湖南大学学报（自然科学版）
Journal of Hunan University (Natural Sciences)

第 50 卷 第 5 期
2023 年 5 月

Available online at http://jonuns.com/index.php/journal/index

Vol. 50 No. 5
May 2023

Open Access Article https://doi.org/10.55463/issn.1674-2974.50.5.6

Digital Audio Protection with Confusion and Diffusion Scheme Using Double-Scroll Chaotic Function

M. T. Suryadi*, Yudi Satria, Muhammad Boyke

Department of Mathematics, Universitas Indonesia, Depok, 16424, Indonesia

* Corresponding author: yadi.mt@sci.ui.ac.id

Received: February 22, 2023 / Revised: March 19, 2023 / Accepted: April 15, 2023 / Published: May 31, 2023

Abstract: This article describes a new idea for protecting digital audio with a confusion and diffusion scheme based on the modification of the double-scroll function and SHA-256 function. In the first scheme, the confusion process is carried out by scrambling dual channels of plain audio using the keystream of the double-scroll function in the form of the proposed new nonlinear transformation function. The initial value of the double scroll function is obtained through the SHA-256 function. In the next scheme, the diffusion process is carried out by substituting the value of the dual channels based on the nonlinear transformation function, resulting in cipher audio. The proposed algorithm based on this new idea produces a very large key space of $1111\ 1\ 11^{111}$. This means that this algorithm is highly robust to brute force attacks. Simulation of the algorithm based on the test data used produces a histogram of uniformly distributed cipher audio, and the correlation coefficient is negligible (toward zero), which can be interpreted as uncorrelated. This means that this digital audio encryption algorithm is highly resistant to statistical attacks. Another performance resulting from the algorithm in this article is that it is excellent for doing cipher and decrypted audio with reference to the PSNR value of the cipher audio being negligible (4.66037-5.04020 dB), and the PSNR value of the decrypted audio is much greater (69.28398-81.14115 dB).

Keywords: audio encryption, confusion, diffusion, double-scroll chaotic function, SHA-256.

利用双滚动混沌函数的混淆和扩散方案的数字音频保护

摘要：本文介绍了一种基于双滚动函数和沙-256函数修改的混淆扩散方案来保护数字音频的新思路。在第一个方案中，通过使用双滚动函数的密钥流以所提出的新的非线性变换函数的形式对纯音频的双通道进行加扰来执行混淆过程。双滚动功能的初始值是通过沙-256函数获得的。在下一个方案中，基于非线性变换函数，通过替换双声道的值来进行扩散过程，从而产生密文音频。基于这一新思想的算法产生了1.04×〖10〗^124的非常大的密钥空间。这意味着该算法对于暴力攻击具有很强的鲁棒性。基于所使用的测试数据的算法仿真产生了均匀分布的密码音频的直方图，并且相关系数可以忽略不计（接近于零），这可以解释为不相关。这意味着这种数字音频加密算法对统计攻击具有很强的抵抗力。本文算法带来的另一个性能是，它非常适合加密和解密音频，因为加密音频的峰值信噪比值可以忽略不计

（4.66037-5.04020 dB），而解密音频的峰值信噪比值要大得多(69.28398-81.14115 分贝)。

关键词：音频加密、混乱、扩散、双卷轴混沌函数、沙-256。

1. Introduction

Data security and confidentiality are critical and urgent in the big data era. Various attempts have been made to secure digital data with chaos-based cryptography using logistic maps [1-2], logistic modification maps (MS maps) [3], chaotic permutations with multiple circular shrinking and expanding [4], density and 6D logistic maps [5], and color scrambling based on chaotic permutations with multiple circular shrinking and expanding [6] in image data. However, Chaudhary [7] proposed using the hybrid chaotic and block cipher approach for color image encryption. One critical issue is to have a secure digital voice using a chaos function, which is robust to brute force and statistical attacks.

Several schemes have been proposed using confusion and diffusion schemes based on chaotic multi-scrolling. This method produces a key space of $2^{256} \cong 3.4 \times 10^{80}$ and a key sensitivity level of 10^{-14} [8]. Another scheme, which uses a 2D cosine number transform, results in a key space of $2^{256} \cong 1.16 \times 10^{77}$ [9]. Algorithm with another scheme uses a 2D tent map and two Chebyshev polynomials, which form a key space of $2^{319} \cong 1.07 \times 10^{96}$ [10]. Another article offers a circle map scheme and a modified rotation equation that produces a key space of $2^{149} \cong 7.1 \times 10^{44}$ [11], and there is an audio encryption algorithm using a logistic map with a key space of up to $2^{348} \cong 5.7 \times 10^{104}$ [12], a normalized complex quadratic map (NCQM), which produces a key space of $2^{156} \cong 9{,}1 \times 10^{46}$ (single NCQM) and $2^{364} \cong 3{,}8 \times 10^{109}$ (double NCQM) [13], and a 3D Lorenz–Logistic map with a key space formed reaching $2^{66} \cong 7.4 \times 10^{19}$ [14]. Moreover, Abdul Kadhim et al. [15] proposed audio steganography with 4D grid multi-wing hyper-chaotic system and introduced a speech encryption algorithm based on the Lorenz chaotic map [16]; a new speech encryption algorithm based on a dual shuffling Hénon chaotic map [17] uses a chaotic elliptic map [18]. Another article offers a hybrid modified lightweight algorithm [19] that uses integer wavelet transform and geometric handling [20]. The schema we use in this paper is inspired by [8].

