https://doi.org/10.56038/oprd.v2i1.234

Conference Article

A Lossless Audio Encryption Method based on Chebyshev Map

Mehmet Demirtaş[1*]

[1]Necmettin Erbakan University, Konya, Turkey, Orcid ID: 0000-0002-9018-3124
*Correspondence: mdemirtas@erbakan.edu.tr

(First received January 17, 2023 and in final form March 9, 2023)

3rd International Conference on Access to Recent Advances in Engineering and Digitalization
March 15 - 17, 2023

Reference: A Lossless Audio Encryption Method based on Chebyshev Map. Orclever Proceedings of Research and Development,2(1), 28-38

Abstract

This paper presents a lossless and secure audio encryption method based on the chaotic Chebyshev map. Firstly, the input audio samples are preprocessed to obtain the integer and decimal parts. The integer parts are rescaled to the interval [0,255]. By iterating the Chebyshev map in the chaotic range using plaintext-dependent variables, the integer parts of the input audio sample are scrambled and then diffused. Finally, a post-processing operation is applied to the diffused audio samples. Keyspace and key sensitivity analysis, histogram analysis, the correlation between adjacent samples analysis, information entropy analysis, number of sample change rate analysis, and speed analysis results are presented. These security analysis results show that the proposed audio encryption method can be used in secure voice transmission applications.

Keywords: audio encryption, chaotic maps, Chebyshev map, cryptography, security

1. Introduction

Since audio transmission has become an important part of daily life, the security of private conversations must be ensured. In this regard, audio encryption algorithms can be used to transfer an audio file securely. Audio samples are encrypted with a secret key known only to the other party so that third parties cannot correctly decrypt the transmitted audio. Therefore, even if an attacker accesses the encrypted data, he cannot understand the actual content of the audio.

Similar to image encryption techniques, scrambling and diffusion operations can be applied to the input audio signals [1]. The scrambling process shuffles the audio samples with the help of a key-dependent sequence. After the scrambling process, the diffusion operation changes the values of the audio samples based on a diffusion sequence. In the literature, different chaotic maps are employed to generate scrambling and diffusion parameters. In [2], for example, an audio encryption scheme based on confusion and diffusion operations using a three-dimensional scroll chaotic system is proposed. Similarly, in [3], a mixture of three different chaos functions is used to encrypt audio messages. A speech encryption method based on chaotic maps such as Chen's map, logistic map, tent map, quadratic map, and Bernoulli's map is proposed in [4]. In [5], a bit-scrambling process and multi-chaotic systems are combined with DNA encoding for an audio encryption scheme. Similarly in [6], both DNA encoding and piecewise linear chaotic map are used in an audio encryption algorithm. In another digital audio signal encryption method, Mobius transformation is used for substitution and chaotic Henon map is used for pixel permutation [7]. A pseudorandom byte generator based on Ikeda chaotic map is used to encrypt audio files [8]. In another scheme, Chen memristor chaotic system is used [9]. There are also non-chaotic audio encryption methods available in the literature [10], [11].

In this paper, a lossless mono-channel audio encryption algorithm is proposed. The encryption scheme is based on the chaotic sequences produced by the Chebyshev map. Scrambling and diffusion of the input audio samples are carried out using chaotic sequences. Several security analyses of the proposed method are also presented. The following sections contain a description of the proposed audio encryption method and the results of the security analysis.

2. The Proposed Encryption Method

The proposed encryption method consists of four steps: preprocessing of the input audio, scrambling, diffusion, and postprocessing.

2.1. Chebyshev Map

Using the chaotic Chebyshev map, whose equation is given in (1), scrambling and diffusion sequences are produced.

$$z_{n+1} = \cos(\omega \arccos(z_n)) \tag{1}$$

where $z_0 \in (-1,1)$ is the initial condition and $\omega \in (2,\infty)$ is the control parameter. The bifurcation diagram of the Chebyshev map is illustrated in Fig. 1. This map shows a fully chaotic behavior if the control parameter is larger than two.

