KSÜ Mühendislik Bilimleri Dergisi, 27(2), 2024
Araştırma Makalesi

KSU J Eng Sci, 27(2), 2024
Research Article

Kahramanmaras Sutcu Imam University
Journal of Engineering Sciences

Geliş Tarihi : 31.12.2023
Kabul Tarihi :04.03.2024

Received Date : 31.12.2023
Accepted Date : 04.03.2024

A BIT-LEVEL AUDIO ENCRYPTION ALGORITHM USING A NEW HYBRID CHAOTIC MAP

YENİ BiR HİBRİT KAOTİK HARİTA İLE BİT-SEVİYESİ SES ŞİFRELEME ALGORİTMASI

Mehmet DEMİRTAŞ[1] (ORCID: 0000-0002-9018-3124)

[1] Necmettin Erbakan Üniversitesi, Elektrik ve Elektronik Mühendisliği Bölümü, Konya, Türkiye

*Sorumlu Yazar / Corresponding Author: Mehmet DEMİRTAŞ, mdemirtas@erbakan.edu.tr

ABSTRACT

Audio data is increasingly transmitted worldwide, necessitating robust encryption techniques to safeguard it from malicious actors. To secure transmitted audio files, a novel, and effective audio encryption method is introduced using a newly designed 1D chaotic map and bit-level operations in this work. The Sine-Chebyshev Hybrid Map (SCHM) is a new chaotic map with high randomness, created using two classical maps, such as the Sine map and the Chebyshev map. Two-dimensional (2D) and three-dimensional (3D) phase trajectories, bifurcation diagrams, initial condition sensitivity, Lyapunov exponent, and approximate entropy results of the proposed map are given. The analysis results show that SCHM has better chaotic properties and a wider chaotic range than the sine and Chebyshev maps. The algorithm implemented with SCHM, bit-level permutation, and diffusion operations can encrypt mono-channel or stereo-channel audio files losslessly. Various security analyses are performed to test the degree of security of the proposed audio encryption algorithm. The performance tests conducted on four different audio data verify that the proposed scheme is secure and can be used to encrypt one-channel or two-channel audio files.

Keywords: audio files, chaotic maps, encryption, multimedia security

ÖZET

Ses verilerinin dünya çapında giderek daha fazla iletilmesi, kötü niyetli aktörlerden korunmak için güçlü şifreleme tekniklerinin kullanılmasını gerektirmektedir. İletilen ses dosyalarının güvenliğini sağlamak için, bu çalışmada yeni bir 1B kaotik harita ile bit düzeyinde işlemler kullanılarak yenilikçi ve etkili bir ses şifreleme yöntemi önerilmiştir. Tasarlanan Sine-Chebyshev Hibrit Haritası (SCHM), sinüs haritası ve Chebyshev haritası gibi iki klasik harita kullanılarak oluşturulan, yüksek rastgeleliğe sahip yeni bir kaotik haritadır. Önerilen harita için 2B ve 3B faz yörüngeleri, çatallanma diyagramları, başlangıç durumu duyarlılığı, Lyapunov üssü ve yaklaşık entropi sonuçları verilmiştir. Analiz sonuçları, SCHM'nin sinüs ve Chebyshev haritalarına kıyasla daha geniş bir kaotik aralığa ve daha iyi kaotik özelliklere sahip olduğunu göstermektedir. SCHM ve bit düzeyinde permütasyon ve difüzyon işlemleriyle uygulanan algoritma, tek kanallı veya stereo kanallı ses dosyalarını kayıpsız bir şekilde şifreleyebilir. Önerilen ses şifreleme algoritmasının güvenlik derecesini test etmek için çeşitli güvenlik analizleri yapılmıştır. Dört farklı ses dosyası üzerinde yapılan performans testleri, önerilen şemanın güvenli olduğunu ve tek kanallı veya iki kanallı ses dosyalarını şifrelemek için kullanılabileceğini doğrulamıştır.

Anahtar Kelimeler: kaotik haritalar, multimedia güvenliği, ses dosyaları, şifreleme

ToCite: DEMİRTAŞ, M., (2024). A BIT-LEVEL AUDIO ENCRYPTION ALGORITHM USING A NEW HYBRID CHAOTIC MAP. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi*, 27(2), 601-614.

INTRODUCTION

The widespread sharing of audio files on social networks in the digital world necessitates security precautions to protect against privacy breaches and malicious actors. Similar to multimedia data such as images, texts, and videos, audio files can also be effectively protected with encryption (Hosny, Zaki, Lashin, Fouda, and Hamza, 2023). Audio encryption algorithms can protect audio information from unauthorized access by transforming its content into an incomprehensible data form. Since classical symmetric cryptographic algorithms like Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are unable to encrypt multimedia data efficiently, chaotic functions can be employed to provide security to the audio data (Kafetzis, Volos, Nistazakis, Goudos, and Bardis, 2023). Chaotic functions are suitable for encryption algorithms due to their nonlinear properties and initial condition sensitivity (Muthu and Murali, 2021). Therefore, there is a growing interest in chaos-based audio encryption techniques. Additionally, there are audio encryption algorithms that employ the cosine number transform (Lima and da Silva Neto, 2016), discrete wavelet transform (DWT) (Al-kateeb and Mohammed, 2020), Elliptic-Curve Cryptography (ECC) (Sasikaladevi, Geetha, and Venkata Srinivas, 2018), and Collatz conjecture (Renza, Mendoza, and Ballesteros L, 2019) in the literature.

Spatial domain image encryption methods, which typically involve permuting and diffusing pixels, directly manipulate pixels without transforming them (M. Demirtaş, 2022; Mehmet Demirtaş, 2023b). Similarly, permutation and diffusion operations can be applied to audio samples in audio files. In (Hato and Shihab, 2015), for example, the Lorenz and Rossler chaotic systems are used to produce number sequences for permutation and diffusion processes. In this work, histogram and information entropy results are missing. Liu et al. (H. Liu, Kadir, and Li, 2016) proposed a lossless audio encryption scheme that can encrypt dual-channel audio inputs. This scheme also confuses and diffuses the plaintext audio using a multi-scroll chaotic system. Differential attack analysis is not performed in this article. An audio message encryption method is proposed in (Ghasemzadeh and Esmaeili, 2017) where the confusion and diffusion parameters are generated from three chaotic functions. However, in this study, histogram graphs and key sensitivity analysis are not presented. Kordov (Kordov, 2019) proposed a novel audio encryption scheme based on bit-level permutations and substitutions using pseudo-random numbers generated by a circle map. The statistical test results of the generated binary streams are provided. In (Sathiyamurthi and Ramakrishnan, 2020), a speech encryption algorithm based on the Fast Fourier Transform (FFT) and 3D chaotic map is presented. The transformed input speech samples are permuted and diffused using the number sequences obtained by the chaotic map. The input speech samples cannot be obtained losslessly in this method. In (Wang and Su, 2020), DNA encoding and piecewise linear chaotic map (PWLCM) are employed to implement confusion and diffusion on the plaintext audio samples. This method can encrypt both mono-channel and stereo-channel audio samples. The permutation and diffusion architecture is also used in (Mokhnache, Daachi, Bekkouche, and Diffellah, 2022) for a speech encryption scheme. The logistic map and cubic map are combined to obtain an enhanced 1D chaotic map. The combined map is used to produce the necessary parameters to scramble and diffuse the input audio. Histogram analysis of the proposed method is not given. An error-free sound encryption scheme is proposed in (Raducanu, Cheroiu, and Nitu, 2022). Permutation, XOR operation, and diffusion operations are applied using an Arnold 3D map and a tent map. Key sensitivity analysis is missing in the paper. Wu et al. (Wu et al., 2022) proposed an audio encryption algorithm based on a newly designed 2D chaotic system. The 2D system generates the required keystream for the scrambling and diffusion processes. Although most of the necessary security analyses are carried out in this study, histogram analysis is missing. The audio signal encryption algorithm in (Alanazi, Munir, Khan, and Hussain, 2023) uses the 3D Gensio-Tesi chaotic map to generate substitution and permutation networks. All security analyses except key space and key sensitivity are performed. In (Albahrani, Alshekly, and Lafta, 2023), a modified Lorenz system and 1D Bernoulli map are used to confuse and diffuse the original audio data. The algorithm in this study, in which all necessary security analyses are carried out, is a lossy voice encryption algorithm. A lossless encryption algorithm for audio files is proposed in (Mehmet Demirtaş, 2023a). The input audio samples are preprocessed before permutation and diffusion operations. This method can only encrypt mono-channel audio signals. In (Kumar and Dua, 2023), the plaintext audio is first permuted using the sine-cosine map and then scrambled and diffused using DNA encoding.