The chaos function is a random mapping, sensitive to initial values, and has ergodicity [21], so it can be used as a random number generator. The chaos function is suitable for designing digital data protection algorithms [22].

This paper describes a study on increasing the security of audio data encryption based on the chaos function with pre-processing using a 256-bit hash function. In the following process, confusion and diffusion schemes are used. Finally, the chaos function used is double-scroll to generate the keystream. The performance measure of this algorithm is based on various analyses, namely key space analysis, key sensitivity analysis, correlation coefficient analysis, histogram analysis, and audio quality analysis (using peak signal-to-noise ratio (PSNR) value).

The double-scroll chaos function developed in this article is inspired by ordinary differential equations [23, 24] represented by multivalued functions such as Equations (1) and (2).

$$\begin{cases} \frac{dx}{dt} = \alpha(y - x) - f(x) \\ \frac{dy}{dt} = \beta(x - y) + z \\ \frac{dz}{dt} = -\gamma(y) \end{cases} \quad (1)$$

where

$$f(x) = \begin{cases} -0.8x, & -1 \le x \le 1 \\ -0.8 - 0.5(x - 1) & 1 < x \\ -0.8 - 0.5(x + 1) & x < -1 \end{cases} \quad (2)$$

with t as time, x, y, and z are initial conditions, and $\alpha = \frac{1}{9}$, $\beta = 1$, and $\gamma = \frac{7}{10}$. This function generates three sequences, $\frac{dx}{dt}$, $\frac{dy}{dt}$, and $\frac{dz}{dt}$, with a length of L.

The Lyapunov exponent can examine the stability or chaotic nature of a dynamic (non-linear) system [25]. Fig. 1 shows that this nonlinear system is always chaotic because the largest Lyapunov exponents, when $\alpha = \frac{1}{9}$, $\beta = 1$, and $\gamma = \frac{7}{10}$, are always positive.

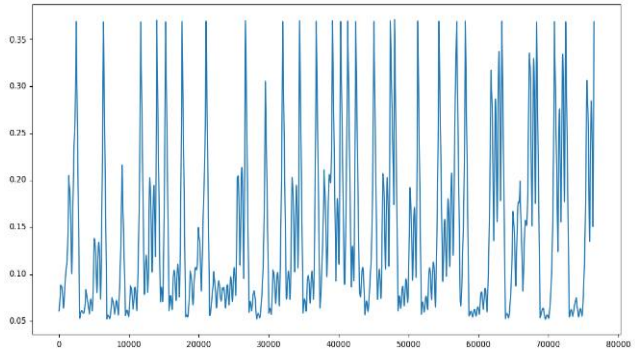

Fig. 1 The Lyapunov exponents (Developed by the authors)

2. Methods/Materials

The encryption and decryption processes developed

in this article are described in a concise and systematic manner (Fig. 2 and 3).

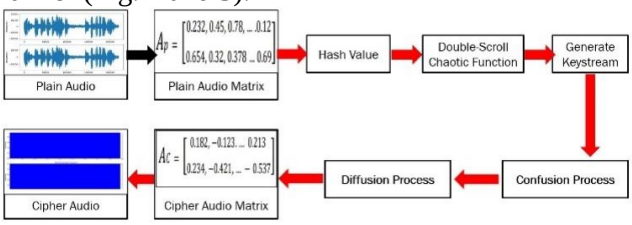

Fig. 2 The proposed digital audio encryption process (Developed by the authors)

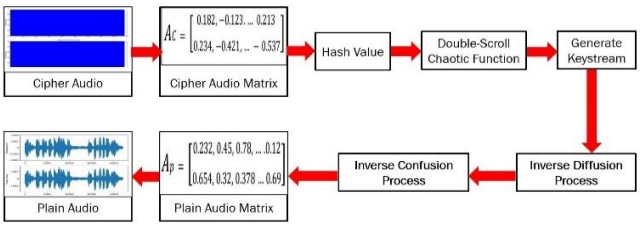

Fig. 3 The proposed digital audio decryption process (Developed by the authors)

2.1. Generating the Keystream

Obtaining cipher audio from plain audio begins by generating the keystream with the first step calculating the initial condition value, which is carried out after calculating the hash value of the plain audio file AP on dual channels with length L, using the 256-bit hash function algorithm according to Equation (3).

$$\begin{cases} x_0 = x'_0 + hex2dec\left(\frac{(h_1:h_{21})}{L\times 10^{21}}\right) \\ y_0 = y'_0 + hex2dec\left(\frac{(h_{22}:h_{42})}{L\times 10^{21}}\right) \\ z_0 = z'_0 + hex2dec\left(\frac{(h_{43}:h_{64})}{L\times 10^{22}}\right) \end{cases} \quad (3)$$

Then, we use the initial conditional values to obtain three floating-point sequences from X, Y, and Z, each of which has length L. Next, we obtain two sequences, Y_c and Z_c, with Equation (4).

$$\begin{cases} Y_c(i) = mod(a \times Y(i), 1), \ \ y \in Y \\ Z_c(i) = mod(b \times Z(i), 1), \ \ z \in Z \end{cases} \quad (4)$$

where $i = L+1, \ L, L-1, \ldots, 2$

The function $hex2(x)$ in equation (3) is to convert the hexadecimal number x to a decimal number. The function $mod(x, 1)$ in Equation (4) is the modulus operation to obtain the fraction value or the equivalent of $x - \lfloor x \rfloor$.

