Article

Audio Encryption Algorithm Based on Chen Memristor Chaotic System

Wanying Dai ^{1,2} , Xiangliang Xu ^{1,3} , Xiaoming Song ¹ and Guodong Li ^{1,4,*}

¹ School of Mathematics and Computing Science, Guilin University of Electronic Technology, Guilin 541004, China; dx160622@126.com (W.D.); xd160622@126.com (X.X.); songxiaoming97@gmail.com (X.S.)

² School of Data and Statistical Sciences, Xinjiang University of Finance and Economics, Urumqi 830012, China

³ School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

⁴ Guangxi Colleges and Universities Key Laboratory of Data Analysis and Computation, Guilin University of Electronic Technology, Guilin 541004, China

* Correspondence: lgdzhzy@guet.edu.cn

Abstract: The data space for audio signals is large, the correlation is strong, and the traditional encryption algorithm cannot meet the needs of efficiency and safety. To solve this problem, an audio encryption algorithm based on Chen memristor chaotic system is proposed. The core idea of the algorithm is to encrypt the audio signal into the color image information. Most of the traditional audio encryption algorithms are transmitted in the form of noise, which makes it easy to attract the attention of attackers. In this paper, a special encryption method is used to obtain higher security. Firstly, the Fast Walsh–Hadamard Transform (FWHT) is used to compress and denoise the signal. Different from the Fast Fourier Transform (FFT) and the Discrete Cosine Transform (DCT), FWHT has good energy compression characteristics. In addition, compared with that of the triangular basis function of the Fast Fourier Transform, the rectangular basis function of the FWHT can be more effectively implemented in the digital circuit to transform the reconstructed dual-channel audio signal into the R and B layers of the digital image matrix, respectively. Furthermore, a new Chen memristor chaotic system solves the periodic window problems, such as the limited chaos range and nonuniform distribution. It can generate a mask block with high complexity and fill it into the G layer of the color image matrix to obtain a color audio image. In the next place, combining plaintext information with color audio images, interactive channel shuffling can not only weaken the correlation between adjacent samples, but also effectively resist selective plaintext attacks. Finally, the cryptographic block is used for overlapping diffusion encryption to fill the silence period of the speech signal, so as to obtain the ciphertext audio. Experimental results and comparative analysis show that the algorithm is suitable for different types of audio signals, and can resist many common cryptographic analysis attacks. Compared with that of similar audio encryption algorithms, the security index of the algorithm is better, and the efficiency of the algorithm is greatly improved.

Keywords: memristor chaotic system; fast Walsh–Hadamard transform; audio map; channel shuffle; encryption algorithm

Citation: Dai, W.; Xu, X.; Song, X.; Li, G. Audio Encryption Algorithm Based on Chen Memristor Chaotic System. *Symmetry* **2022**, *14*, 17. <https://doi.org/10.3390/sym14010017>

Academic Editor: Christos Volos

Received: 19 October 2021

Accepted: 16 December 2021

Published: 23 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2021 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

With the rapid development of the internet, wireless voice communication technology was widely applied in real-life, and in the process of data transmission there is the risk of information leakage; therefore, audio information encryption research is of great significance. Many traditional encryption algorithms are widely used in audio encryption and achieved good encryption results, such as Advanced Encryption Standard (AES) [1,2], Data Encryption Standard (DES) [3,4] and S-box algorithm [5,6], etc., Although these algorithms have perfect encryption technology, some algorithms still have some defects and cannot fully ensure the security of encryption. The main disadvantage of AES is that it uses a static S-box in the

whole algorithm, which damages the security of AES and may be subject to different algebraic attacks. Therefore, to overcome this shortcoming, Amandeep S. [7] and others proposed a dynamic S-box AES encryption algorithm. Because the chaotic system has the characteristics of ergodicity, initial value sensitivity, and strong pseudo-random sequence, many scholars proposed to encrypt plaintext information by combining the AES algorithm with the chaotic system, and the results were satisfactory. Alireza A. [8] et al. Proposed to encrypt the image by combining the chaotic sequence with the improved AES algorithm. The experimental results show that this encryption method reduces the time complexity of the algorithm, increases the keyspace of the algorithm, and significantly improves security. The chaotic system has made an important contribution to the encryption scheme. Therefore, in recent years, chaotic systems were widely used in encryption algorithms [9–11]. Abdelfatah R.I. [9] proposed a multichaotic mapping audio encryption scheme, and the novel features of this algorithm are as follows: adaptive scrambling and cryptographic feedback are used to realize global scrambling and deep diffusion, respectively. At the same time, four different audio encryption technologies are combined in the same scheme to make it more secure. Shah D. et al. [10] proposed that Mobius transform was used as the source to generate a strong S-box substitution network and Henon chaotic map to perform pixel-level displacement. However, the Henon chaotic map has a low dimension, and its keyspace is limited. To solve this problem, Zhao H. et al. [11] proposed an adaptive symmetric Henon chaotic map, which has the characteristics of wide parameter range and high complexity. Therefore, it has a larger keyspace and is more suitable for encryption algorithms. Farsana F.J. et al. [12] introduced a modified discrete Henon map, which can weaken the correlation between adjacent samples. At the same time, an improved super-Lorenz chaotic system was proposed to iterate and fill the silent period in speech conversation, and a dynamic key flow mechanism was designed to enhance the correlation between Ming and ciphertext. Some audio encryption schemes meet the security requirements of the design by enhancing the complexity of the algorithm but increasing the difficulty of data processing and the time of audio encryption, such as Naskar P.K. et al. [13] proposed an audio encryption algorithm based on DNA Encoding and Channel Shuffling, which overcomes the inefficient algorithm of multiple rounds. However, due to the adoption of an encryption scheme based on traditional mathematical methods, the timeliness of the encryption algorithm is reduced. Of course, in the existing research, there is no lack of many encryption algorithms that were decoded. Saeed N. et al. [14] found the loopholes through simulation, obtained the key of the algorithm, and decoded an image encryption algorithm related to chaotic mapping. This is a good example.