Since chaotic functions are aperiodic, unpredictable, deterministic, and sensitively dependent on the initial values, they are preferred in cryptographic applications (L. Liu and Wang, 2023). One-dimensional chaotic functions, which have simple equations and ease of implementation, can be used to generate pseudorandom sequences. However, 1D chaotic maps may suffer from some drawbacks such as a narrow discontinuous chaotic range, discontinuities, and non-uniform output sequences (Khairullah, Alkahtani, Bin Baharuddin, and Al-Jubari, 2021). For example, the

classical sine map has a limited chaotic range and there are periodic windows in the chaotic regime. These problems can be overcome by either creating new chaotic maps or combining the existing chaotic maps.

The first contribution of this study is the design of a new 1D hybrid chaotic map using the sine map and Chebyshev map. The proposed map has a simple equation with cost-effective implementation. Moreover, the problem of narrow chaotic intervals and discontinuities in the sine and Chebyshev maps has also been solved with the proposed map. The chaotic complexity and randomness of the designed map are proven by several graphs and metrics such as phase diagrams, bifurcation diagrams, Approximate entropy results, and Lyapunov exponent measurements. Secondly, the proposed method can encrypt both single-channel and stereo-channel input audio, which demonstrates the flexibility of the algorithm. Moreover, this algorithm is capable of encrypting and decrypting audio data without losing any information. Therefore, the quality of the transmitted audio data can be preserved with the proposed technique. To assess the reliability of the algorithm tests such as key analysis, information entropy, correlation analysis, histogram analysis, and differential attack analysis were carried out. The security tests performed show us that the proposed audio encryption method is safe and applicable.

The outline of the rest of the paper is given as follows. In Section 2, the newly created Sine-Chebyshev Hybrid Map (SCHM) is introduced and analyzed. SCHM-based bit-level audio encryption algorithm is described in Section 3. The security analysis results of the proposed algorithm are given in Section 4. In Section 5, the work is concluded.

MATERIALS AND METHODS

Description of Sine-Chebyshev Hybrid Map (SCHM)

The traditional sine map is defined by Eq. (1).

$$x_{n+1} = \rho \sin(\pi x_n) \tag{1}$$

when the control parameter $\rho \in [0.87, 1]$, the sine map exhibits chaotic behavior. Similarly, the Chebyshev map is mathematically expressed as in Eq. (2).

$$x_{n+1} = \cos(\gamma \cos^{-1}(x_n)) \tag{2}$$

when the control parameter $\gamma > 2$, the Chebyshev map is chaotic. A new 1D chaotic map called SCHM is created by combining Eq. (1) with Eq. (2) and adding exponential terms. The definition of the SCHM is given in Eq. (3).

$$x_{n+1} = \sin(\pi 10^{\alpha} \cos(\pi^{\alpha+10} \cos^{-1}(x_n))) \tag{3}$$

where α is the control parameter and $x_n \in [-1, 1]$. When $\alpha \in [0, +\infty)$, SCHM shows chaotic behavior without non-chaotic regions.

Phase Diagrams

The attractor of a chaotic map can be depicted by plotting the 2D and 3D phase diagrams. The phase diagrams can be obtained by plotting two or three adjacent time series data generated by the chaotic map. The 2D and 3D phase diagrams for the sine map, Chebyshev map, and SCHM are illustrated in Fig. 1 and Fig. 2 for an initial condition $x_0 = 0.25$, respectively. 50,000 time series data were used to draw these graphs. The phase diagrams of the sine map and Chebyshev map show that a specific path is traced by both maps and a quite limited region in the 2D and 3D phases are visited. On the other hand, SCHM's time series data are distributed all over the graphs. SCHM shows better ergodicity compared to its classical counterparts because its time series data will eventually visit most of the phase spaces.

Bifurcation Diagrams

The bifurcation diagram of a chaotic function visualizes the long-term behavior of the map versus the control parameter. With the bifurcation diagram, it can be observed for which values of the control parameter the chaotic state is entered. The bifurcation diagrams for the sine map, Chebyshev map, and SCHM are shown in Fig. 3. In the bifurcation diagram of the sine map, stable fixed points and period doublings can be seen. When the control parameter is less than one, there is a chaotic region only for values greater than or equal to 0.87. If the control parameter is greater than one, non-chaotic regions are also visible. Similarly, the Chebyshev maps enter the chaotic regime when

the control parameter is larger than or equal to two. It has a single fixed point if the control parameter is less than or equal to one. On the other hand, SCHM can produce chaotic values between -1 and 1 for all cases where the control parameter is equal to or greater than zero. The chaotic features and chaotic intervals of both the Chebyshev and the sine map are increased with SCHM.

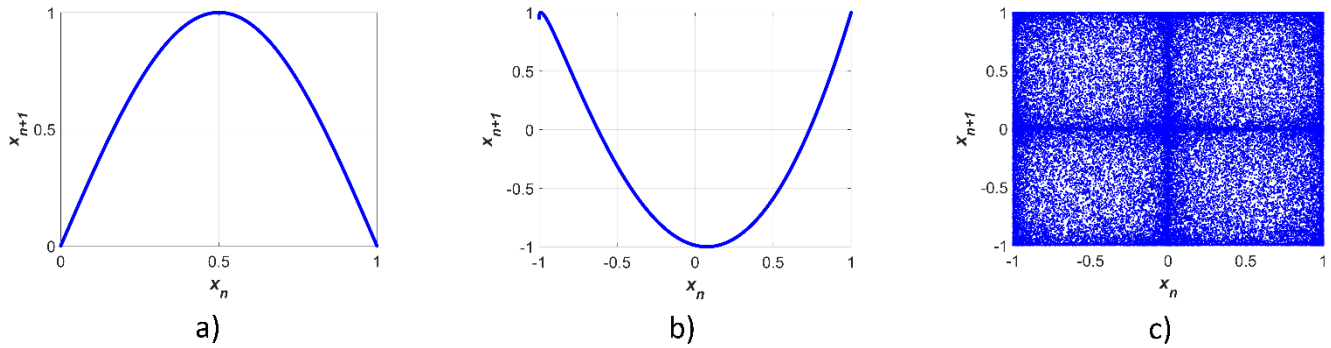

Figure 1. 2D Phase Diagrams. **a**. Sine Map **b**. Chebyshev Map **c**. SCHM ($x_0 = 0.25$)

