A Study of Encryption for Multimedia Digital Audio Security

Xiaodong Zhou*, Chao Wei, Xiaotang Shao
School of Literature-Journalism and Communication, Sanjiang University, Nanjing, Jiangsu 210012, China

Abstract—**Driven by the development of multimedia, the encryption of multimedia digital audio has received more attention; however, cryptography-based encryption methods have many shortcomings in encryption of multimedia information, and new encryption methods are urgently needed. This paper briefly introduced cryptography and chaos theory, designed a chaos-based encryption algorithm that combined Logistic mapping and Sine mapping for confusion and used a Hopfield chaos neural network for diffusion, explained the encryption and decryption process of the algorithm, and tested the algorithm. It was found that the keys obtained by the proposed algorithm passed the SP800-22 test, and the correlation between the three encrypted audio and the original audio was 0.0261, -0.0536, and 0.0237, respectively, all of which were small, and the peak signal-to-noise ratio (PSNR) values were -0.348 dB, -7.645 dB, and -3.636 dB, respectively, which were significantly different from the original audio. The NSCR and UACI were also closer to the original values. The results prove that the proposed algorithm has good security and can encrypt the actual multimedia digital audio.**

Keywords—Multimedia digital audio; chaotic theory; encryption; logistic mapping; sine mapping; security

I. Introduction

The dissemination speed of multimedia information is increasingly accelerated with the development of computer technology [1]. Relying on the Internet, mobile terminals, etc., digital images, video, audio, and other multimedia information is generated and transmitted all the time, which facilitates people's communication and exchange and also brings new challenges to information security. Multimedia information is mostly transmitted and stored in public environment, and under the influence of network, it spreads faster and wider, and the danger of information leakage is also greater [2]. Encryption can effectively improve the security of multimedia information, so multimedia encryption has also become an important content [3]. At present, many methods have been applied in the encryption of texts and images; however, compared with them, audio has greater redundancy and higher relevance, so the traditional text and image encryption methods are not applicable to audio. Therefore, encryption for digital audio has become a common concern for researchers [4]. Singh et al. [5] compared the performance of dynamic advanced encryption standard (AES) and standard AES for audio encryption and analyzed the quality of the algorithms by histogram, correlation, etc. Babu et al. [6] converted audio data to image data, studied the encryption and decryption of audio using a fractional order hyperchaotic system, and verified the security of the system through analysis. Wang et al. [7] proposed an encryption method using a chaotic system and deoxyribonucleic acid (DNA) coding and found that the method performed well in multichannel audio processing through comparative experiments on different types of audio. Zaid et al. [8] proposed two chaos-based permutation algorithms: Arnold cat mapping and Baker mapping. The experiments showed that both algorithms can provide reliable security, but in most cases, Arnold cat mapping performs better. At present, there are still many challenges in multimedia digital audio encryption, and the security of existing methods cannot meet such encryption needs yet. Therefore, in order to find out a more suitable encryption method for multimedia digital audio, this paper designed a chaos-based method and proved the reliability of the method through experiments. This work provides a new method for the research of multimedia digital audio encryption and also provides theoretical support for the in-depth research of multimedia information encryption. This paper first briefly introduces cryptography and chaos theory in Section II. It describes the encryption and decryption method based on Logistic mapping, Sine mapping, and Hopfield chaotic neural network designed in this paper. Section III presents the experiments on the proposed encryption and decryption method used to prove its security for multimedia digital audio encryption and decryption. Section IV is the conclusion section, which briefly summarizes and reflects on the research of this paper.

II. Chaos-based Audio Encryption Algorithm

A. Cryptography and Chaos Theory

A simple password system generally consists of several components, as shown in Fig. 1.

