indicator of how extreme the peaks are in relation to the overall signal level. For a constant DC signal, the CF reaches its minimum, equivalent to 0 dB, since no peaks exist. In contrast, higher CF values reveal the presence of significant peaks. The Crest Factor can be determined using the following expression

Table 2 displays the calculated RMS and CF values for the audio files that were evaluated according to the suggested scheme. These results demonstrate that there is no significant statistical correlation between the cipher and plain signal.

Table 2: The CF and RMS outcomes of the proposed encryption technique

Audio Samples	RMS	CF
sample-1	75.98906	16
sample-2	74.43473	16
sample-3	81.63372	16
sample-4	77.75303	16
sample-5	79.50714	16

4.11 Log-Likelihood Ratio (LLR):

The proposed Log-Likelihood Ratio (LLR) is a distance measure that can be directly calculated from the initial LPC vector for encoded and unprotected signals. This measure indicates the similarity or dissimilarity between signals and is defined as listed in Table 3 [18]:

Table 3: Indicates the analysis of the computation of LLR

Audio Samples	LLR
sample-1	4.55736
sample-2	4.84019
sample-3	4.96490
sample-4	5.16546
sample-5	5.26059

The Log-Likelihood Ratio (LLR) values in Table 8 show a large gap between encoded and unencrypted signals. This attests to the strong dissimilarity, ensuring reliability, security, and practical performance.

5. Comparison with Related Works

Compared with current methods, Table 4 shows that the proposed approach achieves robust, well-balanced performance. It has a key space of 2^{139} . It has good resistance against brute-force attacks. At the same time, it has a lower computational difficulty than those with too large a key space. This scheme achieved a positive SNR value of 5.23, which is better than the negative metrics obtained in multiple previous experiments. Excellent pixel decorrelation is confirmed by the correlation coefficient, which is almost zero (0.0000). Moreover, the approach suggested obtains the best LLR value (4.557) compared with other methods and offers a competitive PSNR (10.51), which is close to Ref. [14]. The CF is 16, which is higher than Ref. [15] but a little lower than Ref. [14]. The high MSE (5774.33) shows the strength of the encryption, and the entropy value (7.9966) is close to the ideal value of 8, which is better than most of the related works. In general, the results confirm that the proposed scheme provides high security and strong statistical performance compared with the previous methods.

Table 4: Comparison of the performance with other related works

Ref.	Key space	SNR	Correlation	LLR	PSNR	CF	MSE	Entropy
[16]	2^{510}	-27.8068	-	-	0.9142	-	0.63191	-
[12]	2^{11}	-40.097	-0.0009	-	-20.84	-	-	15.936
[13]	-	-3.0131	-0.000639	-	-	-	-	-
[14]	-	-	0.0031	-	10.7163	49.3	37.4487	7.9471
[15]	-	-	0.000207	-	-	4.8	-	-
[17]	2^{880}	-29.5849	-	-	0.004306	0.0001325	-	-
[18]	-	-23.0296	-0.0029	2.8841	-	-	-	-
[19]	-	-23.0106	0.0010	4.3764	-	-	-	-

Our	2^{139}	5.23395	0.00000	4.55736	10.5158	16	5774.33759	7.99661
-----	-----------	---------	---------	---------	---------	----	------------	---------

6. Conclusions

This research introduced a new cryptosystem and compared its effectiveness to several earlier methods. The findings showed that the suggested approach maintains computational efficiency while achieving a key space of 2^{139} , guaranteeing strong resistance to brute-force attacks. The proposed method achieved a low SNR of 5.23, which indicates superior encryption quality. The correlation coefficient (0.0000) demonstrates excellent pixel decorrelation, and the LLR (4.557) is better than comparable works, i.e., greater reliability. Also, the scheme achieved a PSNR of 10.51, comparable with the highest reported ones, and a CF value of 16, better than some existing approaches. Strong distortion between plain and encrypted images is indicated by the comparatively high MSE (5774.33), and quantitative security and high randomness are demonstrated by the entropy value (7.9966), which is near the ideal of 8. The suggested cryptosystem generally provides a good trade-off among security, strength, and efficiency, and is better than the related methods in key metrics such as SNR, correlation, LLR, and entropy. This result confirms its applicability for secure audio encryption applications. For future directions, concentrate on improving the scheme through deep learning methods and expanding its use to areas like secure communications and authenticating identities.

Acknowledgment

The author would like to thank the Department of Computer Engineering Techniques, Bilad Alrafidain University, Diyala, Iraq, for providing the technical support and resources necessary to carry out this research.

Conflict of Interest

The author declares that there is no conflict of interest regarding the publication of this article.