A memristor is a kind of nonlinear element with memory function and nanoscale size. It can be used as a nonlinear part of a chaotic system and has rich dynamic behaviors, which significantly improves the randomness and complexity of chaotic system signals [15]. Because the memristor is a controllable nonlinear device, in some systems, the chaotic attractors of the even and singular vortices can be obtained only by changing the parameters of the memristor. Therefore, the memristor chaotic system can provide a complex, variable, and reliable pseudo-random cipher generator for the encryption algorithm and can effectively avoid the degradation of the chaotic system dynamics.

Bao B.C. [16] designed and studied a chaotic circuit based on memristor. The active double-ended memristor circuit is used to replace Chua's diode. The circuit is directly extended from Chua's oscillator to obtain a new chaotic system. The results show that the introduction of memristor makes the dynamic behavior of the system more complex. Ma Xujiong [17] proposed a chaotic circuit with memristor, mode resistance capacitor, and linear inductor established the dimensionless mathematical model of the circuit and found that 19 different types of chaotic attractors will be generated in the circuit. Compared with that of the traditional chaotic attractors, the circuit has rich dynamic characteristics and good application prospects in the field of secure communication. Chen J.J. [18] designed an image encryption algorithm of a new hyperchaotic system based on memristor, which can produce complex chaotic attractors. The experimental results show that the circuit simulation and numerical simulation results of the system always proved the feasibility, effectiveness, and ability to produce chaotic behavior of the system. Combined with the

proposed image encryption scheme, the security analysis shows that the scheme is not easy to crack and can resist all kinds of attacks. Peng G. [19] proposed a new modal memristor chaotic system, realized its circuit simulation, and applied it to image encryption. The application scope of the memristor is far beyond these. For example, Kamal F.M. [20] designed a new fractional nonautonomous chaotic circuit model by introducing a fractional element memristor circuit; Akgul A. [21] proposed a new fractional-order chaotic circuit with memristor and linear inductor. To show the application advantages of the proposed chaotic system, it also realized the synchronization of fractional-order chaotic system and applied it to secure communication system for the first time. In addition, in their latest research, Yan D. [22] also proposed a chaotic attractor based on the combination of fractal transformation and memristor chaotic system. The main advantage of the system is that multiple rolling attractors and extended chaotic attractors can be generated only by modifying system parameters, and various circular chaotic attractors can be generated in combination with classical Julia fractal. Its attractor has complex dynamic behavior [23], which is very suitable for all kinds of secure communication fields.

In recent years, with the in-depth study of memristor chaotic system, it is more and more widely used in encryption algorithms. To improve the security and efficiency of digital speech encryption algorithm, an audio encryption algorithm based on Chen memristor chaotic system is proposed in this paper. To further improve the security of the traditional scrambling and diffusion encryption framework, a special audio encryption method is proposed. The Fast Walsh–Hadamard Transform is used for adaptive compression, denoising, and reconstruction of the audio signal. The high complexity chaotic mask block is used as the filling layer, and the dual-channel audio signal is cleverly transformed into a color audio image. To make the encryption algorithm highly correlated with plaintext audio, the audio's stored byte information is taken as the parameter of interactive channel shuffling operation, and the cipher block is used for overlapping diffusion encryption to obtain ciphertext audio. Ciphertext audio is transmitted in the form of a noise image so that the algorithm has two protective barriers, which can effectively reduce the risk of ciphertext audio information being intercepted and cracked in the transmission process. In addition, compared with that of Chen chaotic system, the Chen memristor chaotic system has a larger bifurcation interval in the range of parameter c , which means that it has a larger keyspace and can resist violent attacks. The encryption scheme not only solves the security problems of simple scrambling and diffusion operation but also improves the efficiency of the encryption algorithm.

Our contributions are as follows:

- (1) The Chen memristor chaotic system has a larger chaotic parameter interval and can produce pseudo-random sequences with high complexity, which is more difficult to predict than general chaotic signals.
- (2) A method of skillfully transforming the audio signals into image information is proposed.
- (3) We propose an audio encryption algorithm based on interactive channel shuffling and overlapping diffusion. Experimental simulation shows that the algorithm has high security.

The rest of this paper is organized as follows: in Section 2, a new memristor chaotic system model is proposed and the correlation dynamics are analyzed; in Section 3, an encryption algorithm for compressing and denoising audio signals and transforming them into image information is proposed. In the algorithm, interactive channel shuffling and overlapping diffusion are also designed; in Section 4, the experimental simulation and security analysis of the encryption algorithm is carried out; and Section 5 summarizes and discusses the full text.

2. Model and Dynamic Analysis of a Novel Memristor Chaotic System

2.1. Chen Chaotic System Model Based on Magnetically Controlled Titania Memristor

There is an insulating layer of TiO_2 film and a conductive layer of TiO_{2-x} film between the two platinum electrodes. The pure TiO_2 layer has high resistivity, while TiO_{2-x} material is conductive due to oxygen vacancy. When the current flows through the device in one

direction, the boundary between the two materials moves, increasing the percentage of conductive layer TiO_{2-x} . At this time, the resistance of the memristor decreases. When the current direction is opposite, the boundary will move in the opposite direction, the percentage of TiO_2 (insulating layer) increases, and the resistance of the memristor increases. When the current stops, the boundary stops moving, and the boundary between the two layers of the memristor freezes and maintains the last resistance value. In other words, the memristor “remembers” the current flowing through it. The physical model of the memristor [24] is shown in Figure 1.

Figure 1. Schematic of HP memristor.

The known dynamic equation of the Chen chaotic system [25] is

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a)x - xz + cy, \\ \dot{z} = xy - bz. \end{cases} \quad (1)$$

where a, b, c are the system parameter and its values are $a = 35, b = 3, c = 28$, respectively, the system is in a chaotic state.