2.2. Confusion Process

In the confusion process for the test data in scrambled audio files, first, generate two ascending line numbers of the two-channel AP matrix. This is presented in two additional arrays H_1 and H_2, as in Equation (5).

$$\begin{cases} H_1 = [1,2,3,4, \ldots . L] \\ H_2 = [1,2,3,4, \ldots . L] \end{cases} \quad (5)$$

The sequences of X and Y generated from Equation (1) are sorted, and the position of each component is found to obtain arrays of $H_1{}'$ and $H_2{}'$.

Let S_1 and S_2 as two rows of matrix AP represent channel-1 and channel-2 of plain audio, respectively. Permute S_1 and S_2 by Equation (6) to obtain the permuted arrays $S_1{}'$ and $S_2{}'$; then, elements in AP are confused.

$$\begin{cases} S'_1(i) = S_1[H'_1(i)] \\ S'_2(i) = S_2[H'_2(i)] \end{cases} \quad (6)$$

where $i = 1,2,3, \ldots, L$.

2.3. Diffusion Process

A simple nonlinear transformation is used [17] for the diffusion process, as in Equation (7).

$$f(x,m) = \frac{x(2+xm-m)}{k} \quad (7)$$

where $x \in [-1.0, \ 1.0]$ is a number generated by equation (1) and $m \in [-1.0, \ 1.0]$ is a value that represents the normalized audio sample, k $\in \mathbb{N}$. Diffuse the elements to obtain the arrays $S_1{}''$ and $S_2{}''$ and the rows of the ciphered audio data matrix AC by Equation (8).

$$\begin{cases} S''_1(i) = \frac{Y_c(i)(2+\left(Y_c(i)\times S'_1(i)\right)-S'_1(i))}{a} \\ S''_2(i) = \frac{Z_c(i)(2+\left(Z_c(i)\times S'_2(i)\right)-S'_2(i))}{b} \end{cases} \quad (8)$$

where $i = 1, \ 2 \ldots L$, and $a, b \in \mathbb{N}$.

2.4. Embedding the Hash Value

The keys used in this algorithm are symmetric, so the hash value used to generate the key stream must be obtained in the decryption process. Let $hash_1$ be an array containing $h_1, h_2, h_3, \ldots, h_{32}$ and $hash_2$ be an array containing $h_{33}, h_{34}, h_{35}, \ \ldots, h_{64}$. Then, convert $hash_1$ and $hash_2$ from hexadecimal to decimal form, divide them by 16 because the values $S_1{}''$ and $S_2{}''$ are between −1.0 and 1.0. Finally, concatenate $hash_1$ with $S_1{}'''$ and $hash_2$ with $S_2{}'''$ in Equation (9).

$$\begin{cases} S'''_1(i) = S''_1(i) \ \mid \ hash_1 \\ S'''_2(i) = S''_2(i) \ \mid \ hash_2 \end{cases} \quad (9)$$

where $i = 1,2,3, \ldots, L$.

3. Results and Discussion

The simulation environment is Python version 3.7 and NIST test suite with Intel(R) Core (TM) i7-2670QM CPU @ 2.20 GHz (overclocked to 2.80 GHz), RAM 6 GB DDR3 1333 MHz. To test the performance of the encryption algorithm in terms of keystream randomness level, key space and key sensitivity, processing time, spectrum histogram, correlation coefficient, and audio quality test using peak signal-to-noise ratio.

This audio encryption and decryption algorithm was successfully developed to protect audio data confidentiality. The implementation and performance analysis of the algorithm was carried out on all audio samples as test data (Audio1: bung_tomo.wav and Audio2: JFK.wav) according to Table 1. We describe the implementation and analysis results in the

following sections, which show several output parameters as an indication of guaranteed security for audio data.

Table 1 Data used in the experiment and analysis (Developed by the authors)

Test Data	Data Name (wav)	Duration (seconds)	Size (Kb)
1	Audio – 1	5	860
2		10	1680
3		20	3360
4		40	6720
5	Audio – 2	5	862
6		10	1680
7		20	3360
8		40	6720

Fig. 4 and 5 show the frequency spectrum images of plain and cipher audio from Audio1.wav. As shown in Fig. 5, the results of the audio encryption result in the frequency values being dominant and evenly distributed (dense) throughout the time interval. The sound from the encrypted result (cipher audio) is boisterous, so the contents of the message from the original audio (plain audio) cannot be obtained.