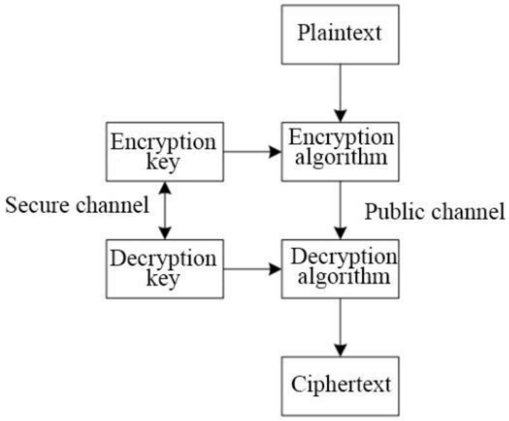


Fig. 1. A simple password system.

As shown in Fig. 1, the plaintext is the original message to be encrypted, written as M. The ciphertext is the encrypted message, written as C. It is assumed that there is an encryption algorithm E, then the encryption process is written as: $E(M) = C$. Let the decryption algorithm be D, then the decryption process is written as: $D(C) = M$.

For audio information with high redundancy and high correlation, traditional encryption algorithms, such as AES and DES [9], are unable to encrypt effectively. Chaos contains characteristics such as ergodic, unpredictable, and random, and it can be applied to encryption to get good results [10]. In the Devaney's definition of chaos [11], for mapping f in the metric space V, if it is chaotic, then the following conditions are satisfied:

1) There exists $\delta > 0$, for any $\varepsilon > 0$ and $x \in V$, there exists y and natural number n in the ε neighbourhood of x such that $d[f^n(x), f^n(y)] > \delta$;

2) For any open sets X and Y in V, there exists $k > 0$ such that $f^k(x) \cap Y \neq \emptyset$;

3) The periodic orbit of f is dense in V.

Chaos is usually determined using the Lyapunov exponential method [12]. In a one-dimensional chaotic system, there exists an orbit: $x_0, x_1 = f(x_0), \cdots, x_n = f(x_{n-1}), \cdots$. A perturbation δx_0 is added to x_0. After n-step iterations, the resulting perturbation is written as:

$$\delta x_n = f'(x_{n-1}) f'(x_{n-2}) \cdots f'(x_0) \delta x_0. \qquad (1)$$

The Lyapunov exponent is written as:

$$\Lambda = \lim_{\delta x_0 \to 0} \lim_{n \to \infty} \frac{1}{n} \log \left| \frac{\delta x_n}{\delta x_0} \right| =$$

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \log |f'(x_i)|. \qquad (2)$$

When $\lambda > 0$, it means that the orbit is sensitive to the initial value, i.e., it is a chaotic orbit.

Classical chaotic systems include the following types.

1) Logistic mapping [13]: $x_{r+1} = \mu x_r (1 - x_r)$, where r is the number of iterations and μ is the system bifurcation parameter, $\mu \in (0,4)$. When $3.5699456 < \mu \leq 4$, the system is in a chaotic state.

2) Henon mapping [14]: $\begin{cases} x_{r+1} = -p x_r + y_r + 1 \\ y_{r+1} = q x_r \end{cases}$. When $p = 1.76$ and $q = 0.1$, the system is in a chaotic state.

3) Sine mapping [15]: $x_{r+1} = \mu \sin(\pi x_r)$. When $\mu \in [3.48,4]$, the system is in a chaotic state.

4) Lorenz chaotic system [16]: $\begin{cases} x' = -\delta(x - y) \\ y' = -xz + \gamma x - y \\ z' = xy - bz \end{cases}$, where δ, γ, and b are the system control parameters. When $\delta = 10$, $\gamma = 28$, $b = 8/3$, or $\delta = 16$, $\gamma = 40$, $b = 4$, the system is in a chaotic state.

B. Audio Encryption Algorithm

One-dimensional chaotic mapping is simple in the chaotic system. In order to improve the security of chaotic encryption, this paper proposes an improved method, i.e., combining two one-dimensional chaotic mappings. Logistic mapping has the problem of uneven data distribution, and the same defect also exists in the Sine mapping. Therefore, they are combined to obtain the Logistic-Sine-coupling mapping (LSCM), and the corresponding equation is:

$$x_{r+1} = (\mu x_r (1 - x_r) + (4 - \mu) \sin(\pi x_r) / 4) \mathrm{mod} 1. \qquad (3)$$

When $\mu \in (3, 4]$, the system is in a chaotic state.