Memristor is a nonlinear electronic component and has great potential in chaotic system design. Here, the charge variable flowing through the titanium dioxide memristor is used to replace a single variable of the system (1) to generate more complex chaotic signals. The state equation of the new memristor chaotic system constructed is as follows.

$$\begin{cases} \dot{x} = a(y - x), \\ \dot{y} = (c - a) * df(-|x|) - xz + cy, \\ \dot{z} = xy - bz. \end{cases} \quad (2)$$

where a, b, c, d is the system parameter, $f(\cdot)$ is the nonlinear term of the system, and the relationship between the flux and charge of the titania memristor is satisfied.

$$f(x) = \begin{cases} \frac{x - C_3}{R_{off}} & x < C_5, \\ \frac{\sqrt{2kx - M^2(0)} - M(0)}{k} & C_5 \leq x < C_6, \\ \frac{x - C_4}{R_{on}} & x \geq C_6. \end{cases} \quad (3)$$

where, R_{off} and R_{on} are two limit values of the memristor, and $R_{off} = 20 \text{ k}\Omega$, $R_{on} = 100 \Omega$. x is the input flux of the memristor. $M(0)$ is the initial state value of the memristor, and the value is 16,000. $C_i \ i = (3, 4, 5, 6)$ satisfies the following relation.

$$\begin{cases} C_3 = -\frac{(R_{off} - M(0))^2}{2k}, \\ C_4 = -\frac{(R_{on} - M(0))^2}{2k}, \\ C_5 = -\frac{R_{off}^2 - M(0)^2}{2k}, \\ C_6 = -\frac{R_{on}^2 - M(0)^2}{2k}. \end{cases} \quad (4)$$

where k is a constant and satisfies the relation,

$$k = \frac{(R_{on} - R_{off}) - u_v R_{on}}{D^2} \quad (5)$$

where, u_v represents the average mobility of oxygen vacancies, and the value is $10^{-14} \text{ m}^2 \cdot \text{s}^{-1} \cdot \text{V}^{-1}$. D is the thickness of the film, and the value is 10 nm. Set the parameters of the system (2) $a = 35$, $b = 3$, $c = 20$, $d = 2000$, the initial value of $(x, y, z) = (0.6, 0.2, 0.3)$. The variable step fourth-order Runge–Kutta method is used to simulate the system (2), which presents a double scroll chaotic attractor, and the complex topological structure of the attractor phase diagram is shown in Figure 2.

Figure 2. Attractor phase diagram: (a) x-y plane of new memristor chaotic system; (b) x-z plane; (c) y-z plane; (d) 3D chaotic attractor.

2.2. System Bifurcation and Maximum Lyapunov Exponent

The stability of the system will also change with the change of parameters, so the system will be in different states. The bifurcation diagram and the maximum Lyapunov exponential diagram can intuitively reflect the state of the system with the change of parameter values. The system parameters are fixed, and the initial state is selected as $(x, y, z) = (0.6, 0.2, 0.3)$. Figure 3a shows that when the parameter $c < 20$, the system (1) stays in a cycle, when the parameters $c \in [20, 28]$ system (1) is in a chaotic state, and when $c = 26$ in system (1) periodic window. Figure 3b embodies the bifurcation of system (2) effect, which can be seen from the diagram under the scope of a fixed system parameter c . Although the interval of the periodic window of the system (2) moves to the left, relative to the interval of the system (1), it increased the system (2) the bifurcation interval of chaotic state, thereby expanding the scope of the chaotic system parameters, which reflects the system (2) under the larger parameter range in a chaotic state.

Figure 3. System bifurcation: (a) system (1)'s bifurcation diagram; (b) bifurcation diagram of system (2).

Lyapunov exponent can determine whether the system is in a chaotic state. When a Lyapunov exponent of the system is greater than zero, the system is chaotic. The calculation of the maximum Lyapunov exponent of differential equations is complex. The algorithm for calculating the maximum Lyapunov exponent of differential equations proposed by

benettin G [26] is used to experiment with the above system. The maximum Lyapunov exponent of the system (1) is 2.51 when the parameter $c = 27.14$ is used. The maximum Lyapunov exponent of the system (2) is 2.994 when the parameter $c = 25.18$. As can be seen from Figure 4, the maximum Lyapunov exponent of the system (2) is much larger than that of the system (1) under a wide range of the parameter, and the separation speed of attractor phase-space orbit of system (2) is faster and the system is more chaotic.

Figure 4. Maximum Lyapunov exponent of system.

2.3. Multivariable Complexity Chaos Diagram

There are many methods to measure the complexity of time series, such as C0 complexity, spectral Sample Entropy (SE), Permutation Entropy (PE), and Multiscale Permutation Entropy (MPE) [27], etc. Among them, the MPE algorithm is the best choice to estimate the complexity of numerical sequence accurately and quickly. Based on the PE algorithm, the sequence is coarsely granular. The complexity measure values are obtained under different scale factor parameters. The larger the MPE value is, the more complex the time series is. To better grasp the complexity of the system from a macro perspective, the parameters $a \in [9, 36]$ and $c \in [22, 26]$ planes were divided into 251×251 points, and the MPE complexity at each point was calculated to obtain the multivariable complexity chaos diagram.

The MPE complexity of the system (1) and system (2) under parameter c is calculated respectively. Figure 5a shows that the complexity of the system (2) in the chaotic state interval is kept at $[0.9, 1]$, and the MPE complexity of the system (2) relative to the system (1) is kept at a high state range. As shown in Figure 5b,c, due to the system (2) periodic window near the parameters $c = 25$, there is a sharp fall in the number of single variable MPE complexity under the parameters. From Figure 5b, the local amplification of the figure, under the multivariable parameter range, forms a “sinking area”. This is consistent with the bifurcation and maximum Lyapunov exponential analysis of system (2), but does not affect the high complexity of the overall system (2).