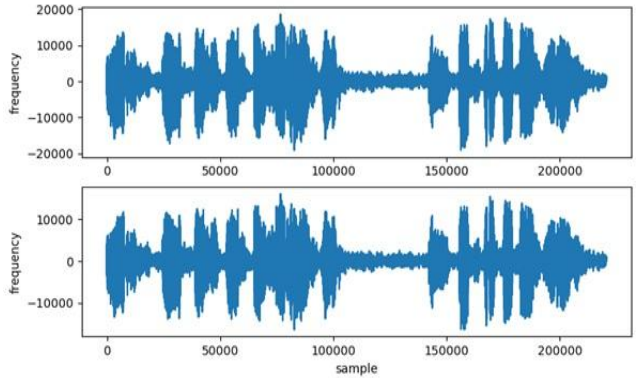

Fig. 4 The frequency spectrum image of the plain audio (Developed by the authors)

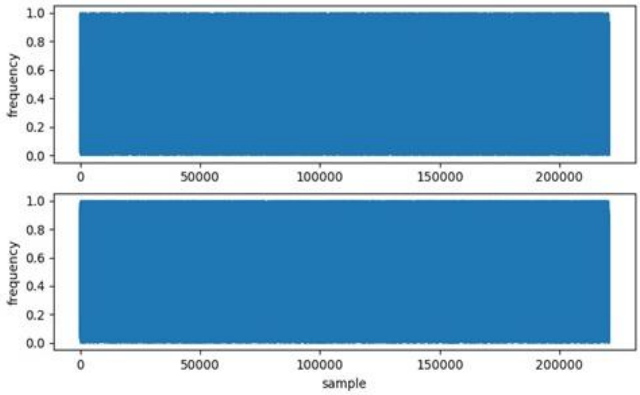

Fig. 5 The frequency spectrum image of the cipher audio (Developed by the authors)

3.1. Key Randomness Analysis (NIST Test Suite)

The NIST Test Suite was used to analyze the randomness of the keys generated by this algorithm. This test consists of 15 statistical tests with a significance level of $\alpha = 1\%$ [26].

Table 2 shows that the results of testing the keystream algorithm using the NIST Test Suite are random. This test is based on 15 statistical tests with a $P\text{-}value$, which is always greater than the significance level of $\alpha = 1\%$. In addition, the pass rate of the 15 statistical tests is almost 100%.

Table 2 NIST randomness test results (Developed by the authors)

Statistical Test	Repetition	P-Value	Proportion
Frequency	1	0.304	97/100
Block Frequency	1	0.419	98/100
Cumulative Sums	2	0.457	99/100
Runs	1	0.596	99/100
Longest Run	1	0.779	99/100
Rank	1	0.457	100/100
FFT	1	0.130	100/100
Non-Overlapping	148	0.543	99/100
Overlapping	1	0.699	99/100
Universal	1	0.868	99/100
Approximate entropy	1	0.422	100/100
Random Excursions	8	0.368	69/70
Random Exurcsions Var.	18	0.539	69/70
Serial	2	0.713	98/100
Linear Complexity	1	0.514	98/100

3.2. Time Analysis

Simulations for each test data were carried out ten times each. Table 3 shows the results of calculating the average encryption and decryption times. The average encryption time is faster than the average decryption time because we need to generate the permutated matrix in the decryption process and obtain its inverse.

Table 3 Average times of the encryption and decryption processes (Developed by the authors)

Test Data	Average time (seconds)	
	Encryption process	Decryption process
1	55.7549	60.2349
2	128.9539	140.0469
3	229.9700	235.6570
4	528.4219	539.8790
5	52.4580	60.1350
6	123.0590	136.5339
7	232.6790	243.5669
8	539.0869	552.7350

3.3. Key Space and Sensitivity Analysis

One of the characteristics of a chaotic system is its high sensitivity to initial values. This is very significant, as indicated by the key space size, so that it can provide a high level of security or resistance to brute force attacks.

The key used in this article is symmetric, and the decryption key is the same as the encryption key. The size of the key space generated from this audio encryption algorithm is $1.6 \times 10^{77} \times 10^{42} \times 6.5 \times 10^{4} = 1.04 \times 10^{124} \cong 2^{412}$. It can be concluded that this algorithm is robust in resisting brute force attacks compared to other algorithms (Table 4) because it has the largest key space size.

Table 4 Comparison based on chaotic maps and key space (Developed by the authors)

Chaotic Maps	Key Space
Multi-scrolling – SHA 256-bit [8]	$2^{267} \cong 3.4 \times 10^{80}$
2D cosine number transform [9]	$2^{256} \cong 1.16 \times 10^{77}$
2D tent map and two Chebyshev polynomials [10]	$2^{319} \cong 1.07 \times 10^{96}$

Continuation of Table 4	
Circle map and modified rotation equation [11]	$2^{149} \cong 7.1 \times 10^{44}$
Logistic map [12]	$2^{348} \cong 5.7 \times 10^{104}$
Single NCQM [13]	$2^{156} \cong 9.1 \times 10^{46}$
Double NCQM [13]	$2^{364} \cong 3.8 \times 10^{109}$
3D Lorenz – Logistic map [14]	$2^{66} \cong 7.4 \times 10^{19}$
Double scrolling – SHA 256-bit (proposed)	$2^{412} \cong 1.04 \times 10^{124}$

3.4. Histogram Analysis

A histogram test was performed on the plain and cipher audio to determine the distribution of values of all samples in digital audio (Fig. 6).