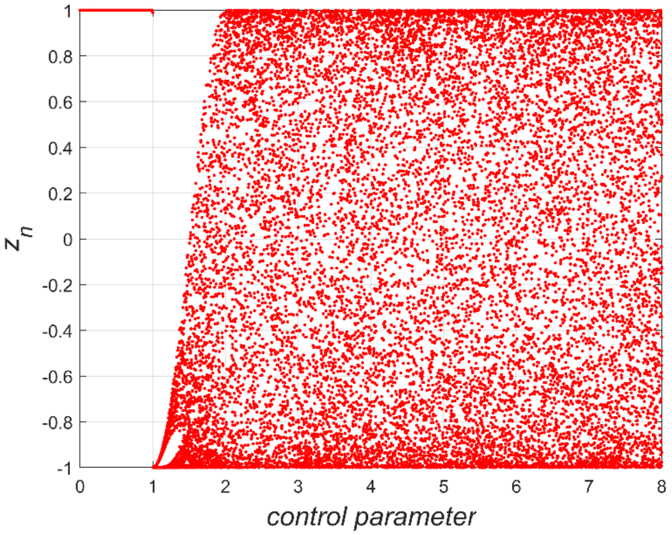


Figure 1: Bifurcation Diagram of Chebyshev Map

2.2. The Audio Encryption Steps

The first step of the proposed audio encryption algorithm is preprocessing the input audio file. Before preprocessing the input data, three secret keys are obtained from the raw audio. The maximum, minimum, and average values of the input signal, which are assigned to variables a, b, and c, respectively, are chosen as secret keys. Assuming that the input audio's magnitude is in the range of [-1,1], the following operations are applied to the input audio samples.

$$x_2 = 256 \times \left(\frac{x+1}{2}\right) \tag{2}$$

$$x_{2i} = \lfloor x_2 \rfloor \tag{3}$$

$$x_{2d} = x_2 - \lfloor x_2 \rfloor \tag{4}$$

where x is the input audio samples, x_2 is the preprocessed audio samples, $x_{2i} \in [0,255]$ is the integer part of x_2 and $x_{2d} \in [0,1)$. The Chebyshev map given in (1) is iterated by the number of samples of the input audio signal using the following initial condition and control variable.

$$z_0 = 2 + |10^{15}a + 10^{15}b + 10^{15}c| \tag{5}$$

$$\omega = (10^{15}a + 10^{15}b + 10^{15}c) \bmod 1 \tag{6}$$

When the Chebyshev map is iterated using the Eqs. (5-6), a chaotic sequence called Y is produced. This sequence is sorted in descending order and a new sequence called Y_2 is obtained. The index values ($index$) satisfying (7) are found.

$$Y_2 = Y(index) \tag{7}$$

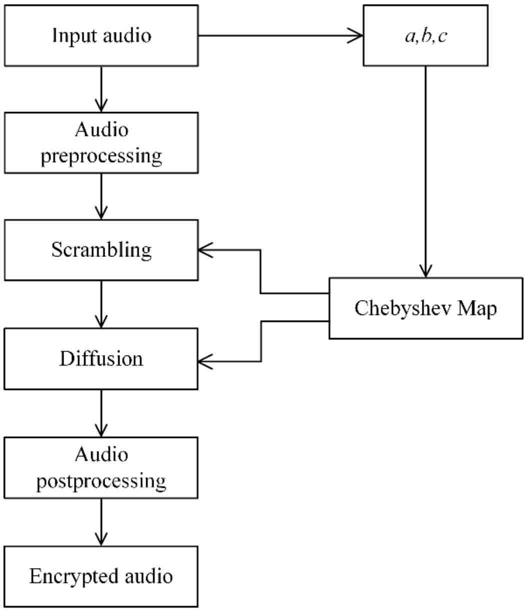


Figure 2: Flowchart of the Proposed Method

The index values are used to scramble the integer part of the preprocessed audio samples.