Figure 5. Chaotic map of multivariable Multiscale Permutation Entropy (MPE) complexity: (a) system MPE complexity; (b) a–c plane of memristor chaotic system; (c) 3D-MPE chaotic map.

3. The Encryption Algorithm

The encryption algorithm is mainly divided into three parts: the main audio signal, compression de-noising, and audio image conversion process. The process of generating mask block and cipher block in memristor chaotic system involves interactive channel shuffle and overlapping diffusion encryption process. The algorithm encryption process design is shown as Figure 6.

Figure 6. Encryption flow chart.

3.1. Preliminaries

The pseudo-random sequence generated by the chaotic system is a floating-point number, which cannot be directly used in an encryption system. Therefore, the preprocessing of a chaotic sequence is the key to generating a random keystream. MATLAB uses the “audioread” function to read audio files and obtain audio data stream and audio sampling frequency. The value range of recorded voice signal is between $[-1, 1]$, and the effective value range of digital audio information is four decimal places. Using FWHT compression, a one-dimensional signal abandoned in pulse code modulation audio signal data of human hearing is not important, so choosing a suitable one according to the characteristics of audio data-adaptive coefficient of high-energy can reconstruct the original signal [12], which reduces the redundancy of audio signal. It can not only increase the storage and computing

power of a computer, but also improve the efficiency of audio encryption. Therefore, it is necessary to preprocess the audio signal.

3.1.1. Chaotic Sequence Preprocessing

Step 1 Set the initial value of the system $[x_0, y_0, z_0] = [0.98, 0.21, 0.46]$, iterate the system (1) M times, skip the initial state effect of the chaotic system, and then iterate $M \times N$ times to get the random sequence $x_i, y_i, z_i, i \in M \times N$. The sequence is processed as follows, receive x_i, y_i, z_i, w_i , as shown in formula (6).

$$\begin{cases} x_1(i) = \text{floor}((x_i + y_i + 100 \bmod 1) \times 10^{16}) \bmod 256 \\ y_1(i) = \text{floor}((x_i + z_i + 100 \bmod 1) \times 10^{16}) \bmod 256 \\ z_1(i) = \text{floor}((y_i + z_i + 100 \bmod 1) \times 10^{16}) \bmod 256 \\ w_1(i) = \text{floor}((x_i + y_i + z_i + 100 \bmod 1) \times 10^{16}) \bmod 256 \end{cases}, i \in [1, M \times N]. \quad (6)$$

where, the processing sequence of value in the range of 0–255, each sequence can be represented by a 64-bit binary number DB63–DB0; $\text{floor}(x)$ returns no greater than an integer value.

Step 2 The first eight bits selected x_i, y_i, z_i are used for the encryption algorithm. Three one-dimensional arrays $x_2(k), y_2(k), z_2(k)$ are obtained, that is $k \in [1, M \times N \times 8]$, each sequence value is represented by an 8-bit binary number. The related operations are as follows.

$$\begin{cases} x_2(1, k) = \text{bitget}(x_1(1, i), 9 - j) \\ y_2(1, k) = \text{bitget}(y_1(1, i), 9 - j) \\ z_2(1, k) = \text{bitget}(z_1(1, i), 9 - j) \end{cases}, j = 1, 2, \dots, 8. \quad (7)$$

3.1.2. Audio Signal Preprocessing

Step 1 Intercept audio. Take an $M \times N$ length Audio-channel (two-channel Audio).

Step 2 Compress and reduce noise.

(1) Firstly, FWHT transformation is carried out for audio left- and right-channel, respectively, so that most of the signal energy is concentrated at the lower column rate value.

$$\begin{cases} \text{single1}(i) = \text{fwht}(\text{Left}(i)) \\ \text{single2}(i) = \text{fwht}(\text{Right}(i)) \end{cases}, i \in M \times N. \quad (8)$$

(2) Based on the characteristics of the audio signal adaptive truncation of higher prevalence rate coefficient H , leaving $M \times N - H$ coefficient of signal energy is higher, can not only help to noise suppression but also can reduce the distortion of the audio signal.

$$\begin{cases} \text{single1}(H : \text{length}(\text{Left}(i))) = 0 \\ \text{single2}(H : \text{length}(\text{Right}(i))) = 0 \end{cases}, i \in M \times N. \quad (9)$$

(3) For the rest of the column rate coefficient of FWHT inverse transformation, after being reshaped the audio signal.

$$\begin{cases} \text{Le}(i) = \text{ifwht}(\text{single1}(i)) \\ \text{Rig}(i) = \text{ifwht}(\text{single2}(i)) \end{cases}, i \in M \times N. \quad (10)$$

Step 3 Enlarge and round the reconstructed audio signal at the same time to obtain u_1 and u_2 respectively. The related operations are as follows.

$$\begin{cases} u_1(i) = \text{round}(1 - \text{Le}(i) * 10^2) \\ u_2(i) = \text{round}(1 - \text{Rig}(i) * 10^2) \end{cases}, i \in M \times N. \quad (11)$$

where $\text{round}(x)$ means return the rounded integer value.

Step 4 Use the shape function to transform one-dimensional arrays u_1, w_1 and u_2 into numeric matrices R, G and B of size M by N , respectively.

Step 5 Raise the dimension of the number matrix. The cat function is used to take the digital matrices R , G and B as the “ R layer”, “ G layer” and “ B layer” of the color audio graph respectively to form a color audio graph with the size of $M \times N$. Related operations are as follows.

$$P = \text{cat}(3, R, G, B). \quad (12)$$

where, $\text{cat}(\cdot)$ stands for constructing multidimensional arrays, in this case, a 3D array is constructed.

3.2. The Encryption Process

3.2.1. Scrambling

Step 1 Convert the “ R layer”, “ G layer” and “ B layer” of the color audio diagram into a binary one-dimensional array respectively (the operation is the same as **Step 2** of Section 3.1.1) to get R' , G' , B' .