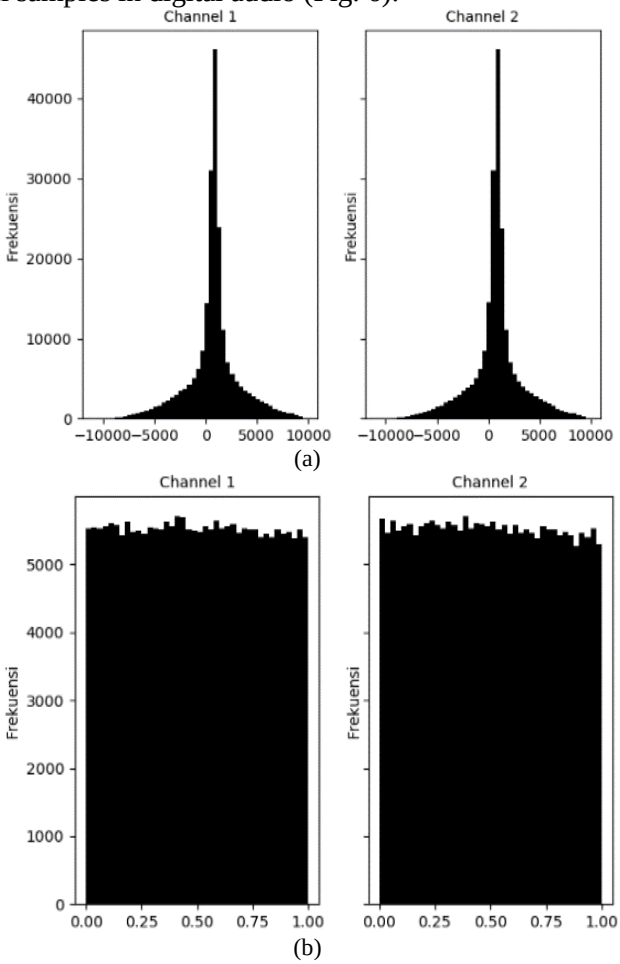

Fig. 6 Histogram of the plain (a) and cipher audio (b) (Developed by the authors)

The result shows a histogram of the sample distribution in plain audio having the frequency of occurrence of the sample value in a fluctuation form, which indicates the dominance of a sample value in digital audio. On the other hand, Fig. 6b has a form of histogram that is close to flat, indicating that the cipher audio has a uniformly distributed value for each value in the range [-1,1], making it difficult for the attacker to deduce which sample values are dominant to obtain the plain audio samples.

3.5. Correlation Coefficient Analysis

The correlation coefficient test was performed to check how close the relationship between audio data is. The analysis was performed on encrypted audio to determine the correlation of all samples against the plain audio, as shown in Table 5.

Table 5 Coefficient of correlation between the plain and cipher audio (Developed by the authors)

Test data	Plain Audio	Cipher Audio	Plain Audio and its Cipher	
	L_p/R_p	L_c/R_c	L_p/L_c	R_p/R_c
1	0.999	0.00049	0.00325	-0.00138
2	0.999	-0.00076	-0.00023	-0.00084
3	0.999	0.00038	-0.00005	-0.00104
4	0.999	0.00021	-0.00016	-0.00069
5	0.999	0.00313	0.00027	-0.00099
6	0.999	0.00445	0.00110	0.00099
7	0.999	0.00135	0.00014	-0.00064
8	0.999	-0.00005	-0.00013	-0.00160

The correlation value of each left (L) and right (R) channel of plain audio to encrypted audio from all test data is negligible (close to 0). This means that the correlation is weak or can be called no correlation. It can be stated that this algorithm is robust against statistical attacks.

3.6. PSNR Analysis

Table 6 shows the results of calculating the PSNR value of encrypted audio files against plain audio and decrypted audio files against plain audio from all test data. The PSNR value of encrypted audio is negligible, indicating that the resulting encrypted audio is very noisy or the contents of the message are not heard clearly and intact so that the information contained in plain audio files remains well protected.

Table 6 PSNR result for encrypted and decrypted audio (Developed by the authors)

Test Data	PSNR (dB)	
	Encrypted Audio	Decrypted Audio
1	4.68500	71.23889
2	4.69617	71.34967
3	4.66037	70.28735
4	4.65486	69.28398
5	5.03259	81.09750
6	5.03346	81.11023
7	5.03841	81.12663
8	5.04020	81.14115

4. Conclusion

This article proposes dual-channel audio encryption with a dual-scroll function, and the dual-scroll function is used to generate the key stream. This algorithm has high resistance to brute force attacks because the key space size reaches $2^{412} \cong 1.04 \times 10^{124}$ (the largest compared to the other 8 algorithms). In addition, based on the test results of the test data, it is found that the histogram analysis shows that the audio cipher is uniformly distributed, and the correlation coefficient on the audio cipher is close to zero, which means that the correlation is weak or can be called no correlation. both of these indicate that the algorithm proposed in this article is very resistant to statistical attacks. Meanwhile, the PSNR value of the audio cipher is negligible in the range of 4.66037-5.04020 dB, indicating that the audio cipher is very noisy and very different from the plain audio. So that information from plain audio can be protected very well. While the

PSNR value of the decrypted audio is much greater than 40 dB in the range of 69.28398-81.14115 dB, the information from the plain audio can be recovered well.