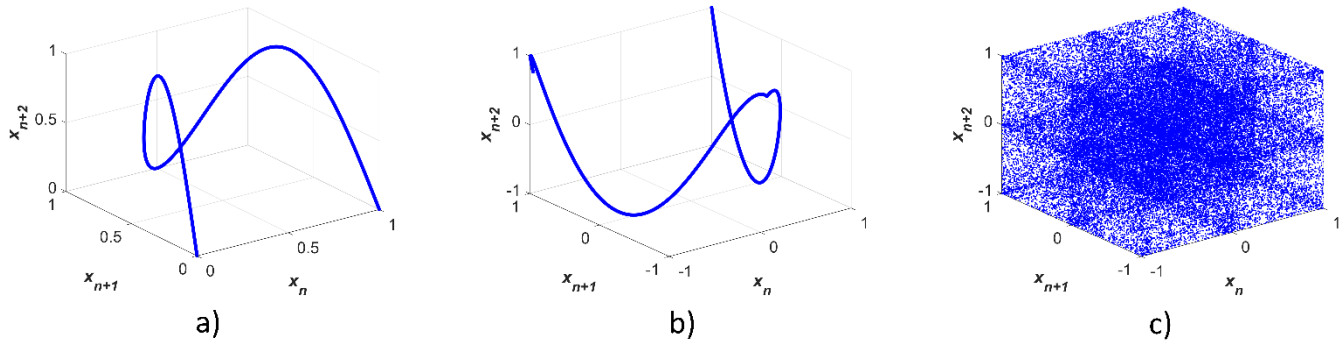

Figure 2. 3D Phase Diagrams. **a**. Sine Map **b**. Chebyshev Map **c**. SCHM ($x_0 = 0.25$)

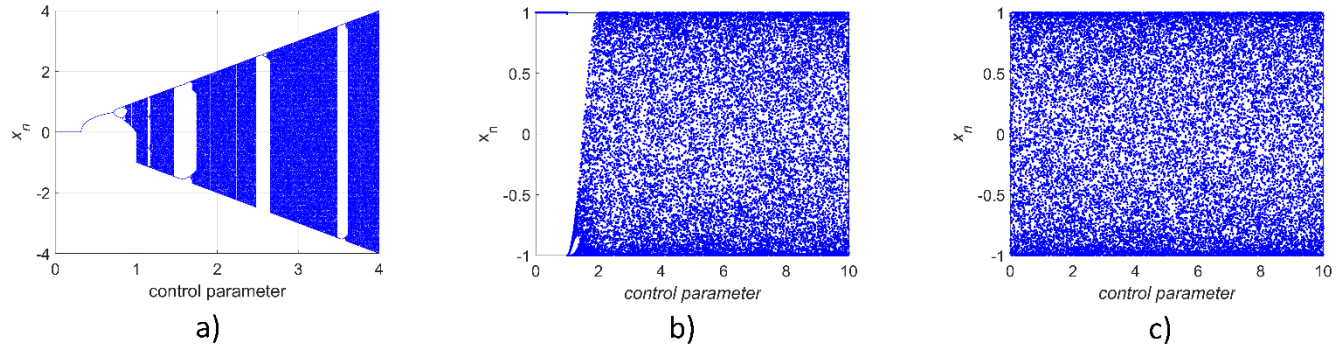

Figure 3. Bifurcation Diagrams. **a**. Sine Map **b**. Chebyshev Map **c**. SCHM

Initial Condition Sensitivity of SCHM

Chaotic maps exhibit extreme sensitivity to initial conditions, implying that even a tiny change in the initial values can yield significantly different outcomes. The initial condition sensitivity of chaotic maps is one of the key properties of chaotic maps and makes them unpredictable, making chaotic maps a good choice for cryptography applications. To measure the initial condition sensitivity of SCHM, the results of 40 iterations for two initial conditions with 10^{-16} differences are shown in Fig. 4. The proposed chaotic map can generate very different output values even if the initial values are changed very slightly.

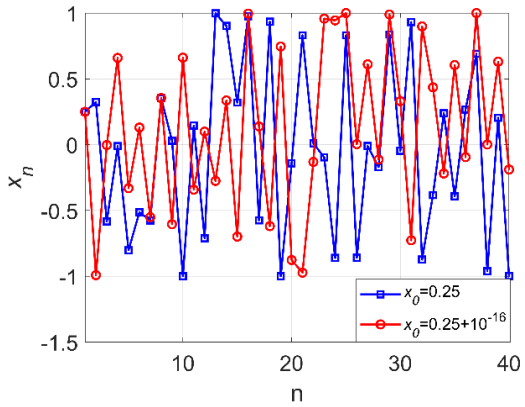

Figure 4. Initial Condition Sensitivity of SCHM

Comparison of Lyapunov Exponents

Lyapunov exponent (LE) measures the rate of the separation of two trajectories that have very close initial conditions. Chaotic behavior and sensitivity to the initial conditions can be indicated by a positive value of the Lyapunov exponent. LE of a chaotic map $f(x_i)$ can be calculated using Eq. (4).

$$LE = \lim_{K\to\infty} \frac{1}{K} \sum_{n=0}^{K} ln|f'(x_n)| \quad (4)$$

In Fig. 5, the plots of LEs of the sine map, Chebyshev map, and SCHM are illustrated. The LE values of SCHM are always positive and are greater than the LE values of the Chebyshev map and sine map. Since a higher LE value indicates more chaotic behavior, SCHM has better chaotic properties than the sine map and Chebyshev map.

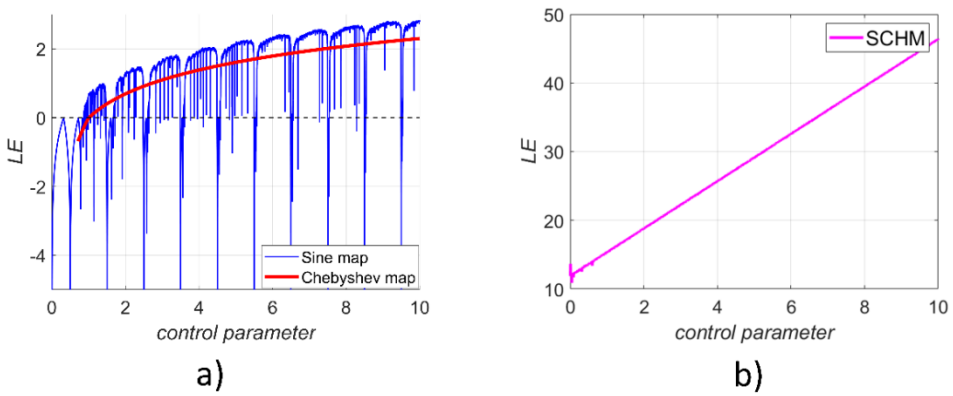

Figure 5. Comparison of Lyapunov Exponents. **a**. Sine Map and Chebyshev Map **b**. SCHM

Comparison of Approximate Entropies

Approximate entropy (ApEn) is a measure of the level of regularity in time-series data (Delgado-Bonal and Marshak, 2019). A higher ApEn value implies greater unpredictability in time-series data. The sine map, Chebyshev map, and SCHM are iterated 1000 times to calculate ApEn values. In Fig. 6, ApEn values are plotted against the control parameter. SCHM is less repetitive and predictive compared to the sine map and Chebyshev map.