References

- [1] Wang, X., & Su, Y. (2019). An audio encryption algorithm based on DNA coding and chaotic system. *Ieee Access*, 8, 9260-9270.
- [2] Abdelfatah, R. I. (2020). Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. *IEEE Access*, 8, 69894-69907.
- [3] Abdallah, H. A., & Meshoul, S. (2022). A multilayered audio signal encryption approach for secure voice communication. *Electronics*, 12(1), 2.
- [4] Abduljaleel, I. Q., & Abdullah, S. M. (2021). Speech encryption technique using S-box based on multi chaotic maps. *TEM Journal*, 10(3), 1429.
- [5] Abed, Q. K., & Al-Jawher, W. A. M. (2024a). A secure and efficient optimized image encryption using block compressive sensing and logistic map method. *Journal of Cyber Security and Mobility*, 13(5), 983-1006.
- [6] Abed, Q. K., & Al-Jawher, W. A. M. (2024b). Enhanced hyperchaotic image encryption with CAW transform and sea-lion optimizer. *Journal of Cyber Security and Mobility*, 13(5), 1207-1237.
- [7] Abed, Q., & Al-Jawher, W. A. M. (2024c). Image encrypted using circular map, block compressed sensing and hyper GWO-COOT optimization. *International Journal of Intelligent Engineering & Systems*, 17(5).
- [8] Ameen, M. J. M., & 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), 3467-3479.
- [9] Albahrani, E. A., Alshekly, T. K., & Lafta, S. H. (2023). New secure and efficient substitution and permutation method for audio encryption algorithm. *The Journal of Supercomputing*, 79(15), 16616-16646.
- [10] Aziz, H., Gilani, S. M. M., Hussain, I., Janjua, A. K., & Khurram, S. (2021). A noise-tolerant audio encryption framework designed by the application of S8 symmetric group and chaotic systems. *Mathematical Problems in Engineering*, 2021, 5554707.
- [11] Feng, J., & Fei, H. (2009). FAN transform in image scrambling encryption application. In *2009 International Conference on Wireless Communications & Signal Processing* (pp. 1-4). IEEE.
- [12] Honglian, L., & Jing, F. (2012). Generalization of Arnold transform—FAN transform and its application in image scrambling encryption. In

- Recent advances in computer science and information engineering: Volume 5 (pp. 511–516). Springer.
- [13] Jawad, A. K., Karimi, G., & Radmalekshahi, M. (2024). A novel digital audio encryption algorithm using three hyperchaotic Rabinovich system generators. *ARO: The Scientific Journal of Koya University*, 12(2).
- [14] Kadhim, Q., & Al-Jawher, W. A. M. (2025). A new multiple-chaos image encryption algorithm based on block compressive sensing, Swin Transformer, and wild horse optimization. *Multidisciplinary Science Journal*, 7(1), 2025012.
- [15] Kamat, V. G., & Sharma, M. (2014). Symmetric image encryption algorithm using 3D Rossler system. *International Journal of Computer Science and Business Informatics*, 14(1).
- [16] Khaleel, A. H., & Abduljaleel, I. Q. (2021). A novel technique for speech encryption based on K-means clustering and quantum chaotic map. *Bulletin of Electrical Engineering and Informatics*, 10(1), 160–170.
- [17] Magfirawaty, M., Allamanda, A., Ayunasari, M., & Zulfikar, M. N. (2024). Confusion and diffusion techniques for image encryption process based on chaos system. *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, 13(2), 93–100.
- [18] Naik, R. B., & Singh, U. (2024). A review on applications of chaotic maps in pseudo-random number generators and encryption. *Annals of Data Science*, 11(1), 25–50.
- [19] Naskar, P. K., Paul, S., Nandy, D., & Chaudhuri, A. (2019). DNA encoding and channel shuffling for secured encryption of audio data. *Multimedia Tools and Applications*, 78(17), 25019–25042.
- [20] Natiq, H., Said, M. R. M., Al-Saidi, N. M. G., & Kilicman, A. (2019). Dynamics and complexity of a new 4D chaotic laser system. *Entropy*, 21(1), 34.
- [21] Patel, S., & Muthu, R. K. (2020). Image encryption decryption using chaotic logistic mapping and DNA encoding. *arXiv*. <https://arxiv.org/abs/2003.06616>
- [22] Pham, D. T., Ghanbarzadeh, A., Koç, E., Otri, S., Rahim, S., & Zaidi, M. (2006). The bees algorithm—A novel tool for complex optimization problems. In *Intelligent production machines and systems* (pp. 454–459). Elsevier.
- [23] Roy, M., Chakraborty, S., & Mali, K. (2021). The MSK: A simple and robust image encryption method. *Multimedia Tools and Applications*, 80(14), 21261–21291.
- [24] Roy, M., Chakraborty, S., Mali, K., Roy, D., & Chatterjee, S. (2021). A robust image encryption framework based on DNA computing and chaotic environment. *Microsystem Technologies*, 27(10), 3617–3627.
- [25] Shah, D., Shah, T., Hazzazi, M. M., Haider, M. I., Aljaedi, A., & Hussain, I. (2021). An efficient audio encryption scheme based on finite fields. *IEEE Access*, 9, 144385–144394.
- [26] Wang, X., & Su, Y. (2019). An audio encryption algorithm based on DNA coding and chaotic system. *IEEE Access*, 8, 9260–9270.
- [27] Zghair, H. K., Mehdi, S. A., & Sadkhan, S. B. (2021). Speech scrambler based on discrete cosine transform and novel seven-dimension hyper chaotic system. In *Journal of Physics: Conference Series* (p. 012048). IOP Publishing.