References

[1] EVA N., & SURYADI M. T. Chaos-Based Encryption Algorithm for Digital Image. Proceeding IICMA 2013, Yogyakarta, 2014, pp. 169-177. https://www.researchgate.net/profile/Samsul-Arifin-2/publication/319502474_DESIGNING_ADDITION_OPERATION_LEARNING_IN_THE_MATHEMATICS_OF_GASING_FOR_RURAL_AREA_STUDENT_IN_INDONESIA/links/5d4b8b5592851cd046ab08c3/DESIGNING-ADDITION-OPERATION-LEARNING-IN-THE-MATHEMATICS-OF-GASING-FOR-RURAL-AREA-STUDENT-IN-INDONESIA.pdf#page=183

[2] SURYADI M. T., EVA N., and DHIAN W. Performance of Chaos-Based Encryption Algorithm for Digital Image. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, 2014, 12(3): 675-682. http://doi.org/10.12928/telkomnika.v12i3.106

[3] SURYADI M. T., MARIA Y. T. I., and SATRIA Y. Encryption Algorithm using New Modified map for digital image. *Journal of Physisc: Conference Series*, 2017, 893: 012050. http://doi.org/10.1088/1742-6596/893/1/012050

[4] SURYANTO Y., SURYADI M. T., and RAMLI K. A Secure and Robust Image Encryption Based on Chaotic Permutation Multiple Circular Shrinking and Expanding. *Journal of Information Hiding and Multimedia Signal Processing*, 2016, 7(4): 697-713. https://bit.nkust.edu.tw/2016/vol7/JIH-MSP-2016-04-003.pdf

[5] RASHID A. A., & HUSSEIN K. A. Image encryption algorithm based on the density and 6D logistic map. *International Journal of Electrical and Computer Engineering*, 2023, 13(2): 1903-1913. http://doi.org/10.11591/ijece.v13i2.pp1903-1913

[6] SURYANTO Y., SURYADI M. T., and RAMLI K. A new image encryption using color scrambling based on chaotic permutation multiple circuler shrinking and expanding. *Multimedia Tools and Applications*, 2017, 76(15): 16831-16854. https://doi.org/10.1007/s11042-016-3954-5

[7] CHAUDHARY N., SHAHI T. B., and NEUPANE A. Secure Image Encryption Using Chaotic, Hybrid Chaotic and Block Cipher Approach. *Journal of Imaging*, 2022, 8(6): 167. https://doi.org/10.3390/jimaging8060167

[8] LIU H., KADIR A., and LI Y. Audio encryption scheme by confusion and diffusion basedon multi-scroll chaotic system and one-time keys. *International Journal for Light and Electron Optics*, 2016, 127: 7431–7438. https://doi.org/10.1016/j.ijleo.2016.05.073

[9] LIMA J. B. and DA SILVA NETO E. F. Audio encryption based on the cosine number transform. *Multimedia Tools and Applications*, 2016, 75(14): 8403–8418. https://doi.org/10.1007/s11042-015-2755-6

[10] ALBAHRANI E. A. A new audio encryption algorithm based on chaotic block cipher. Proceedings of the Annual Conference on New Trends in Information & Communications Technology Applications, Baghdad, 2017, pp. 22–27. https://doi.org/10.1109/NTICT.2017.7976129

[11] KORDOV K. A novel audio encryption algorithm with permutation-substitution architecture. *Electronics*, 2019, 8(5): 530. https://doi.org/10.3390/electronics8050530

[12] NAJIM AL SAAD S., & HATO E. A Speech Encryption Based on Chaotic Maps. *International Journal of Computer Applications*, 2014, 93(4): 19–28. http://dx.doi.org/10.5120/16203-5488

[13] SURYADI M. T., GUNAWAN T. S., and SATRIA Y. Securing Digital Audio Using Complex Quadratic Map. *Journal of Physics: Conference Series*, 2018, 974: 012014. https://doi.org/10.1088/1742-6596/974/1/012014

[14] SATHIYAMURTHI P., & RAMAKRISHNAN S. Speech encryption algorithm using FFT and 3D-Lorenz–logistic chaotic map. *Multimedia Tools and Applications*, 2020, 79(25–26): 17817–17835. https://doi.org/10.1007/s11042-020-08729-5

[15] ABDULKADHIM H. A., & SHEHAB J. N. Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system. *International Journal of Electrical and Computer Engineering*, 2022, 12(1): 320-330. http://doi.org/10.11591/ijece.v12i1.pp320-330

[16] AL-HAZAIMEH O. M. A new dynamic speech encryption algorithm based on lorenz chaotic map over internet protocol. *International Journal of Electrical and Computer Engineering*, 2020, 10(5): 4824-4834. http://doi.org/10.11591/ijece.v10i5.pp4824-4834

[17] AL-HAZAIMEH O. M. A new speech encryption algorithm based on dual shuffling Hénon chaotic map. *International Journal of Electrical and Computer Engineering*, 2021, 11(3): 2203-2210. http://doi.org/10.11591/ijece.v11i3.pp2203-2210

[18] AL-HAZAIMEH O. M., ABU-EIN A. A., NAHAR K. M., and AL-QASRAWAI I. S. Chaotic elliptic map for speech encryption. *Indonesian Journal of Electrical Engineering and Computer Science*, 2022, 25(2): 1103-1114. http://doi.org/10.11591/ijeecs.v25.i2.pp1103-1114