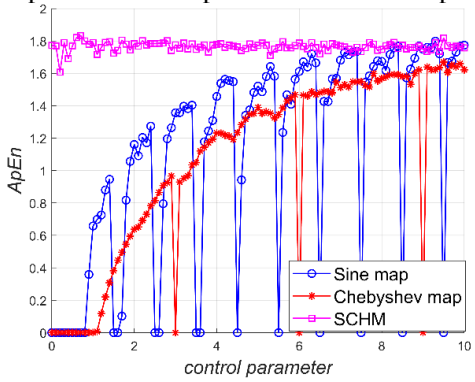

Figure 6. Comparison of Approximate Entropies

THE PROPOSED AUDIO ENCRYPTION METHOD

The proposed audio encryption algorithm is based on bit-level operations using the sequences generated by SCHM. The encryption process of the proposed algorithm is shown in Fig. 7. In general, the encryption process consists of four main steps: conversion to bit-level, permutation, diffusion, and post-processing. Two secret keys k and Key are exchanged with the receiver in a secure channel before the transmission of the audio file. Assume that the input audio A is of length N. The first secret key k is obtained from the plaintext audio file using Eq. (5).

$$k = \begin{cases} \mathrm{mod}\left(\sum_{i=1}^{N} A_i, 1\right) \text{ if } \sum_{i=1}^{N} A_i \geq 0 \\ 1 - \mathrm{mod}\left(\sum_{i=1}^{N} A_i, 1\right) \text{ if } \sum_{i=1}^{N} A_i < 0 \end{cases} \tag{5}$$

where $A = \{A_1, A_2, \ldots, A_N\}$ and $A_i \in [-1,1]$ represents the value of the ith sample. On the other hand, Key is an external key of 400 bits length. Key is then divided into four equal parts $\{K_1, K_2, K_3, K_4\}$, each 100-bit long. The procedure of the proposed audio encryption scheme is described in the following steps.

Step 1. Firstly, the samples of the plaintext audio are mapped to the range $[0, 255]$. Additionally, integer and decimal parts of the transformed samples are obtained separately using Eqs. (6)-(8).

$$A_T = \frac{(A \times 255) + 255}{2} \tag{6}$$

$$A_{int} = \mathrm{floor}(A_T) \tag{7}$$

$$A_d = A_T - A_{int} \tag{8}$$

where A_T represents the transformed audio samples. A_{int} and A_d are the integer and decimal parts of A_T, respectively. Subsequently, A_{int} is converted to a binary A_{bit} matrix of size $8 \times N$. The 8-bit equivalents of each integer in A_{int} are found and placed in the columns of A_{bit}.

Step 2. SCHM is iterated $N + 500$ times and the last N elements are stored in a chaotic array called P. The control parameter a and x_0 are selected using Eq. (9) and Eq. (10).

$$a = \frac{\mathrm{sum}(K1)}{\mathrm{sum}(K)} + 3k \tag{9}$$

$$x_0 = 1 - k - \frac{\mathrm{sum}(K2)}{\mathrm{sum}(K)} \tag{10}$$

where the $\mathrm{sum}(\cdot)$ function finds the total number of non-zero elements in its input.

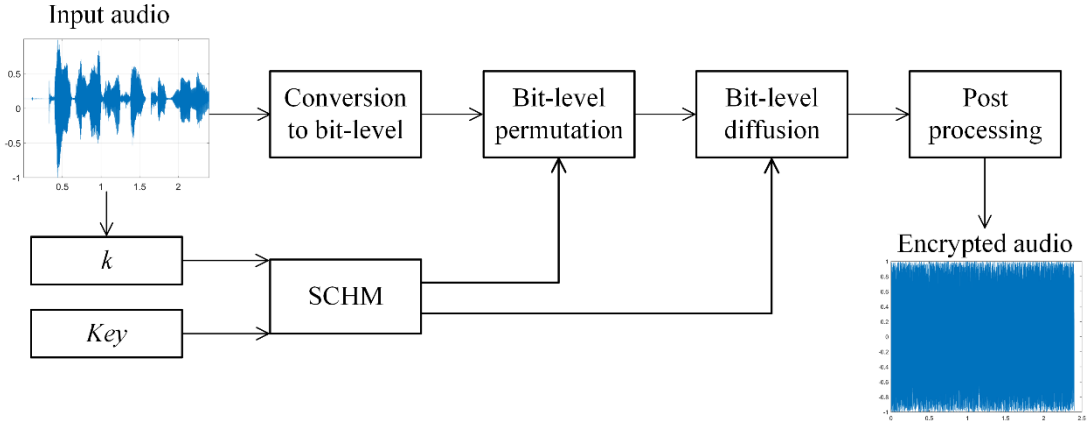

Figure 7. The Proposed Audio Encryption Process

Step 3. The bit-level permutation is performed on A_{bit} using the permutation array P. Each column of A_{bit} is shifted upwards or downwards according to the value of P using the definitions in Eq. (11).

$$A_{per} = \begin{cases} shift(A_{bit}(:,i),3), & P(i) < 0 \\ shift(A_{bit}(:,i),-3), & P(i) \geq 0 \end{cases} (i = 1,2,\dots,N) \quad (11)$$

where $shift(\cdot)$ circularly shifts ith column of A_{bit} 3 positions upwards if $P(i)$ is positive, and 3 positions downwards if it is negative. A_{per} is the bit matrix obtained as a result of the permutation process.

Step 4. To obtain the diffusion sequence, SCHM is iterated again $N + 500$ times and the last N elements are stored in an array called D_0. The control parameter a and the initial value x_0 are chosen as in Eqs. (12)-(13).

$$a = \frac{\text{sum}(K3)}{\text{sum}(K)} + 5k \quad (12)$$

$$x_0 = -1 + k - \frac{\text{sum}(K4)}{\text{sum}(K)} \quad (13)$$

The diffusion array $D \in [0,255]$ is obtained from the chaotic sequence D_0 using Eq. (14).

$$D = \text{mod}(\lfloor |D_0(i)| \times 10^{10} \rfloor, 256) \quad (i = 1,2,\dots,N) \quad (14)$$

D is converted to a binary D_{bit} matrix of size $8 \times N$ by finding the 8-bit equivalent of each integer. D_{bit} is the bit-level diffusion matrix that is used in the following step.

Step 5. A bit-wise diffusion operation is implemented between A_{per} and D_{bit} using an XOR operator.

$$E_{bit} = A_{per} \oplus D_{bit} \quad (15)$$

where E_{bit} represents the bit-wise encrypted samples. In addition, E_{bit} is converted from binary to decimal to obtain an integer sequence $E_0 \in [0,255]$.