$$x_{2i\_scrambled} = x_{2i}(index, :) \tag{8}$$

After the scrambling part, the diffusion operation is implemented using the diffusion sequence D which is obtained as follows.

$$D = \lfloor |Y \times 10^{12}| mod 256 \rfloor \tag{9}$$

A bitwise XOR operation is implemented between scrambled audio samples and the diffusion sequence as in (10).

$$x_f = x_{2i\_scrambled} \oplus D \tag{10}$$

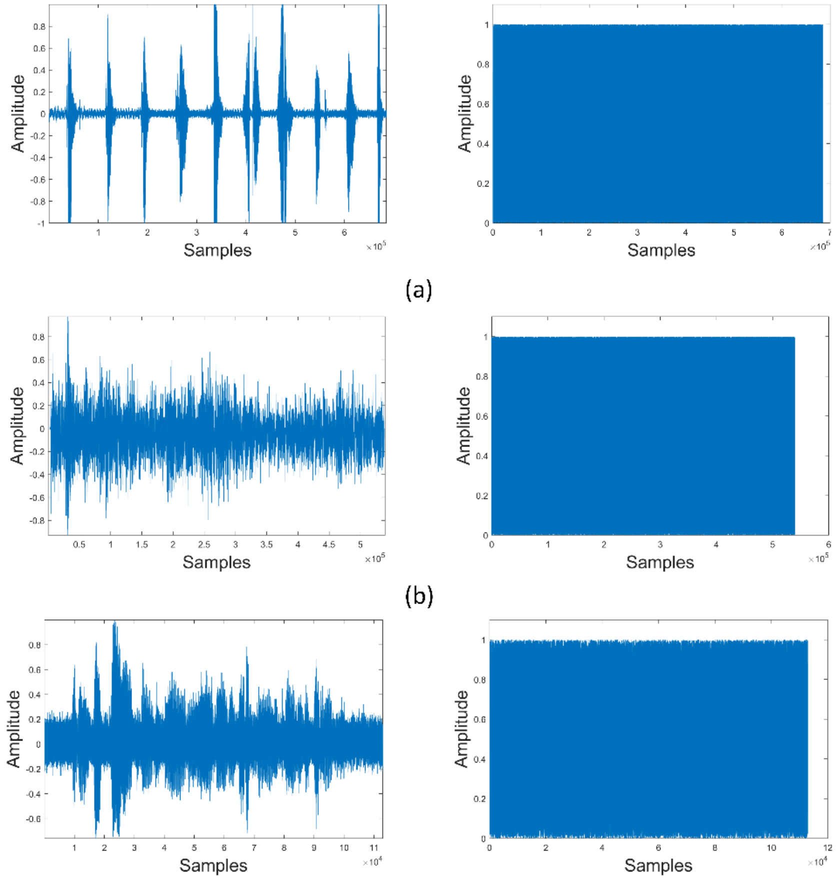
Finally, postprocessing is applied as in (11) to create the ciphered audio message.

$$x_c = (x_f + x_{2d})/256 \tag{11}$$

where x_c are the encrypted audio samples. The encrypted audio samples can be decrypted using the correct secret keys and following the encryption steps in reverse order. The flowchart of the proposed audio encryption method is shown in Fig. 2.

Table 1: Details of the Used Audio Files

Name	Content	Length (s)	Sample Rate
Audio 1	Counting 16	15.5	44100
Audio 2	Ambiance	12.2	44100
Audio 3	Noisy Speech	5.0	22500



(c)

Figure 3: Plaintext and Encrypted Audios: (a) Audio 1 (b) Audio 2 (c) Audio 3

3. Security Analysis Results

Three different uncompressed mono-channel audio samples from MATLAB's Audio Toolbox were used in the performance analysis. The details of the used audio files are listed in Table 1. In Fig. 3, the audio samples and their encryption results are shown. For the simulations, MATLAB 2020a is executed on a PC with a 2.80 GHz Intel Core i7 and 16 GB RAM.