With the continuous development of neural networks, their applications in fields such as artificial intelligence are becoming more and more widespread, and neural networks also carry the chaotic characteristics. Hopfield neural networks are enough to meet the requirements of cryptography and have good performance in encryption [17]. It is divided into two types, discrete and continuous. The discrete type is used in this paper, and its expression is:

$$x = -x_i + \sum_{i=1}^{3} w_{ij} v_i, \qquad (4)$$

$$v_i = \tanh(x_i) = \frac{e^{x_i} - e^{-x_i}}{e^{x_i} + e^{-x_i}}, \qquad (5)$$

where w_{ij} is the weight matrix. The three-dimensional Hopfield neural network with high operational efficiency and a good chaotic state is called Hopfield chaotic neural network (HCNN), and the corresponding equation is:

$$\begin{cases} x_1' = -x_1 + 2 \tanh(x_1) - \tanh(x_2) \\ x_2' = -x_2 + 1.7 \tanh(x_1) + 1.7 \tanh(x_2) + 1.1 \tanh(x_3) \\ x_1' = -x_3 - 2.5 \tanh(x_1) - 2.9 \tanh(x_2) + 0.56 \tanh(x_3) \end{cases}. \qquad (6)$$

In multimedia digital audio encryption and decryption, the LS mapping is used to perform confusion operation on audio, and then HCNN is used to generate diffusion sequence. First, the encryption process is as follows:

1) The original audios from the left and right channels are read and denoted as two sets of audio A (L × 2).

2) Hash operation is performed on the original audios to get hashed value h: $h = hash(A, 'SHA - 512')$.

3) The key generation process is as follows. $hex2dec$ is a function that converts a hexadecimal hash code to a decimal number, and m is the number of iterations.

$$\begin{cases} x_{01} = hex2dec\big(h(1{:}25)\big)/(L \times 10^{24}) \\ x_{02} = hex2dec\big(h(26{:}50)\big)/(L \times 10^{24}) \\ x_{03} = hex2dec\big(h(51{:}75)\big)/(L \times 10^{24}) \\ x_{04} = hex2dec\big(h(76{:}100)\big)/(L \times 10^{24}) \\ x_{05} = hex2dec\big(h(101{:}125)\big)/(L \times 10^{24}) \\ m = 10000 + hex2dec\big(h(126{:}128)\big) \end{cases} \qquad (7)$$

4) Initial values x_{01} and x_{02} are processed to obtain initial values x_1 and μ of LSCM: $\begin{cases} x_1 = mod(x_{01}, 1) \\ \mu = mod(x_{02}, 1) \end{cases}$, where mod is the modulo operation. Then, the LSCM is subjected to m preiteration to fully reach the chaotic state, and then it is iterated 2 L times to obtain the chaotic sequence: $\begin{cases} X_1 = \{x_{11}, x_{12}, \cdots, x_{1L}\} \\ X_2 = \{x_{21}, x_{22}, \cdots, x_{2L}\} \end{cases}$.

5) Random sequences $X - H_1$ and $X - H_2$ without repetition are generated based on X_1, X_2, and two arrays of natural numbers $H_1 = \{1,2,\cdots,L\}$ and $\mathrm{H}_2 = \{1,2,\cdots,\mathrm{L}\}$ to confuse audio A. Then, A': $\begin{cases} A'(1{:}L,1) = A(X - H_1(1{:}L),1) \\ A'(1{:}L,2) = A(X - H_2(1{:}L),2) \end{cases}$ is obtained.

6) x_{03}, x_{04}, and x_{05} are substituted into the three-dimensional HCNN to obtain three diffusion sequences: . $\begin{cases} Y_1 = \{y_{11}, y_{12}, \cdots, y_{1L}\} \\ Y_2 = \{y_{21}, y_{22}, \cdots, y_{2L}\}. \\ Y_3 = \{y_{31}, y_{32}, \cdots, y_{3L}\} \end{cases}$

7) Exclusive OR diffusion is performed to obtain encrypted speech C : $\begin{cases} C_1(i) = bitXOR\big(B_1(i-1), Y_1(i)\big) \\ C_2(i) = bitXOR\big(B_2(i-1), Y_2(i)\big) \end{cases}$, where $bitXOR$ is the bitwise exclusive OR function and Y_1 and Y_2 are the chaotic sequence obtained by HCNN.