Step 2 To make the encryption algorithm related to the plaintext, the sum of the binary one-dimensional array R' , G' , B' is calculated respectively, which is used for right loop shift number, denoted as Sum_1 , Sum_2 , Sum_3 , in turn.

Step 3 The interactive channel shuffling operation is carried out for the binary 1D number group R' , G' , B' and R_2 , G_2 , B_2 is obtained.

$$\begin{cases} R_2 = \text{circshift}(R', [0, \text{Sum}_2]), \\ G_2 = \text{circshift}(G', [0, \text{Sum}_3]), \\ B_2 = \text{circshift}(B', [0, \text{Sum}_1]). \end{cases} \quad (13)$$

3.2.2. Shuffling

Step 1 According to Formula (14), the R_2 , G_2 , B_2 obtained after channel shuffling is carried out by overlapping for diffusion respectively, and stored in e_1 , e_2 , e_3 .

$$\begin{cases} e_1(1, k) = \text{bitxor}(\text{bitxor}(R_2(1, k), y_2(1, k)), z_2(1, k)) \\ e_2(1, k) = \text{bitxor}(\text{bitxor}(G_2(1, k), x_2(1, k)), z_2(1, k)) \\ e_3(1, k) = \text{bitxor}(\text{bitxor}(B_2(1, k), x_2(1, k)), y_2(1, k)) \end{cases}, k \in [1, M \times N \times 8] \quad (14)$$

Step 2 Convert e_1 , e_2 , e_3 to decimal array respectively to obtain $E_1(i)$, $E_2(i)$, $E_3(i)$, $i \in M \times N$.

Step 3 Store $E_1(i)$, $E_2(i)$, $E_3(i)$ in the size of E is $M \times N$, in turn, to obtain the final color ciphertext image E .

4. Experimental Simulation and Safety Analysis

The experimental environment is Matlab 2017a, with a 2.60 GHz Intel i7 processor and 8.0GB memory. To test the security performance of the algorithm, the key sensitivity, statistical characteristics, spectrum diagram, antidifferential attack ability, root mean square and peak factor, peak signal-to-noise ratio, and encryption efficiency are tested and analyzed, respectively. To reflect the effectiveness of the algorithm, four segments of audio with different storage sizes (MB) and different amplitudes are selected as the test objects for comparative analysis of the experimental results, as shown in Table 1.

Table 1 shows the experimental results of different types of audio after the encryption algorithm. To verify the effect of the algorithm, the semisilent period Audio 1, non-silent period Audio 3, intermittent silent period Audio 2, and Audio 4 are selected as the experimental objects of the algorithm. The results show that the time sequence diagram of ciphertext information after the encryption algorithm is evenly distributed, and there is almost no difference, indicating that the algorithm has a good encryption effect.

Figure 7 shows the effect of the algorithm after encryption and decryption. The algorithm can effectively encrypt the audio information and skillfully hide it in the color audio encryption diagram, which not only achieves the encryption effect but also confuses

the audio and visual of the attacker, greatly reducing the risk of audio information being cracked after the interception.

Table 1. Original information and encrypted information of different audio signals.

Filename	Size(MB)	Original Audio Waveform	Encrypted Graph
Audio 1	0.260
Audio 2	0.128
Audio 3	2.56
Audio 4	1.05

Figure 7. Compression and encryption of audio signal: (a) original audio diagram; (b) compressed audio signal; (c) noise suppression; (d) reshaped audio signal; (e) reconstructed audio signal; (f) color audiogram; (g) color encrypted audio map; (h) decrypt audio map.

4.1. Key Sensitivity Analysis

Key sensitivity analysis refers to the difference between two ciphertext audios obtained by encrypting the same audio when the key changes slightly. A good encryption system should have strong key sensitivity. Take Audio 1 as an example: minor changes in the three initial keys of the encryption algorithm will lead to incorrect decryption. The experimental results of the wrong key decryption and correct key decryption are shown in Figure 8.

As shown in Figure 8a–c can see, add 10^{-6} , 10^{-10} , 10^{-14} to the three initial keys *Key1*, *Key2*, *Key3* of the encryption algorithm to obtain the wrong decrypted audio. The result of correct key decryption is shown in Figure 8d. Experimental results show that the algorithm experiences very small changes in the key, the decrypted audio cannot reflect the original

audio signal, presents the state of audio noise completely, and there are many differences between the correct key to decrypt the audio. This indicates that the algorithm is highly sensitive to the key, has stronger sensitivity to the key, and can effectively resist brute force attacks.

Figure 8. Key sensitivity test: (a) Change Key 1; (b) change Key 2; (c) change Key 3; (d) Correct decryption.

4.2. Statistical Characteristic Analysis

This section mainly analyzes the statistical characteristics of audio ciphertext by histogram and correlation.

4.2.1. Histogram

Histogram can reflect the characteristics of statistical distribution before and after the original audio signal encryption, and select has a long silent period of Audio 1 as histogram analysis object and encrypted audio signal histogram. As shown in Figure 9b, the histogram distribution uniformity and good password encryption algorithm can spread to the silence of the audio area, presenting the irregular noise completely. This show that the algorithm can effectively adapt to different types of audio signal encryption and can better resist attacks of statistical analysis.

Figure 9. Histogram: (a) histogram of original audio signal; (b) histogram of encrypted audio signal.

4.2.2. Correlation Analysis

(i) Autocorrelation of the audio signal Autocorrelation is defined as the cross-correlation between the signal and itself. Table 2 describes the autocorrelation results of different types of audio signals. The following expression is used to calculate the autocorrelation of a given signal.

$$r_{XX}(\lambda) \triangleq E[\overline{X(i)}X(i + \lambda)]. \quad (15)$$

where, λ is the delay coefficient.

The autocorrelation of different types of test audio signals is shown in Table 2. The autocorrelation of the four encrypted signals are consistent, showing complete noise behavior. The autocorrelation diagrams of the original audio and decrypted audio are highly consistent with the waveform, and the autocorrelation diagrams of the two are consistent, indicating that the algorithm has a good encryption effect and can achieve lossless reconstruction.