Step 6. In the post-processing step, the permuted and diffused audio samples are mapped back to the range $[-1,1]$ as in Eqs. (16)-(17).

$$E_1 = E_0 + A_d \quad (16)$$

$$E = \frac{E_1}{128} - 1 \quad (17)$$

Table 1. Tested Audio Files

File Name	Content	Compression Method	Number of Channels	Sampling Rate (Hz)	Duration (s)	Total Samples
Audio 1	Female Speech	Uncompressed	1	8,000	3	24,000
Audio 2	Jet Airplane	Uncompressed	1	11,025	16.35	180,224
Audio 3	Engine	Uncompressed	2	44,100	20.02	882,688
Audio 4	Rock Drums	MP3	2	48,000	11.47	550,656

where $E \in [-1,1]$ denotes the encrypted audio file. In Eq. (16), decimal parts of the transformed input audio file are added to the encrypted samples so that a lossless audio encryption scheme has been achieved. Moreover, a stereo-channel plaintext audio file can be encrypted losslessly using this algorithm by encrypting each channel separately with the proposed algorithm. The decryption algorithm can be performed by taking the secret keys and the encrypted audio file as inputs and following the encryption steps in reverse order. Therefore, the decrypted audio file will be identical to the plaintext audio file as the proposed algorithm is a lossless method.

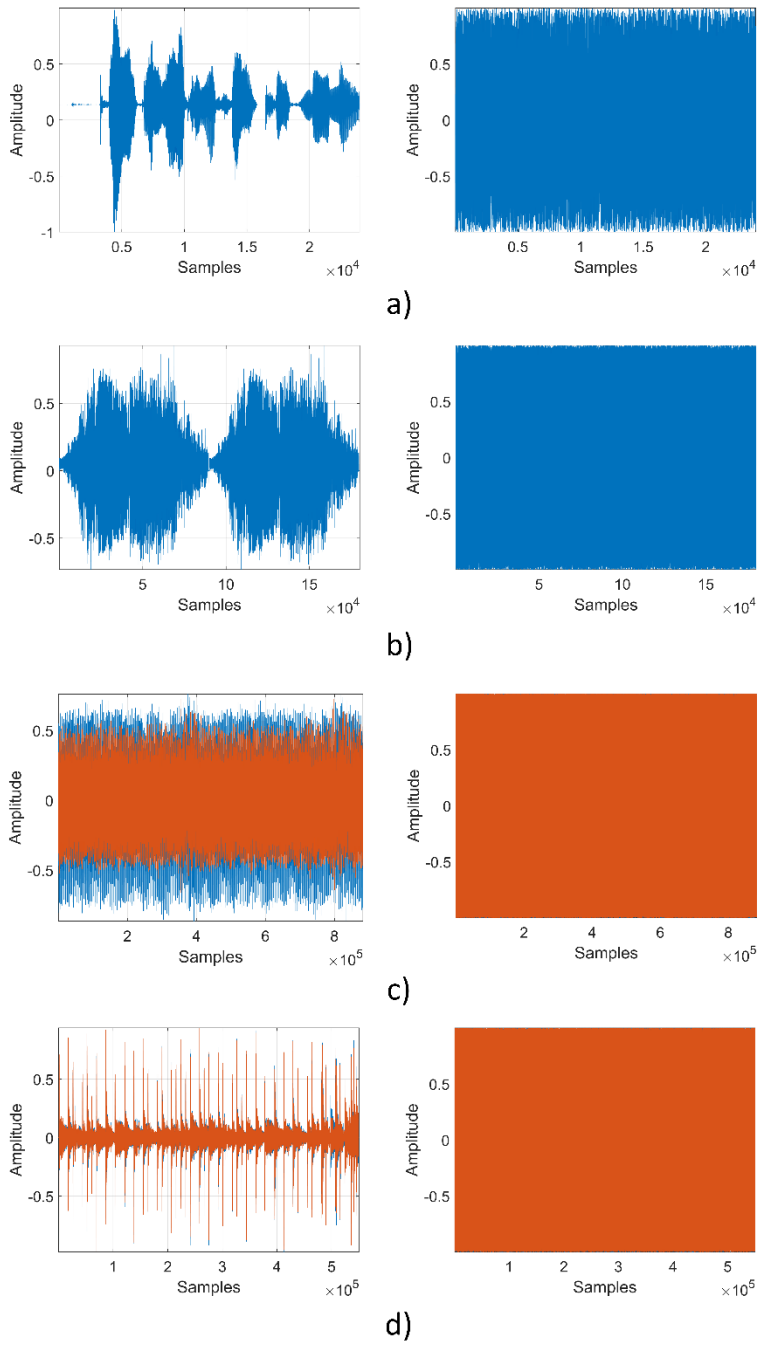

Figure 8. Waveforms of the Test Audios and Encrypted Audios. **a.** Audio 1 **b.** Audio 2 **c.** Audio 3 **d.** Audio 4

SECURITY ANALYSIS RESULTS

Four audio files taken from MATLAB's Audio Toolbox, detailed in Table 1, were tested. Test audio files are sampled with different sampling rates and have different numbers of channels. Thus, the algorithm's performance in encrypting audio files with different features was observed. The waveforms of the test images and their corresponding encrypted versions are illustrated in Fig. 8. When the proposed method is used to encrypt single-channel or two-channel audio files, the sample values of the resulting encrypted audio data are evenly distributed as shown in the figure. It is not possible to obtain meaningful information from encrypted files, which proves the strength of the proposed algorithm.

Histogram Analysis

A histogram plot of audio data is the representation of the distribution of the signal amplitudes. It's a visual depiction that illustrates the occurrence frequency of various amplitudes within the audio signal. The histogram graph's horizontal axis depicts the amplitude values, while the vertical axis illustrates the quantity of samples within each bin. In Fig. 9, histogram graphs of the test audio files are presented. Whether it is a single-channel or two-channel

audio file, a uniform histogram graph can be obtained as a result of the proposed algorithm. Therefore, it is not possible to extract statistical information from audio files encrypted with this method.

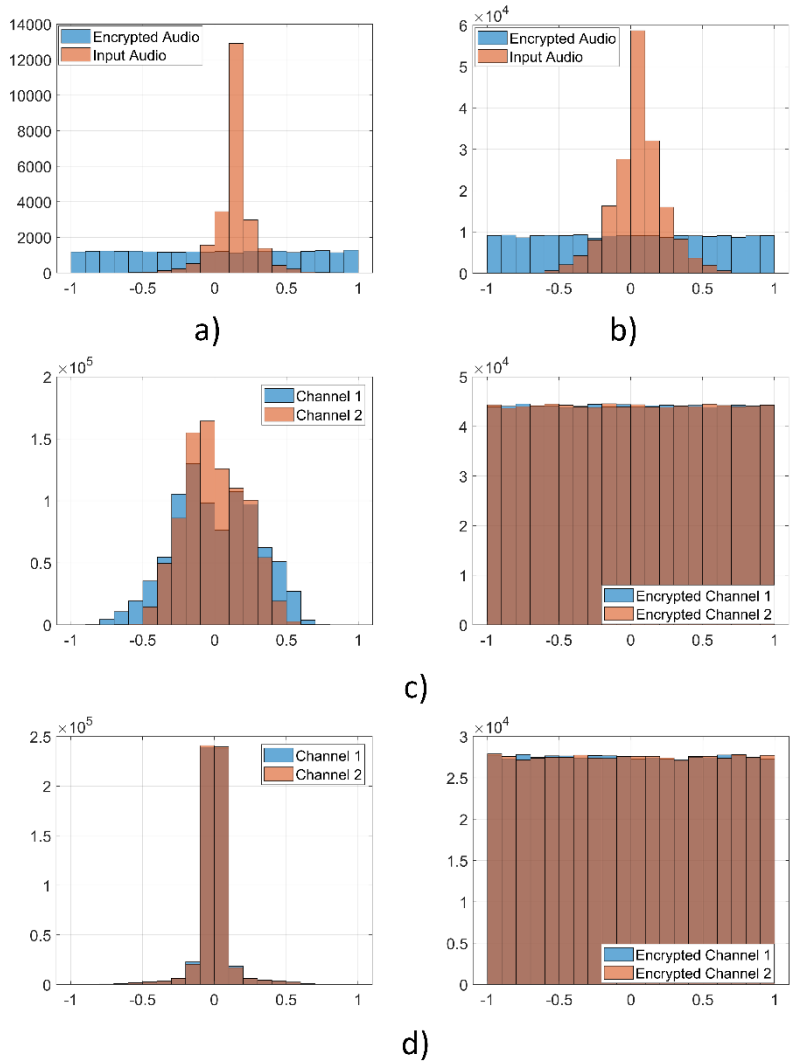

Figure 9. Histogram Plots. **a.** Audio 1 **b.** Audio 2 **c.** Audio 3 **d.** Audio 4