8) To further improve the encryption performance, Y_1, Y_2, and Y_3 are combined two by two for three times of diffusion to obtain the final encrypted speech and complete the encryption of the audio.

The decryption process of multimedia digital audio is as follows:

1) The encrypted audio is read.

2) Initial values are obtained using LSCM and HCNN in accordance with the same steps as encryption to get chaotic sequences X_1 and X_2 needed for decryption.

3) X_1 and X_2 are used to obtain decrypted diffusion sequences Y_1, Y_2, and Y_3.

4) The encryption process is reversed to perform decryption diffusion on the encrypted audio, followed by confusion. Finally, the decrypted audio is obtained.

III. Audio Encryption Algorithm Security Analysis

Experiment was carried out in Windows 10 environment, 3.4GHz processor, and 4G RAM. In the chaotic system, the value of μ was set as 3.707 and 3.808, respectively, and initial values $\mathrm{x}_{01} = 0.7$, $\mathrm{x}_{02} = 0.8$. The audios to be tested were all in wave format. The first three audios, named audio1.wav, audio2.wav, and audio3.wav, came from the Internet, and the other three audios came from THCHS-30 voice library [18]. Audios in THCHS-30 voice library were collected in a quite office environment at a sampling frequency of 16 kHz, the total duration of those audios was 30 hours, and the sampling size was 16 bits. Three audios were randomly selected from the library for experiments, named audio4.wav, audio5.wav, and audio6.wav. Taking audio1.wav as an example, the result of encryption and decryption using the proposed method is shown in Fig. 2.

Fig. 2 shows the original audio waveform of audio1.wav, and Fig. 3 shows the audio waveform obtained after audio1.wav was encrypted. It was found from the comparison between Fig. 2 and 3 that the encrypted audio did not have similarities with the original audio and was not associated with the original audio, which showed that the audio encryption method was effective and could encrypt the audio well. Fig. 4 shows the audio waveform obtained after decrypting the encrypted audio. The comparison between Fig. 2 and 4 showed that the correct original audio was obtained after decrypting using the proposed method, which proved the usability of the method.

First, the randomness of the key was tested using 15 items in the SP800-22 test package from National Institute of Standards and Technology (NIST) test, and the randomness was judged by the P value. The higher the P value, the stronger is the randomness. The results of the key test are displayed in Table I.

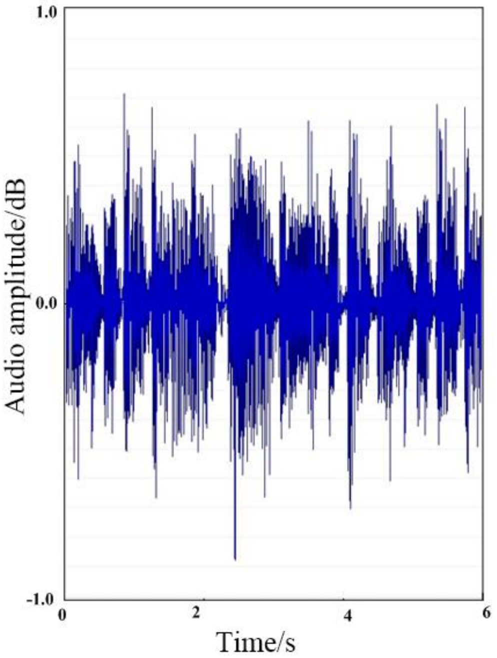


Fig. 2. Original audio.