3.1. Keyspace and Key Sensitivity Analysis

In the proposed audio encryption scheme, the maximum, minimum, and average values of the input audio file are used as secret keys. Keyspace can be calculated by finding the precision of each key experimentally. During the simulations, each key's precision is found to be 10^{-16}. Therefore, the total keyspace is calculated as $10^{16} \times 10^{16} \times 10^{16} = 10^{48} \cong 2^{159}$. The proposed method can resist brute-force attacks because it is larger than the required minimum keyspace (2^{100}). In the key sensitivity test, only one of the secret

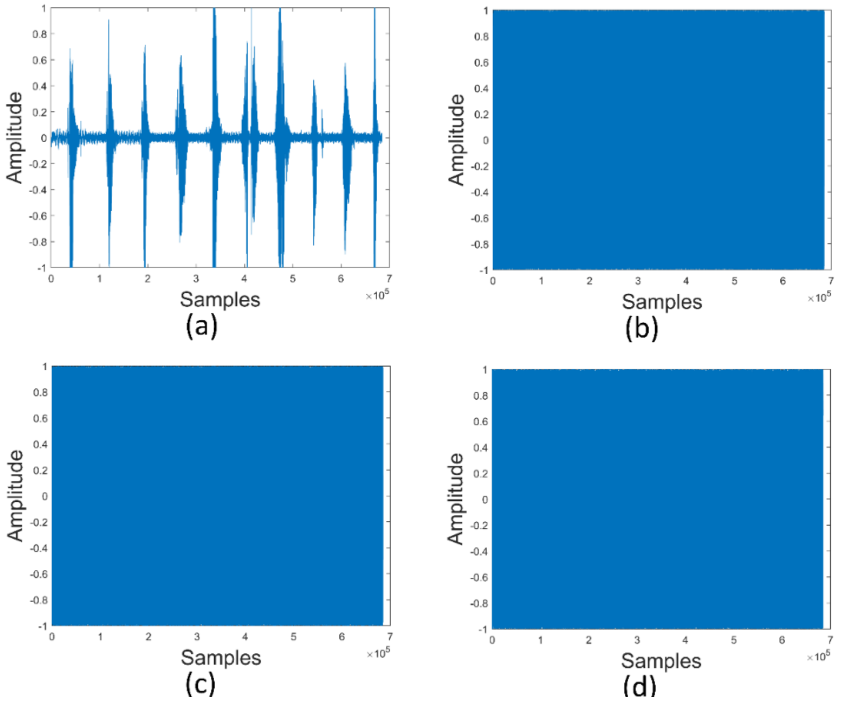


Figure 4: Decryption Results. (a) Correct Keys (b) $a - 10^{-16}$ (c) $b + 10^{-16}$ (d) $c - 10^{-16}$