Table 2. Comparison of Keyspaces

Proposed Method	(Mokhnache et al., 2022)	(Wu et al., 2022)	(Albahrani et al., 2023)	(Mehmet Demirtaş, 2023a)	(Kumar and Dua, 2023)	(Wang and Su, 2020)
$\mathbf{2^{453}}$	2^{180}	2^{256}	2^{240}	2^{159}	2^{128}	2^{128}

Keyspace Analysis

In the proposed algorithm, there are two secret keys k and Key. While the first secret key depends on the sample values of the input audio file, the second secret key is chosen as a 400-bit external key. The precision of the first key is found to be 10^{-16}. The keyspace of these two secret keys can be calculated as follows: $2^{400} \times 10^{16} \cong 2^{453}$. Exhaustive search attacks, which adopt the trial-and-error approach, try every possible secret key. Therefore, the key space must be larger than 2^{100} so that an exhaustive search attack can be made infeasible. The proposed method is impossible to break using brute-force attacks due to the high keyspace. In Table 2, keyspace comparison with various algorithms is listed. The proposed method has a larger keyspace than various encryption schemes.

Key Sensitivity Analysis

Key sensitivity analysis is a visual assessment of how sensitive the encryption scheme is to small changes in the secret keys during the decryption process. For Audio 1, the key sensitivity analysis results are shown in Fig. 10. When the correct secret keys are used, the input audio file can be obtained losslessly and accurately. However, if only the secret key k is changed by 10^{-16}, the decrypted audio data is completely unrelated to the original audio file.

Similarly, when only the first or last bit of Key is flipped, the decrypted audio data is completely different from the input audio file. This visualization proves that the proposed algorithm exhibits a high level of sensitivity to the secret keys and displays a strong response to variations in the keys.

Spectrogram Analysis

A spectrogram graph serves as a visual representation of the spectrum of frequencies of an audio file. The time-series audio input samples are transformed into frequency content using the Short-Time Fourier Transform. A uniform distribution in the spectrogram graph is an indicator of efficient encryption. In Fig. 11, the spectrogram graphs of the plaintext and encrypted signals are illustrated for Audio 1 and Audio 2 test files. As can be seen from Fig. 11, the audio files that are encrypted with the proposed method have evenly distributed frequency components.

Correlation Analysis

The consecutive samples in the plaintext audio file are expected to exhibit a strong correlation. Therefore, this strong correlation between successive samples should be reduced by an audio encryption algorithm. Reducing the correlation between audio samples is necessary to resist statistical attacks. The correlation between randomly selected two audio samples can be quantified by the correlation coefficient as defined in Eq. 18.

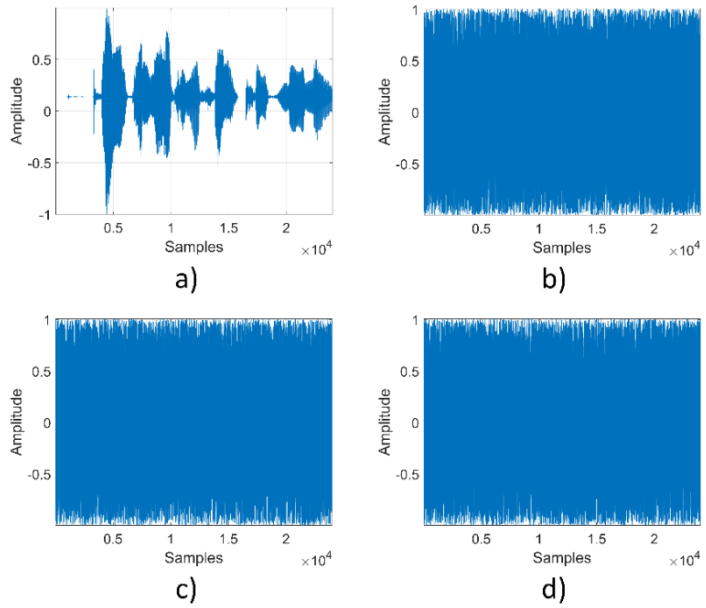

Figure 10. Key sensitivity results. **a.** Correct keys **b.** $k + 10^{-16}$ **c.** Key's first bit toggled **d.** Key's last bit toggled

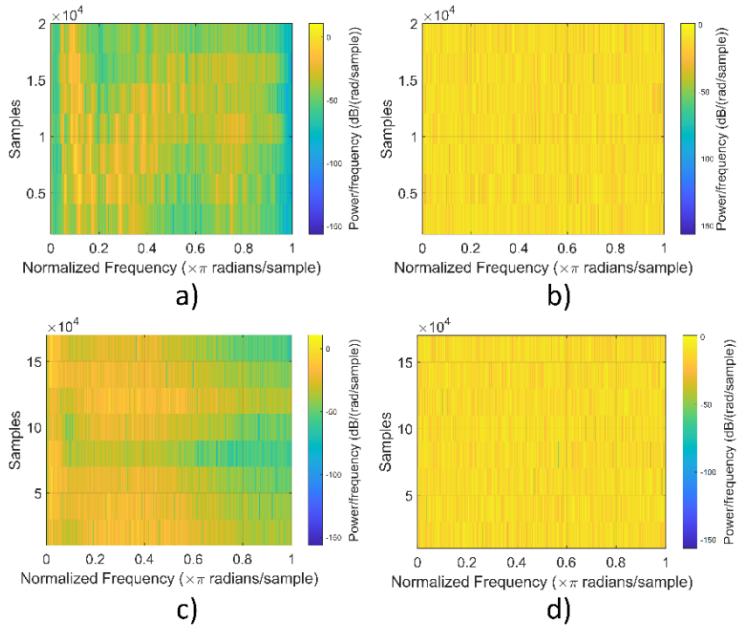

Figure 11. Spectrogram Graphs. **a.** Input Audio 1 **b.** Encrypted audio 1 **c.** Input Audio 2 **d.** Encrypted audio 2

$$c = \frac{\sum_{i=1}^{L}\left(x_i - E(x)\right)\left(y_i - E(y)\right)}{\sqrt{\sum_{i=1}^{L}\left(x - E(x)\right)^2 \sum_{i=1}^{L}\left(y_i - E(y)\right)^2}} \tag{18}$$

where (x_i, y_i) are the amplitude values of the randomly selected audio sample pairs and L is the number of those pairs. $E(x)$ and $E(y)$ are the average values of the audio samples. The calculated correlation coefficient values are listed in Table 3 for the test audio files. Although the correlation coefficient values between randomly selected sample pairs of the input audio files are very high, these values approached zero using the proposed encryption algorithm. Therefore, the proposed audio encryption algorithm can withstand statistical attacks. Furthermore, the correlation between adjacent audio samples can be visualized using correlation graphs. In Fig 12, the correlation graphs representing the distribution of 5,000 randomly selected audio sample pairs are displayed for the test images. In the figure, the left column depicts the distribution of adjacent samples of the input audio signals, while the right column illustrates the distribution of adjacent samples of the encrypted audio signals. In the input audio files, there is a strong correlation between adjacent samples. However, the adjacent samples are distributed widely across the plane in the encrypted audio files, indicating the absence of correlation between them.