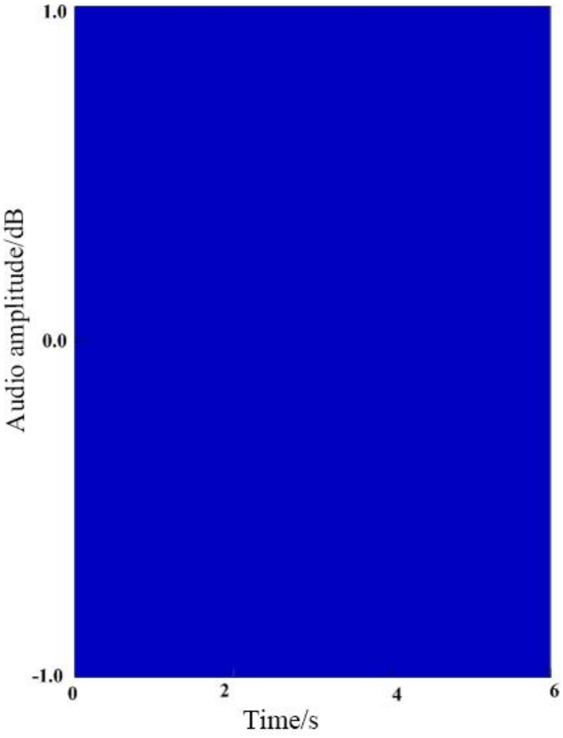


Fig. 3. Encrypted audio.

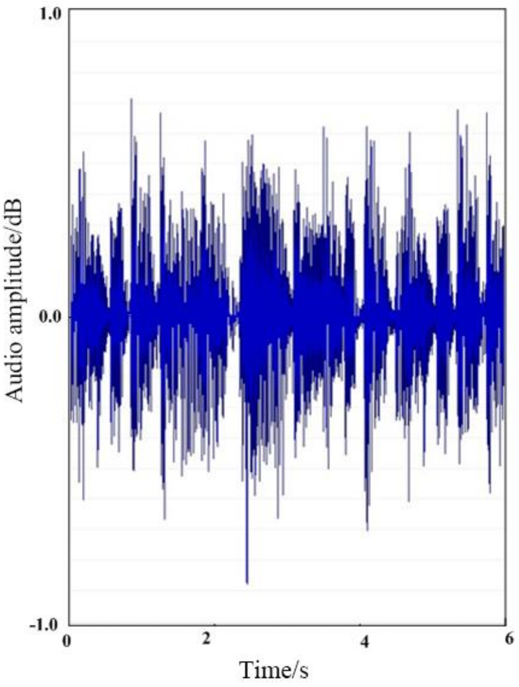


Fig. 4. Decrypted audio.

TABLE I. SP800-22 TEST RESULTS

Statistical test	P value	Result
Frequency	0.6788	Pass
Block Frequency	0.4795	Pass
Cumulative Sums	0.0945	Pass
Runs	0.3152	Pass
Longest Run	0.0528	Pass
Rank	0.7958	Pass
FFT	0.5746	Pass
Non Overlapping Template	0.9954	Pass
Overlapping Template	0.9925	Pass
Universal	0.1452	Pass
Approximate Entropy	0.9258	Pass
Random Excursions	0.6521	Pass
Random Excursions Variant	0.9654	Pass
Serial	0.4215	Pass
Linear Complexity	0.8752	Pass

It was seen from Table I that the keys generated using the proposed method could pass the SP800-22 test, and the P values were all greater than 0.01, indicating that the keys had good randomness and were suitable for encrypting multimedia digital audio.

The correlation coefficient reflects the correlation between two data. If there is a small correlation coefficient between the encrypted audio and the plaintext audio, it means the less similarity between the plaintext and the ciphertext. The correlation coefficient is calculated as follows:

$$r = \frac{\sum_{i=1}^{n}(A(i)-\bar{A})(B(i)-\bar{B})}{\sqrt{\sum_{i=1}^{n}(A(i)-\bar{A})^2 \sum_{i=1}^{n}(B(i)-\bar{B})^2}} \qquad (8)$$

where $\bar{A}$ and $\bar{B}$ are the mean values of A and B. The correlation coefficient of the audio before and after the encryption by the proposed method was calculated, and the results were compared with Mohamed's method [19], as shown in Fig. 5.