Table 2. Autocorrelation of original audio, encrypted audio, and decrypted audio signals.

Filename	Original Audio Data	Encrypted Audio Data	Decrypted Audio Data
Audio 1	(a) Autocorrelation of the Original Audio 1	(b) Autocorrelation of the Encrypted Audio 1	(c) Autocorrelation of the Decrypted Audio 1
	(a) Autocorrelation of the Original Audio 2	(b) Autocorrelation of the Encrypted Audio 2	(c) Autocorrelation of the Decrypted Audio 2
	(a) Autocorrelation of the Original Audio 3	(b) Autocorrelation of the Encrypted Audio 3	(c) Autocorrelation of the Decrypted Audio 3
Audio 4	(a) Autocorrelation of the Original Audio 4	(b) Autocorrelation of the Encrypted Audio 4	(c) Autocorrelation of the Decrypted Audio 4

(ii) Correlation coefficient analysis of audio signal

One of the methods to evaluate the effectiveness of audio encryption algorithms is to calculate the Pearson correlation coefficients between adjacent samples (horizontal and vertical) before and after encryption. In general, the original audio adjacent signals have a high correlation, and a good encryption scheme can destroy the correlation between adjacent audio signals. Audio signals put into a random noise signal with a low correlation coefficient can achieve the desired encryption effect. The calculation formula of the correlation coefficient is as follows.

$$\begin{aligned}
 r_{xy} &= \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \\
 cov(x, y) &= \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)) \\
 D(x) &= \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2 \\
 E(x) &= \frac{1}{N} \sum_{i=1}^N x_i
 \end{aligned}
 \tag{16}$$

where x, y represents two adjacent audio samples and N represents the logarithm of the selected audio samples. To verify the effectiveness of the algorithm, given $N = 3000$, that is, 3000 pairs of adjacent audio samples are randomly selected. The correlation test results of the original audio and encrypted audio in the horizontal and vertical directions are shown in Table 3.

Table 3. Distribution of adjacent samples of original audio and encrypted audio in horizontal and vertical directions.

Table 3a,b shows the correlation distribution diagram of adjacent samples of original audio in horizontal and vertical directions, which is highly correlated in different directions, and the correlation coefficient in the vertical direction is almost 1. Table 3c,d shows the correlation distribution diagram of adjacent samples of encrypted audio in horizontal and vertical directions. The correlation distribution of the encrypted audio signal is uniform and irrelevant, which shows that this method can effectively reduce the correlation between adjacent samples of encrypted audio, achieve a good encryption effect, and has strong security.

Table 4 shows the correlation coefficients of the original audio and encrypted audio in the horizontal and vertical directions. The correlation coefficient of the encrypted audio in this paper is far lower than the optimal audio correlation coefficient in documents [28,29], indicating that the encryption scheme can effectively reduce the correlation between the original audio and the audio signal was effectively diffused.

Table 4. Correlation coefficient between raw audio and encrypted audio.

Filename	Original Audio		Encrypted Audio		Correlation Between Original and Encrypted Audio
	Horizontal	Vertical	Horizontal	Vertical	
Audio 1	0.9925	1.0000	−0.0012	4.5618×10^{-4}	0.0014
Audio 2	0.9668	1.0000	0.0013	4.5302×10^{-4}	0.0054
Audio 3	0.9921	1.0000	-3.2348×10^{-4}	−0.0026	−0.0051
Audio 4	0.9217	1.0000	0.0043	0.0016	0.0021
Reference [28]	0.9445	—	−0.0081	—	—
Reference [29]	0.9981	0.9981	−0.0094	0.0079	0.0056

4.3. Spectral Analysis

The spectrum diagram is created in the time domain signal by Fourier transform. It is a visual representation of the spectrum of audio frequency changing with time. The spectrum is represented by two geometric dimensions of time and frequency. In the time domain, the sampled data is decomposed into overlapping blocks, and Fourier transform is performed to calculate the spectrum size of each block. Different colors in the spectrum represent the decibels of audio signals at different times and frequencies. The dark blue area represents low decibels and the dark red area represents high decibels. The spectrum diagrams of the original audio, encrypted audio, and decrypted audio are shown in Table 5:

As shown in Table 5, in the spectrum diagram of the original audio, the distribution characteristics of high-decibels are consistent with the amplitude diagram of the original audio. The frequency spectrum of encrypted audio is evenly distributed, and all are high-decibel, which indicates that encrypted audio is high-decibel noise without obvious characteristics, and the audio signal was effectively spread. The declassified audio spectrum and the original audio spectrum have no obvious difference, and they keep the original audio signal in a different time and different frequency distribution characteristics of the volume. This shows that the algorithm for different types of encryption audio has a high degree of reduction, can undertake nondestructive reconstruction on the original audio, and embodies the safety and effectiveness of the algorithm.

Table 5. Spectrum diagram.

4.4. Antidifferential Attack Analysis

The antidifferential attack is one of the important indicators to measure the security of the encryption scheme. Encryption algorithm needs to be highly sensitive to plaintext information, that is, changing a data of audio signal and using the same initial key can get different ciphertext audio. Generally, the sensitivity of plaintext information is tested by indicators such as the Number of Sample Change Rate (*NSCR* [12,28,30]) and Unified Average Change Intensity (*UACI* [31]). Its definition is as follows.

$$NSCR = \sum_i \frac{D_i}{N_s} \times 100\% \quad (17)$$

$$UACI = \frac{1}{N_s} \left[\frac{\sum_i x_i - x'_i}{2^Q - 1} \right], D_i = \begin{cases} 1, & x_i \neq x'_i \\ 0, & x_i = x'_i \end{cases} \quad (18)$$

where, x_i and x'_i respectively represent two different ciphertext audio, N_s represents the length of the audio signal and Q represents the bit required to describe the audio.