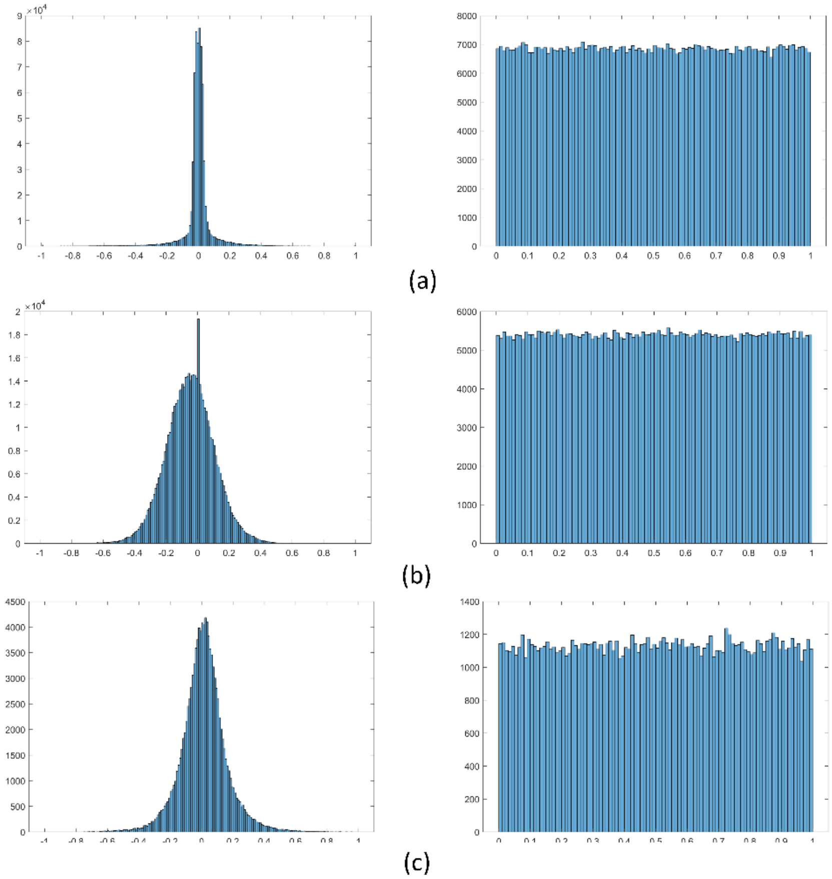
Table 2: Correlation Coefficients

Name	Input Audio	Encrypted Audio
Audio 1	0.90595	0.00288
Audio 2	0.99646	0.00882
Audio 3	0.69499	-0.00282

keys is changed by a very small amount, and decryption is done using the correct keys and the wrong key. Audio 1 is used for the key sensitivity analysis as shown in Fig. 4. If the correct keys are used in the decryption process, original audio can be recovered without loss as in Fig. 4(a). If any of the secret keys is changed by 10^{-16}, a meaningless audio file is obtained as shown in Figs. 4(b), (c), and (d), which indicates key sensitivity.

3.2. Histogram Analysis

The histogram plot of raw audio represents a meaningful distribution of audio samples. However, to resist statistical attacks, the distribution of encrypted audio samples should be uniform. Therefore, an attacker cannot make an inference about the original audio if its encrypted version has a uniform distribution of samples. In Fig. 5, the histogram plots of the input audios and encrypted audios are displayed. As can be seen in Fig. 5, encrypted audio samples are uniformly distributed, indicating resistance to statistical attacks.



(a)

(b)

(c)

Figure 5: Histogram Plots. (a) Audio 1 (b) Audio 2 (c) Audio 3

3.3. Correlation Analysis

The correlation between adjacent samples of the original audio is likely to have a high value. Therefore, a good audio encryption algorithm should lower this correlation so that the proposed cryptosystem can resist statistical attacks. Correlation between adjacent audio samples can be computed using the correlation coefficient as given in (12).

$$\rho_{s,r} = \frac{\sum_{i=1}^{k}\left(s_i - E(s)\right)\left(r_i - E(r)\right)}{\sqrt{\sum_{i=1}^{k}\left(s - E(s)\right)^2 \sum_{i=1}^{k}\left(r_i - E(r)\right)^2}} \tag{12}$$

where s and r are the randomly selected adjacent audio samples, $k = 15000$ is the number of uniquely and randomly selected audio sample pairs, $E(s)$ and $E(r)$ are mean values of the adjacent samples. As shown in Table 2, the correlation coefficient values of the encrypted audio samples are very close to zero. It can be said that the correlation between adjacent audio sample pairs is broken with the help of the proposed audio encryption method. The graphs of the distribution of 5000 unique and randomly selected pairs of audio samples are also shown in Fig. 6. The left column in the figure shows the