It was observed in Fig. 5 that the correlation between the six encrypted test audios and the original audio was small, and the coefficients were 0.0261, -0.0536, 0.0237, 0.0227, -0.0577, and 0.0219, respectively. Compared with Mohamed's method [19], the audio correlation before and after encryption by the method proposed in this paper was smaller, indicating that the similarity between the ciphertext and the plaintext was lower, i.e., the method was safe.

The peak signal-to-noise ratio (PSNR) reflects the quality of signal compression. The larger the value of PSNR, the better is the quality of signal compression, and the closer to the original audio. Conversely, if the PSNR value of the encrypted audio is smaller, it means that it is more different from the original audio. The PSNR calculation formula is:

$$PSNR = 10\log_{10}\left(\frac{maxA}{\sqrt{MSE}}\right)^2 \qquad (9)$$

$$MSE = \frac{1}{M\times N}\sum_{i,j}\big(A(i,j)-B(i,j)\big)^2 \qquad (10)$$

where M and N are the width and height of the audio, A and B are the original and encrypted audio. The PSNR obtained by the method proposed in this paper was compared with the results in Tamimi's study [20] and Liu's study [21], as shown in Fig. 6.

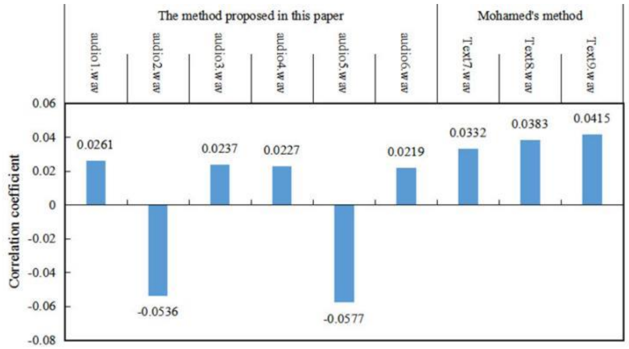
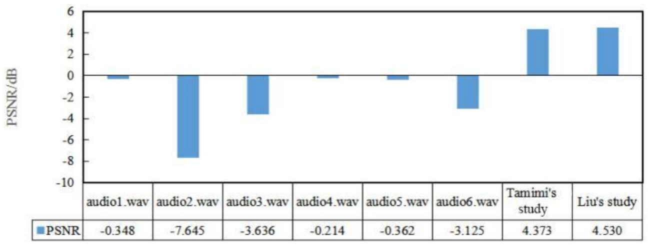


Fig. 5. Comparison of correlation coefficients before and after encryption.



	audio1.wav	audio2.wav	audio3.wav	audio4.wav	audio5.wav	audio6.wav	Tamimi's study	Liu's study
■PSNR	-0.348	-7.645	-3.636	-0.214	-0.362	-3.125	4.373	4.530

Fig. 6. Comparison of PSNR.

It was observed in Fig. 6 that the PSNR of the six audios were -0.348 dB, -7.645 dB, and -3.636 dB, which were small, and the PSNR was 4.373 dB in Tamimi's study [20] and 4.530 dB in Liu's study [21]. The PSNR values obtained in this paper were smaller; indicating that the audios encrypted by the method proposed in this paper had higher security and was more resistant to attacks.

Finally, the performance of this method against differential attacks was analyzed based on the indexes of the number of samples changes rate (NSCR) and the uniform average change intensity (UACI). The following equations are:

$$NSCR = \frac{\sum_{i=1}^{L}|Sign(B(i)-B\prime(i))|}{L} \times 100\%, \quad (11)$$

$$UACI = \frac{1}{L}\sum_{i=1}^{L}\frac{|B(i)-B\prime(i)|}{2^8-1} \times 100\%, \quad (12)$$

where $B(i)$ is the encrypted audio, $B'(i)$ is the encrypted audio with one original audio sampling data randomly changed, and $Sign$ is the sign function. When the audio signal was 8 bit, the ideal values of NSCR and UACI were 100% and 33.33%, respectively. The average values were taken after several tests and compared with the results in Soliman's study [22] and Shah's study [23], and the results are shown in Fig. 7.