Ideally, the theoretical values of sample number change rate and uniform average change intensity are close to 100% and 33.3333% respectively [12]. Under the same initial key, 1000 units of audio signal data are randomly extracted. By changing the lowest bit of these data, two audio with a small difference is encrypted with the help of an audio encryption system to obtain two corresponding ciphertext audio. The mean values of *NSCR* and *UACI* of these four different ciphertext audio are shown in Table 6. The change rate of sample number and unified average change intensity in Table 6 are closer to the theoretical value as a whole compared with that of the References [10,30,31], which proves that the algorithm has a strong sensitivity to plaintext audio and good resistance to differential attack.

Table 6. NSCR and UACI values.

Audio	NSCR	UACI
Audio 1	99.9268%	32.8195%
Audio 2	99.9695%	32.7827%
Audio 3	99.8062%	32.8285%
Audio 4	99.9786%	32.8661%
Reference [10]	99.9884%	30.2437%
Reference [31]	99.60812%	36.39705%
Reference [30]	99.996%	—

4.5. Root Mean Square (RMS) and Crest Factor (CF)

The Root Mean Square (RMS) value is measured as the average amplitude level of the audio signal. When the average value of the input signal is zero, the root means the square value is equal to the standard deviation. For the audio signal a with length, formula (19) is often used to calculate RMS:

$$RMS = \sqrt{\frac{1}{N_s} \sum_{i=1}^{N_s} |A_i|^2} \quad (19)$$

The Crest Factor (CF) [9,13,32] is a parameter of the waveform, such as Alternating Current (AC) or sound parameter, which represents the ratio of peak value to effective value, and is used to describe the extreme degree of peak value in the waveform. CF is defined as follows.

$$CF = 20 \log_{10} \frac{|A_{Peak}|}{A_{RMS}} \quad (20)$$

Table 7 shows the RMS and CF values of different audio signals. The table shows that the RMS and CF values of all encrypted audio are close to 0.6 and 3.4, respectively. Figure 10 is also used to demonstrate the RMS and CF values of the original audio and encrypted audio. The result proves that there is no statistical relationship between the original audio and the corresponding ciphertext audio. The value in the third row in Table 7 represents the lossless decryption of ciphertext audio, and the CF value of the encryption scheme is smaller than that in References [9,13], indicating that the spacing between peaks and troughs of ciphertext audio under this algorithm is small and that Ciphertext audio is evenly distributed and has high security.

Table 7. Root Mean Square (RMS) and Crest Factor (CF).

Audio	Size	RMS(dB)	CF(dB)	Lossless Reconstruction
Audio 1	260 KB	0.1389	10.5234	Yes
EAudio 1	260 KB	0.5701	3.4409	
DAudio 1	260 KB	0.1389	10.5234	
Audio 2	128 KB	0.0536	16.4115	Yes
EAudio 2	128 KB	0.5686	3.4499	
Audio 3	2.56 MB	0.1998	11.0925	Yes
EAudio 3	2.56 MB	0.5675	3.4563	
Audio 4	1.05 MB	0.0652	15.5818	Yes
EAudio 4	1.05 MB	0.5693	3.4453	
Reference [13]	918 KB	0.5786	4.7621	Yes
Reference [32]	—	$\cong 0.6$	—	No
Reference [9]	1.84 MB	0.6042	4.3754	Yes

Figure 10. Bar chart of *RMS* and *CF* values of original audio and encrypted audio. (a) *RMS* value (b) *CF* value.

4.6. Peak Signal-to-Noise Ratio and Encryption Efficiency

To determine the quality of the signal, people widely use two indicators [13,31,33,34] signal-to-noise ratio (*SNR*) and peak signal-to-noise ratio (*PSNR*). The signal-to-noise ratio is a measure of the noise content in the encrypted data signal. Cryptographic analysts always try to increase the noise to encrypt the content of the signal. The encrypted signal is masked by maximization, and the signal-to-noise ratio is greater than 0dB, indicating that the signal is clearer than the noise. For the encrypted audio file, a lower *PSNR* value is required, because it means that there is a high level of noise in the encrypted audio file, so it has a strong antiattack ability. The running time (s) and encryption speed (s/KB) values of four different types of audio encrypted using this scheme are listed in Table 8. *SNR* and *PSNR* between two different audio are defined as follows.

$$SNR = 10 * \log_{10} \frac{\sum_{i=1}^{N_s} x_i^2}{\sum_{i=1}^{N_s} (x_i - y_i)^2} \quad (21)$$

$$PSNR = 10 * \log_{10} \left(\frac{MAX^2}{MSE} \right) \quad (22)$$

where mean-square Error (*MSE*) of data streams is stored in vectors and calculated as follows.

$$MSE = \frac{1}{N_s} \sum_{i=1}^{N_s} (x(i) - y(i))^2 \quad (23)$$

where x_i represents the original audio, y_i represents the encrypted audio, N_s represents the length of the audio signal, and *MAX* represents the maximum value in the data stream.

Table 8. *SNR*, *PSNR* and Encryption efficiency.

Audio	Size	SNR (dB)	PSNR (dB)	Total (s)	Speed (s/KB)
Audio 1	260 KB	−12.5183	4.6302	0.636433	0.002448
Audio 2	128 KB	−20.5570	4.8659	0.326567	0.002551
Audio 3	2.56 MB	−9.5699	4.4186	5.342500	0.002087
Audio 4	1.05 MB	−18.8850	4.8346	2.531556	0.002411
Reference [13]	304 KB	−28.1400	4.3100	58.63000	0.190000
Reference [34]	439 KB	−22.139432	4.7500	1.176000	0.002679

Table 8 calculates the *SNR* value, *PSNR* value, encryption running time, and encryption speed of ciphertext audio. The average value of *SNR*(dB) is −15.38255, the average value of *PSNR*(dB) is 4.687325, and the average encryption speed of the algorithm is 0.0023745. The table shows that the low negative value of *SNR* and the low positive value of *PSNR* indicate the high level of noise in the ciphertext audio, both of which lead to the destruction of the coherence of the original audio; in addition, the running time of the encryption algorithm is positively correlated with the size of the audio file. Compared with that of the

Reference [13], the encryption speed of the algorithm is greatly improved, and the overall index is more secure and efficient compared with the encryption scheme in Reference [34].