[19] MUHALHAL L. A., & ALSHAWI I. S. A hybrid modified lightweight algorithm for achieving data integrity and confidentiality. *International Journal of Electrical and Computer Engineering*, 2023, 13(1): 833-841. http://doi.org/10.11591/ijece.v13i1.pp833-841

[20] AL-KATEEB Z. N., & MOHAMMED S. J. Encrypting an audio file based on integer wavelet transform and hand geometry. *TELKOMNIKA (Telecommunication, Computing, Electronics and Control)*, 2020, 18(4): 2012-2017. http://doi.org/10.12928/telkomnika.v18i4.14216

[21] HIRSCH M. W., SMALE S., and DEVANEY R. L. *Differential equations, dynamical systems, and an introduction to chaos*. 3rd ed. Academic Press, Elsevier, 2013. https://eclass.uoa.gr/modules/document/file.php/MATH626/Morris%20W.%20Hirsch%2C%20Stephen%20Smale%20and%20Robert%20L.%20Devaney%20%28Auth.%29%20-%20Differential%20Equations%2C%20Dynamical%20Systems%2C%20and%20an%20Introduction%20to%20Chaos-Academic%20Press%20%282012%29.pdf

[22] STALLINGS W. *Cryptography and Network Security: Principle and Practice*. 5th ed. Prentice Hall, New York, 2011. https://gacbe.ac.in/images/E%20books/Cryptography%20and%20Network%20Security%20-%20Prins%20and%20Pract.%205th%20ed%20-

%20W.%20Stallings%20(Pearson,%202011)%20BBSbb.pdf
[23] DAI W., XU X., SONG X., and LI G. Audio Encryption Algorithm Based on Chen Memristor Chaotic System. *Symmetry*, 2022, 14(1): 17. https://doi.org/10.3390/sym14010017
[24] YAN D., WANG L., DUWAN S., CHEN J., and CHEN J. Chaotic Attractors Generated by a Memristor-Based Chaotic System and Julia Fractal. *Chaos, Solitons & Fractals*, 2021, 146: 110773. https://doi.org/10.1016/j.chaos.2021.110773
[25] AKGUL A., KACAR S., and PEHLIVAN İ. An Audio Data Encryption with Single and Double Dimension Discrete-Time Chaotic Systems. *The Online Journal of Science and Technology*, 2015, 5(3): 14-23. https://dergipark.org.tr/en/pub/tojsat/issue/22630/241816
[26] BASSHAM L., RUKHIN A., SOTO J., NECHVATAL J., SMID M., LEIGH S., LEVENSON M., VANGEL M., HECKERT N., and BANKS D. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. National Institute of Standards and Technology, Gaithersburg, Maryland, 2010. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762

参考文:

[1] EVA N., & SURYADI M.T. 基于混沌的数字图像加密算法。国际集成电路制造商协会2013论文集，日惹，2014年，第 169-177 页。https://www.researchgate.net/profile/Samsul-Arifin-2/publication/319502474_DESIGNING_ADDITION_OPERATION_LEARNING_IN_THE_MATHEMATICS_OF_GASING_FOR_RURAL_AREA_STUDENT_IN_INDONESIA/links/5d4b8b5592851cd046ab08c3/DESIGNING-ADDI农村地区天然气数学操作学习印度尼西亚学生.pdf#page=183

[2] SURYADI M. T.、EVA N. 和 DHIAN W. 基于混沌的数字图像加密算法的性能。电信公司（电信、计算、电子和控制），2014, 12(3): 675-682。http://doi.org/10.12928/telkomnika.v12i3.106

[3] SURYADI M. T.、MARIA Y. T. I. 和 SATRIA Y. 使用新修改的数字图像映射的加密算法。物理学杂志：会议系列，2017，893：012050。http://doi.org/10.1088/1742-6596/893/1/012050

[4] SURYANTO Y.、SURYADI M. T. 和 RAMLI K. 基于混沌排列多重循环收缩和扩展的安全鲁棒图像加密。信息隐藏与多媒体信号处理学报, 2016, 7(4): 697-713. https://bit.nkust.edu.tw/2016/vol7/JIH-MSP-2016-04-003.pdf

[5] RASHID A. A., & HUSSEIN K. A. 基于密度和6D逻辑图的图像加密算法。国际电气与计算机工程杂志，2023，13(2)：1903-1913。http://doi.org/10.11591/ijece.v13i2.pp1903-1913

[6] SURYANTO Y.、SURYADI M. T. 和 RAMLI K. 一种基于混沌排列多重循环器收缩和扩展的颜色置乱的新图像加密。多媒体工具与应用，2017，76(15)：16831-16854。https://doi.org/10.1007/s11042-016-3954-5

[7] CHAUDHARY N.、SHAHI T. B. 和 NEUPAN A. 使用混沌、混合混沌和分组密码方法进行安全图像加密。成像杂志，2022，8(6)：167。https://doi.org/10.3390/jimaging8060167

[8] LIU H., KADIR A., LI Y. 基于多卷混沌系统和一次性密钥的混淆扩散音频加密方案。国际光与电子光学杂志，2016，127：7431–7438。https://doi.org/10.1016/j.ijleo.2016.05.073