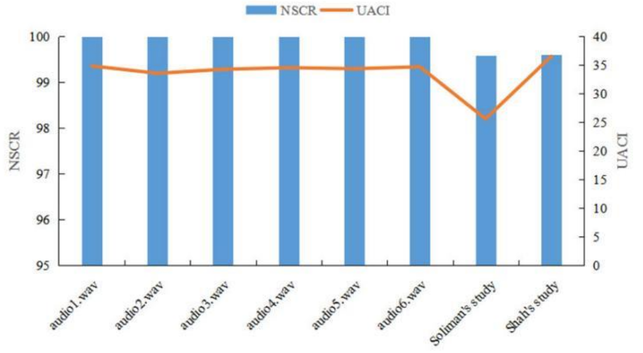


Fig. 7. Comparison of NSCR and UACI.

It was observed in Fig. 7 that compared with Soliman's study [22] and Shah's study [23], the NSCR obtained by the proposed method was always above 99.99%, which was closer to the ideal value (100%), and the UACI obtained by the proposed method was 34.8542%, 33.5628%, 34.2587%, 34.5515%, 34.3637%, and 34.6987%, which was closer to the ideal value (33.33%). These results verified the performance of the chaos-based audio encryption method in resisting differential attacks.

It was concluded from the above experimental results that the method proposed in this paper had a good encryption and decryption performance for multimedia digital audio, the encrypted audio files were not similar to the original files, and the original audio was well recovered after decryption. From the security point of view, the key obtained by the method had good randomness and passed the SP800-22 test. Then, from the comparison of different indicators, the experiments on six different audios revealed that the correlation between the audio before encryption and after decryption obtained by the method was very small, and the PSNR was also significantly smaller compared with the results in other literature, suggesting good resistance to attacks. The experimental results prove the superiority of the method for multimedia digital audio encryption and the reliability of the encryption method combining different chaos methods and further verify the usability of chaos theory for multimedia information encryption.

IV. Conclusion

This paper designed a chaos-based encryption method for the encryption of multimedia digital audio, combined LSCM with HCNN to realize the encryption of digital audio, and analyzed its security. It was found that the key obtained by the proposed method could pass the SP800-22 test, with good randomness, and the encrypted audio had less correlation with the original audio (below 0.03), smaller PSNR value, above 99.99% NSCR value, its UACI was closer to the ideal value (33.33 %), and its resistance to differential attacks was strong. The method can be further applied in practical multimedia digital audio encryption. However, there are also some shortcomings in this paper, such as the small scale of experimental data and no practical application. In future research, further studies can be conducted in hardware implementation and encryption system design to understand the operability of the method in a practical environment.

References

[1] H. Aziz, S. Gilani, I. Hussain, A. K. Janjua, and S. Khurram, "A Noise-Tolerant Audio Encryption Framework Designed by the Application of S 8 Symmetric Group and Chaotic Systems," Math. Probl. Eng., vol. 2021, pp. 5554707.1-5554707.15, April 2021.

[2] N. Sen, R. Dantu, and M. Thompson, "Performance Analysis of Elliptic Curves for VoIP Audio Encryption Using a Softphone," International Conference on Security and Privacy in Communication Systems, pp. 503-508, December 2020.

[3] S. Eldin, S. A. Khamis, A. Hassanin, and M. A. Alsharqawy, "New audio encryption package for TV cloud computing," Int. J. Speech Technol., vol. 18, pp. 131-142, March 2015.

[4] L. Zhou, X. Li, F. Tan, Y. Huang, and W. Ma, "A two-layer networks-based audio encryption/decryption scheme via fixed-time cluster synchronization," Soft Compu., vol. 26, pp. 9761-9774, July 2022.

[5] A. Singh, P. Agarwal, and M. Chand, "A Comparative Study of Audio Encryption Analysis Using Dynamic AES and Standard AES Algorithms," International Workshop Soft Computing Applications, pp. 241-249, January 2021.