Information Entropy Analysis

Information entropy values can be used to quantify the level of randomness of audio signals. An information entropy value closer to 8 means that the relevant signal is more complex and unpredictable (Albahrani et al., 2023). Therefore, an audio encryption algorithm should increase the information entropy closer to 8. Information entropy values of the test audio signals are presented in Table 4. Encrypted audio files have almost ideal information entropy values, which are at least 7.99.

Table 3. Correlation Coefficient Values

	Audio 1	Audio 2	Audio 3 Channel 1	Audio 3 Channel 2	Audio 4 Channel 1	Audio 4 Channel 2
Plaintext	0.7879	0.6213	0.9993	0.9982	0.9873	0.9870
Encrypted	-0.0153	-0.0043	0.0020	-0.0015	0.0011	0.0027

Table 4. Information Entropies

	Audio 1	Audio 2	Audio 3 Channel 1	Audio 3 Channel 2	Audio 4 Channel 1	Audio 4 Channel 2
Plaintext	5.760	4.570	4.434	4.162	3.474	3.458
Encrypted	7.990	7.997	7.998	7.998	7.998	7.998

Differential Analysis

An effective audio encryption method must be capable of dispersing the impact of one sample of the input audio file over a large portion of the encrypted audio file. Therefore, when one sample of the input audio undergoes a minor alteration, the encrypted audio file should be completely different. The number of sample change rate (NSCR) can be used to quantify the difference between two encrypted audio files and it is defined as follows.

$$NSCR = \frac{1}{N}\sum_{i=1}^{N} D(i) \tag{19}$$

$$D(i) = \begin{cases} 1 \text{ if } E_1(i) \neq E_2(i) \\ 0 \text{ if } E_1(i) = E_2(i) \end{cases} \tag{20}$$

where N is the total number of samples and E_1 and E_2 represent audio signals that share the same original input audio source, with only a minor difference in one of their samples. NSCR values were calculated by changing the amplitude value of a randomly selected sample from the input audio files by 5%. For each test audio file, the average of the

Table 5. Average NSCR Values

	Audio 1	Audio 2	Audio 3 Channel 1	Audio 3 Channel 2	Audio 4 Channel 1	Audio 4 Channel 2
NSCR (%)	99.608	99.613	99.603	99.604	99.612	99.607

Table 6. Time Spent for Encryption and Decryption

	Audio 1	Audio 2	Audio 3	Audio 4
Duration (s)	3	16.35	20.02	11.47
Number of Channels	1	1	2	2
Encryption (s)	0.165	0.686	5.461	3.395
Decryption (s)	0.053	0.395	3.525	2.075

NSCR values found for 10 different samples are shown in Table 5. As can be seen from the table, a 5% change of just one sample in the input audio file changes more than 99.6% of the output samples. These results demonstrate the robustness of the proposed audio signal encryption method against differential attacks.

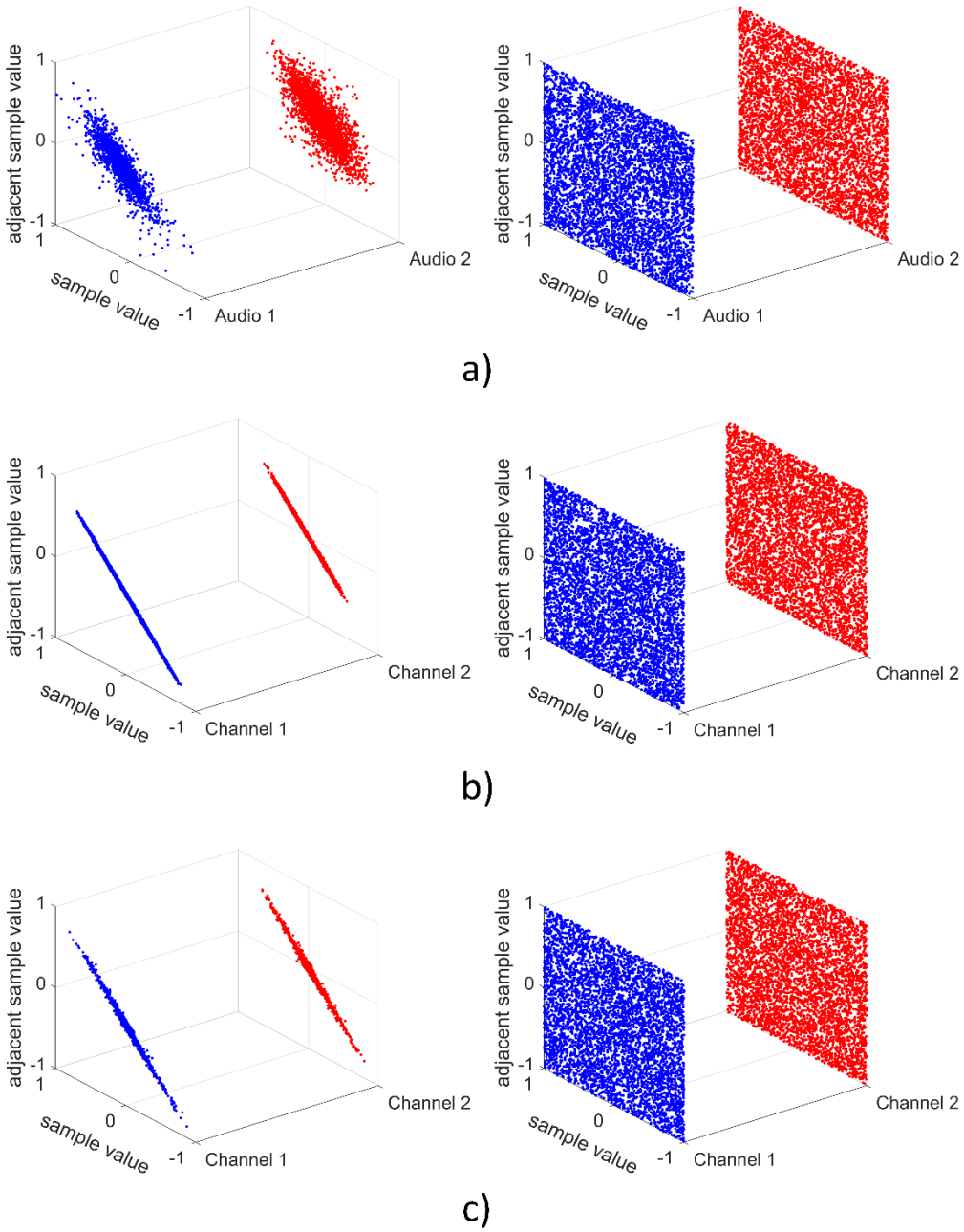

Figure 12. Correlation Graphs. **a.** Audio 1 and Audio 2 **b.** Audio 3 **c.** Audio 4

Running Time Analysis

The proposed algorithm is simulated using MATLAB 2020a software that was implemented on a PC equipped with an Intel Core i7 processor running at 2.80 GHz and 16 GB of RAM. Times spent on encryption and decryption

processes are listed in Table 6. The encryption and decryption durations vary depending on the duration of the input audio file and the number of channels. Two-channel audio files require more time to encrypt or decrypt as expected.