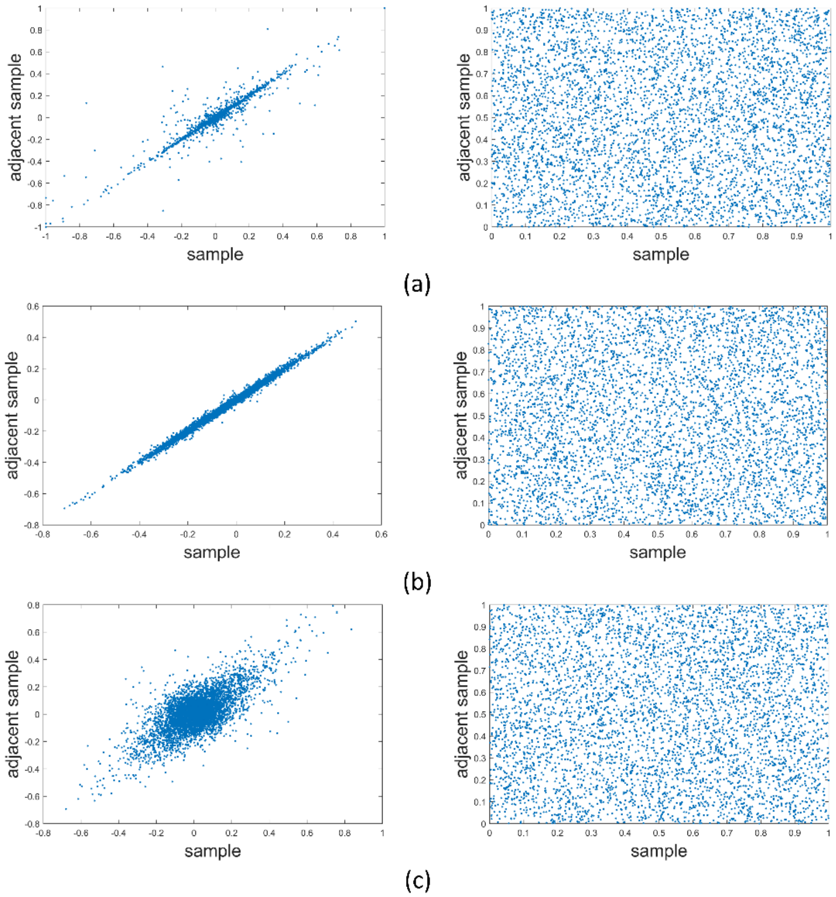


Figure 6: Correlation Plots. (a) Audio 1 (b) Audio 2 (c) Audio 3

Table 3: Information Entropy Values

Name	Input Audio	Encrypted Audio
Audio 1	3.2717	7.9980
Audio 2	3.2038	7.9979
Audio 3	4.3687	7.9963

distribution of adjacent samples of the input audio files. The adjacent samples are highly correlated to each other. On the other hand, the right column includes the graphs of the distribution of adjacent samples of the encrypted audio files. Adjacent samples are scattered all over the plane. There is no correlation between the two adjacent samples.

3.4. Information Entropy

Information entropy is an indicator of the randomness of audio samples. The information entropy value should be increased after the encryption process. For an encrypted audio file, the information entropy value should be close to eight while it has a lower value for

Table 4: NSCR Values

Name	NSCR (%)
Audio 1	99.6076
Audio 2	99.7501
Audio 3	99.8772

raw audio files. Table 3 lists the information entropy values for the test audio files. All encrypted audio files have an information entropy value greater than 7.99. These values are very close to the ideal value. Therefore, the audio encryption method can efficiently encrypt audio files to increase the degree of uncertainty.

3.5. Number of Sample Change Rate Analysis

The number of sample change rate (NSCR) is an evaluation of the cryptosystem's resistance to differential attacks. If a sample of input audio is slightly changed, the audio encryption method should generate an entirely different encrypted audio file. NSCR can be calculated using the following formula.

$$NSCR = \frac{1}{W}\sum_{i,j} E(i,j) \tag{13}$$

$$E(i,j) = \begin{cases} 1 \text{ if } A_1(i,j) \neq A_2(i,j) \\ 0 \text{ if } A_1(i,j) = A_2(i,j) \end{cases} \tag{14}$$

where W is the length of the input audio, A_1 and A_2 are two encrypted audio files whose corresponding input audio files are the same, but their one sample is slightly different. Ideally, NSCR should be very close to 100%. A randomly selected sample from the input audio signal was changed by 10% and the NSCR values in Table 4 are obtained. The NSCR values are very close to 100 %, indicating the proposed audio encryption signal's resistance to differential attacks.