[6] N. R. Babu, M. Kalpana, and P. Balasubramaniam, "A novel audio encryption approach via finite-time synchronization of fractional order hyperchaotic system," Multimed. Tools Appl., vol. 80, pp. 1-25, February 2021.

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

[8] O. Zaid, M. A. Tawfeek, and S. Alanazi, "Applying and Comparison of Chaotic-Based Permutation Algorithms for Audio Encryption," Comput. Mater. Con., vol. 67, pp. 3161-3176, February 2021.

[9] M. Karmani, N. Benhadjyoussef, B. Hamdi, and M. Machhout, "The DFA/DFT-based hacking techniques and countermeasures: Case study of the 32-bit AES encryption crypto-core," IET Comput. Digit. Tec., vol. 15, pp. 160-170, March 2021.

[10] K. Mistry, S. Dash, and S. Tallur, "Audio encryption through synchronization of chaotic oscillator circuits: Teaching non-linear dynamics through simple electrical circuits," Am. J. Phys., vol. 87, pp. 1004-1013, December 2019.

[11] H. Wang, Q. Liu, H. Li, and H. Fu, "Sensitivity, Devaney's chaos and Li–Yorke ε-chaos," Semigroup Forum, vol. 100, pp. 888-909, February 2020.

[12] M. Shafiya, and G. Nagamani, “New finite-time passivity criteria for delayed fractional-order neural networks based on Lyapunov function approach,” Chaos Soliton. Fract., vol. 158, pp. 1-12, May 2022.

[13] S. Kanwal, S. Inam, O. Cheikhrouhou, K. Mahnoor, A. Zaguia, and H. Hamam, “Analytic Study of a Novel Color Image Encryption Method Based on the Chaos System and Color Codes,” Complexity, vol. 2021, pp. 5499538-1-5499538-19, June 2021.

[14] X. Zhuo, M. Bi, Z. Hu, H. Li, X. Wang, and X. Yang, “Secure scheme for OFDM-PON system using TR based on modified Henon chaos,” Opt. Commun., vol. 462, pp. 1-7, May 2020.

[15] Z. Pan, W. Lu, H. Wang, and Y. Bai, “Recognition of a linear source contamination based on a mixed-integer stacked chaos gate recurrent unit neural network–hybrid sparrow search algorithm,” Environ. Sci. Pollut. R., vol. 29, pp. 33528-33543, May 2022.

[16] J. Shen, B. Liu, Y. Mao, R. Ullah, J. Ren, J. Zhao et al., “Enhancing the Reliability and Security of OFDM-PON Using Modified Lorenz Chaos Based on the Linear Properties of FFT,” J. Lightwave Technol., vol. 39, pp. 4294-4299, April 2021.

[17] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, “Hopfield attractor-trusted neural network: an attack-resistant image encryption,” Neural Comput. Appl., vol. 32, pp. 11477-11489, August 2020.

[18] D. Wang, and X. Zhang, “THCHS-30 : A Free Chinese Speech Corpus,” arXiv e-prints, December 2015.

[19] A. A. Mohamed, M. Ismail, and N. Zainal, “Robust Audio Encryption Method for MPEG-2 AAC Audio Based on Module Arithmetic and Chaotic Maps,” IRECOS, vol. 10, pp. 80-89, January 2015.

[20] A. A. Tamimi, and A. M. Abdalla, “An audio shuffle-encryption algorithm,” Lect. Notes Eng. Comput. Sci., vol. 2213, pp. 409-412, October 2014.

[21] 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, pp. 7431-7438, May 2016.

[22] N. F. Soliman, M. I. Khalil, A. D. Algarni, S. Ismail, R. Marzouk, and W. El-Shafai, “Efficient HEVC Steganography Approach Based on Audio Compression and Encryption in QFFT Domain for Secure Multimedia Communication,” Multimed. Tools Appl., vol. 80, pp. 4789-4823, January 2021.

[23] D. Shah, T. Shah, and S. S. Jamal, “Digital audio signals encryption by Mobius transformation and Hénon map,” Multimedia Syst., vol. 26, pp. 235-245, April 2020.