CONCLUSIONS

The need for encryption of audio files is increasing since they contain confidential and personal data. In this study, a novel and lossless audio encryption algorithm is presented to address this need. A newly developed chaotic map called SCHM, and bit-level operations are applied to encrypt different audio files with varying sizes and channels. It is proved using several analyses that SCHM exhibits better chaotic properties with a broader chaotic range compared to the sine and Chebyshev maps. To test the security of the proposed algorithm, the following analyses were conducted: histogram analysis, keyspace and key sensitivity analysis, spectrogram analysis, correlation coefficient and information entropy calculations, differential attack analysis, and running time measurements. The proposed method can withstand statistical attacks since it breaks the correlation between successive samples of the input audio file. Also, the encrypted audio samples exhibit a uniform distribution which is an indicator of resistance to statistical attacks. The uniform distribution of the output frequencies is also shown using the spectrogram graphs. Information entropy results are very close to the ideal value, indicating the proposed method's encryption capability. The proposed algorithm has a larger keyspace than several recently proposed encryption methods. This algorithm is also very sensitive to the secret keys and input samples, as shown by the key sensitivity analysis and differential analysis, respectively. In conclusion, the results of the security analysis affirm the effectiveness of the proposed audio encryption method.

REFERENCES

Al-kateeb, Z. N., & Mohammed, S. J. (2020). A novel approach for audio file encryption using hand geometry. *Multimedia Tools and Applications, 79*(27), 19615-19628. doi:10.1007/s11042-020-08869-8

Alanazi, A. S., Munir, N., Khan, M., & Hussain, I. (2023). A novel design of audio signals encryption with substitution permutation network based on the Genesio-Tesi chaotic system. *Multimedia Tools and Applications, 82*(17), 26577-26593. doi:10.1007/s11042-023-14964-3

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. doi:10.1007/s11227-023-05249-5

Delgado-Bonal, A., & Marshak, A. (2019). Approximate Entropy and Sample Entropy: A Comprehensive Tutorial. *Entropy, 21*(6), 541.

Demirtaş, M. (2022, 7-9 Sept. 2022). *AFast Multiple Image Encryption Algorithm Based on Hilbert Curve and Chaotic Map.* Paper presented at the 2022 Innovations in Intelligent Systems and Applications Conference (ASYU).

Demirtaş, M. (2023a, 03/28). *A Lossless Audio Encryption Method based on Chebyshev Map.* Paper presented at the Orclever Proceedings of Research and Development.

Demirtaş, M. (2023b). A NEW IMAGE ENCRYPTION METHOD BASED ON A 6D HYPERCHAOTIC MAP AND GENETIC OPERATORS. *Kahramanmaraş Sütçü İmam Üniversitesi Mühendislik Bilimleri Dergisi, 26*(1), 261-278. doi:10.17780/ksujes.1208570

Ghasemzadeh, A., & Esmaeili, E. (2017). A novel method in audio message encryption based on a mixture of chaos function. *International Journal of Speech Technology, 20*(4), 829-837. doi:10.1007/s10772-017-9452-y

Hato, E., & Shihab, D. (2015). Lorenz and Rossler Chaotic System for Speech Signal Encryption. *International Journal of Computer Applications, 128*, 25-33.

Hosny, K. M., Zaki, M. A., Lashin, N. A., Fouda, M. M., & Hamza, H. M. (2023). Multimedia Security Using Encryption: A Survey. *IEEE Access, 11*, 63027-63056. doi:10.1109/ACCESS.2023.3287858

Kafetzis, I., Volos, C., Nistazakis, H. E., Goudos, S., & Bardis, N. G. (2023, 28-30 June 2023). *A Real-time Chaos-based Audio Encryption Scheme.* Paper presented at the 2023 12th International Conference on Modern Circuits and Systems Technologies (MOCAST).

Khairullah, M. K., Alkahtani, A. A., Bin Baharuddin, M. Z., & Al-Jubari, A. M. (2021). Designing 1D Chaotic Maps for Fast Chaotic Image Encryption. *Electronics, 10*(17), 2116.

Kordov, K. (2019). A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture. *Electronics, 8*(5), 530.

Kumar, A., & Dua, M. (2023). Audio encryption using two chaotic map based dynamic diffusion and double DNA encoding. *Applied Acoustics, 203*, 109196. doi:https://doi.org/10.1016/j.apacoust.2022.109196

Lima, J. B., & da Silva Neto, E. F. (2016). Audio encryption based on the cosine number transform. *Multimedia Tools and Applications, 75*(14), 8403-8418. doi:10.1007/s11042-015-2755-6

Liu, H., Kadir, A., & Li, Y. (2016). Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys. *Optik, 127*(19), 7431-7438. doi:https://doi.org/10.1016/j.ijleo.2016.05.073

Liu, L., & Wang, J. (2023). A cluster of 1D quadratic chaotic map and its applications in image encryption. *Mathematics and Computers in Simulation, 204*, 89-114. doi:https://doi.org/10.1016/j.matcom.2022.07.030

Mokhnache, S., Daachi, M. E. H., Bekkouche, T., & Diffellah, N. (2022). A Combined Chaotic System for Speech Encryption. *Engineering, Technology & Applied Science Research, 12*(3), 8578-8583. doi:10.48084/etasr.4912

Muthu, J. S., & Murali, P. (2021). Review of Chaos Detection Techniques Performed on Chaotic Maps and Systems in Image Encryption. *SN Computer Science, 2*(5), 392. doi:10.1007/s42979-021-00778-3

Raducanu, M., Cheroiu, D. G., & Nitu, C. M. (2022, 13-15 July 2022). *Sound Encryption Algorithm with Perfect Reconstruction using Tent Map and Multidimensional Arnold Chaotic Systems.* Paper presented at the 2022 45th International Conference on Telecommunications and Signal Processing (TSP).

Renza, D., Mendoza, S., & Ballesteros L, D. M. (2019). High-uncertainty audio signal encryption based on the Collatz conjecture. *Journal of Information Security and Applications, 46*, 62-69. doi:https://doi.org/10.1016/j.jisa.2019.02.010

Sasikaladevi, N., Geetha, K., & Venkata Srinivas, K. N. (2018). A multi-tier security system (SAIL) for protecting audio signals from malicious exploits. *International Journal of Speech Technology, 21*(2), 319-332. doi:10.1007/s10772-018-9510-0

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

Wang, X., & Su, Y. (2020). An Audio Encryption Algorithm Based on DNA Coding and Chaotic System. *IEEE Access, 8*, 9260-9270. doi:10.1109/ACCESS.2019.2963329

Wu, R., Gao, S., Wang, X., Liu, S., Li, Q., Erkan, U., & Tang, X. (2022). AEA-NCS: An audio encryption algorithm based on a nested chaotic system. *Chaos, Solitons & Fractals, 165*, 112770. doi:https://doi.org/10.1016/j.chaos.2022.112770