[9] LIMA J. B. 和 DA SILVA NETO E. F. 基于余弦数变换的音频加密。多媒体工具与应用，2016，75(14)：8403–8418。https://doi.org/10.1007/s11042-015-2755-6

[10] ALBAHRANI E. A. 一种基于混沌分组密码的新型音频加密算法。信息和通信技术应用新趋势年会论文集，巴格达，2017年，第 22-27 页。https://doi.org/10.1109/NTICT.2017.7976129

[11] KORDOV K. 一种具有排列替换架构的新型音频加密算法。电子学，2019，8(5)：530。https://doi.org/10.3390/electronics8050530

[12] NAJIM AL SAAD S., & HATO E. 基于混沌映射的语音加密。国际计算机应用杂志，2014，93(4)：19–28。http://dx.doi.org/10.5120/16203-5488

[13] SURYADI M. T.、GUNAWAN T. S. 和 SATRIA Y. 使用复杂二次映射保护数字音频。物理学杂志：会议系列，2018，974：012014。https://doi.org/10.1088/1742-6596/974/1/012014

[14] SATHIYAMURTHI P., & RAMAKRISHNAN S. 使用快速傅里叶变换和3D-洛伦兹逻辑混沌映射的语音加密算法。多媒体工具和应用，2020，79（25–26）：17817–17835。https://doi.org/10.1007/s11042-020-08729-5

[15] ABDULKADHIM H. A., & SHEHAB J. N. 基于4D网格多翼超混沌系统最低有效位算法的音频隐写术。国际电气与计算机工程杂志，2022，12(1)：320-330。http://doi.org/10.11591/ijece.v12i1.pp320-330

[16] AL-HAZAIMEH O. M. 一种基于互联网协议的洛伦兹混沌映射的新型动态语音加密算法。国际电气与计算机工程杂志, 2020, 10(5): 4824-4834。http://doi.org/10.11591/ijece.v10i5.pp4824-4834

[17] AL-HAZAIMEH O. M. 一种基于双混洗埃农混沌映射的新型语音加密算法。国际电气与计算机工程杂志，2021，11(3)：2203-2210。http://doi.org/10.11591/ijece.v11i3.pp2203-2210

[18] AL-HAZAIMEH O. M.、ABU-EIN A. A.、NAHAR K. M. 和 AL-QASRAWAI I. S. 用于语音加密的混沌椭圆图。印度尼西亚电气工程与计算机科学杂志，2022, 25(2): 1103-1114。http://doi.org/10.11591/ijeecs.v25.i2.pp1103-1114

[19] MUHALHAL L. A., & ALSHAWI I. S. 一种用于实现数据完整性和机密性的混合修改轻量级算法。国际电气与计算机工程杂志，2023, 13(1): 833-841。http://doi.org/10.11591/ijece.v13i1.pp833-841

[20] AL-KATEEB Z. N., & MOHAMMED S. J. 基于整数小波变换和手部几何形状加密音频文件。电信公司（电信、计算、电子和控制），2020, 18(4): 2012-2017。http://doi.org/10.12928/telkomnika.v18i4.14216

[21] HIRSCH M. W.、SMALE S. 和 DEVANEY R. L. 微分方程、动力系统和混沌简介。第三版。学术出版社，爱思唯尔，2013。https://eclass.uoa.gr/modules/document/file.php/MATH626/Morris%20W.%20Hirsch%2C%20Stephen%20Smale%20and%20Robert%20L.%20Devaney%20%28Auth.%29%20-%20Differential%20Equations%2C%20Dynamical%20Systems%2C%20and%20an%20Introduction%20to%20Chaos-Academic%20Press%20%282012%29.pdf

[22] STALLINGS W. 密码学和网络安全：原理与实践。第五版。普伦蒂斯·霍尔，纽约，2011年。https://gacbe.ac.in/images/E%20books/Cryptography%20and%20Network%20Security%20-%20Prins%20and%20Pract.%205th%20ed%20-%20W.%20Stallings%20(皮尔逊,%202011)%20BBSbb.pdf

[23] DAI W.， XU X.， SONG X.， LI G. 基于陈忆阻混沌系统的音频加密算法。对称性，2022，14(1)：17。https://doi.org/10.3390/sym14010017

[24] YAN D., WANG L., DUWAN S., CHEN J., 和 CHEN J. 基于忆阻器的混沌系统和朱莉娅分形生成的混沌吸引子。混沌、孤子和分形，2021，146：110773。https://doi.org/10.1016/j.chaos.2021.110773

[25] AKGUL A.、KACAR S. 和 PEHLIVAN I。单维和双维离散时间混沌系统的音频数据加密。在线科技杂志，2015，5(3)：14-23。https://dergipark.org.tr/en/pub/tojsat/issue/22630/241816

[26] BASSHAM L.、RUKHIN A.、SOTO J.、NECHVATAL J.、SMID M.、LEIGH S.、LEVENSON M.、VANGEL M.、HECKERT N. 和 BANKS D. 随机和随机的统计测试套件用于加密应用的伪随机数生成器。国家标准与技术研究所，马里兰州盖瑟斯堡，2010年。https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762