Table 5: Execution Time Results

Name	Size (MB)	Encryption Time (seconds)	Decryption Time (seconds)
Audio 1	1.30	0.4432	0.3425
Audio 2	1.02	0.3832	0.2702
Audio 3	0.21	0.1727	0.0591

3.6. Encryption/Decryption Time Analysis

The runtime of a cryptosystem must be given so that a designer can predict the applicability of the algorithm. In Table 5, the encryption and decryption times of the proposed method are listed for the test audio signals. Encryption and decryption times are dependent on the size of the input signal as seen in the table. All input signals are encrypted in less than 0.45 seconds and decrypted in less than 0.35 seconds.

4. Conclusion

In this paper, a lossless and reliable audio encryption technique based on the chaotic Chebyshev map is presented. The input audio samples are first preprocessed to get the integer and decimal parts. The integer components of the input audio sample are scrambled and then diffused by repeatedly iterating the Chebyshev map in the chaotic range. The diffused audio samples are then subjected to a post-processing operation. Results of keyspace and key sensitivity analysis, histogram analysis, analysis of the correlation between adjacent samples, information entropy analysis, analysis of the NSCR, and execution time analysis are given. The outcomes of the security analysis demonstrate the viability of the suggested audio encryption technique.

References

[1] R. Wu et al., "AEA-NCS: An audio encryption algorithm based on a nested chaotic system," Chaos, Solitons & Fractals, vol. 165, 2022.

[2] H. Liu, A. Kadir, and Y. Li, "Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys," Optik, vol. 127, no. 19, pp. 7431-7438, 2016/10/01/ 2016.

[3] A. Ghasemzadeh and E. Esmaeili, "A novel method in audio message encryption based on a mixture of chaos function," International Journal of Speech Technology, vol. 20, no. 4, pp. 829-837, 2017/12/01 2017.

[4] P. Sathiyamurthi and S. Ramakrishnan, "Speech encryption using chaotic shift keying for secured speech communication," EURASIP Journal on Audio, Speech, and Music Processing, vol. 2017, no. 1, p. 20, 2017/09/07 2017.

[5] R. I. Abdelfatah, "Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations," IEEE Access, vol. 8, pp. 69894-69907, 2020.

[6] X. Wang and Y. Su, "An Audio Encryption Algorithm Based on DNA Coding and Chaotic System," IEEE Access, vol. 8, pp. 9260-9270, 2020.

[7] D. Shah, T. Shah, and S. S. Jamal, "Digital audio signals encryption by Mobius transformation and Hénon map," Multimedia Systems, vol. 26, no. 2, pp. 235-245, 2020/04/01 2020.

[8] B. Stoyanov and T. Ivanova, "Novel Implementation of Audio Encryption Using Pseudorandom Byte Generator," applied sciences, vol. 11, no. 21, p. 10190, 2021.

[9] W. Dai, X. Xu, X. Song, and G. Li, "Audio Encryption Algorithm Based on Chen Memristor Chaotic System," Symmetry, vol. 14, no. 1, p. 17, 2022.

[10] D. Renza, S. Mendoza, and D. M. Ballesteros L, "High-uncertainty audio signal encryption based on the Collatz conjecture," Journal of Information Security and Applications, vol. 46, pp. 62-69, 2019/06/01/ 2019.

[11] Z. N. Al-kateeb and S. J. Mohammed, "A novel approach for audio file encryption using hand geometry," Multimedia Tools and Applications, vol. 79, no. 27, pp. 19615-19628, 2020/07/01 2020.