5. Conclusions

In this paper, a digital audio encryption scheme based on a new Chen memristor chaotic system is proposed to resist various traditional signal attacks. Chen memristor chaotic system based on magnetron titanium dioxide memristor enhances the robustness of the original chaotic system, expands the parameter range of the system effectively, and further increases the keyspace of the algorithm. In addition, the Fast Walsh–Hadamard Transform (FWHT) is introduced to adaptively compress, denoise, and reconstruct the audio signal, which effectively reduces the audio redundancy and the overall cost of computer storage and running time. In the stage of interactive channel shuffling and overlapping diffusion encryption associated with plaintext, the user holding the correct key can start the encryption algorithm to skillfully convert the 1D audio signal into a 2D digital image matrix for encryption, so that the algorithm has a double-layer security effect. In this paper, four different types of audio files are tested to verify the feasibility and effectiveness of the encryption algorithm. Experimental results show that the performance of the algorithm is better than the above audio encryption algorithm. At the same time, it also provides a certain reference for the application of the combination of adaptive audio compression denoising theory and chaos theory in the field of communication security.

In some audio encryption algorithms, the ciphertext audio is usually stored and transmitted in the form of noise. Assuming that the attacker has access to the decryption system (i.e., select ciphertext attack), but the decryption key is safely embedded in the device and cannot be obtained, at this time, the key can be inferred by decrypting a large number of selected ciphertexts and using the generated plaintext. In future work, we intend to further study the enhanced chaotic system. Multiple chaotic systems are used as the cipher generator of the algorithm to make it have a huge keyspace. Secondly, transform the transmission form of ciphertext audio to provide the algorithm with higher security.

Author Contributions: W.D. and X.X. wrote the manuscript; G.L. and X.S. performed the literature review; and X.S. submitted the manuscript to the journal. All authors have read and agreed to the published version of the manuscript.

Funding: The work presented is supported by the financial supports given by the research outlay item: the Xinjiang Uygur Autonomous Region Natural Science Fund(2017D01A24), the Xinjiang University of Finance and Economics Fund (Grant: 2019XTD002), and a grant from Science and Technology Department of Sichuan province (No. 2020YFG0300).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare that this research was conducted in the absence of any commercial or financial relationships that may be construed as a potential conflict of interest.

References

1. Tang, S.; Jiang, Y.; Zhang, L.; Zhou, Z. Audio Steganography with AES for Real-Time Covert Voice over Internet Protocol Communications. *Sci. China Inf. Sci.* **2014**, *57*, 1–14. [CrossRef]
2. Shakir, H.R. An Image Encryption Method Based on Selective AES Coding of Wavelet Transform and Chaotic Pixel Shuffling. *Multimed. Tools Appl.* **2019**, *78*, 26073–26087. [CrossRef]
3. Gambhir, A.; Arya, R. Performance Analysis of DES Algorithm and RSA Algorithm with Audio Steganography. In Proceedings of the International Conference on Communication and Signal Processing 2016 (iccasp 2016), Lonere, India, 26–27 December 2016; Iyer, B., Nalbalwar, S.L., Pawade, R.S., Eds.; Atlantis Press: Paris, France, 2017; Volume 137, pp. 333–340.
4. Nasution, A.B.; Efendi, S.; Suwilo, S. Image Steganography In Securing Sound File Using Arithmetic Coding Algorithm, Triple Data Encryption Standard (3DES) and Modified Least Significant Bit (MLSB). In Proceedings of the International Conference on Mechanical, Electronics, Computer, and Industrial Technology, Prima, Indonesia, 6–8 December 2017; Iop Publishing Ltd.: Bristol, UK, 2018; Volume 1007, p. 012010.

5. Idrees, B.; Zafar, S.; Rashid, T.; Gao, W. Image Encryption Algorithm Using S-Box and Dynamic Henon Bit Level Permutation. *Multimed. Tools Appl.* **2020**, *79*, 6135–6162. [\[CrossRef\]](#)
6. Zhu, S.; Wang, G.; Zhu, C. A Secure and Fast Image Encryption Scheme Based on Double Chaotic S-Boxes. *Entropy* **2019**, *21*, 790. [\[CrossRef\]](#)
7. Singh, A.; Agarwal, P.; Chand, M. Image Encryption and Analysis Using Dynamic AES. In Proceedings of the 2019 5th International Conference on Optimization and Applications (ICOA), Kenitra, Morocco, 25–26 April 2019; pp. 1–6.
8. Arab, A.; Rostami, M.J.; Ghavami, B. An Image Encryption Method Based on Chaos System and AES Algorithm. *J. Supercomput.* **2019**, *75*, 6663–6682. [\[CrossRef\]](#)
9. Abdelfatah, R.I. Audio Encryption Scheme Using Self-Adaptive Bit Scrambling and Two Multi Chaotic-Based Dynamic DNA Computations. *IEEE Access* **2020**, *8*, 69894–69907. [\[CrossRef\]](#)
10. Shah, D.; Shah, T.; Jamal, S.S. Digital Audio Signals Encryption by Mobius Transformation and Henon Map. *Multimedia Syst.* **2020**, *26*, 235–245. [\[CrossRef\]](#)
11. Zhao, H.; Xie, S.; Zhang, J.; Wu, T. A Dynamic Block Image Encryption Using Variable-Length Secret Key and Modified Henon Map. *Optik* **2021**, *230*, 166307. [\[CrossRef\]](#)
12. Farsana, F.J.; Devi, V.R.; Gopakumar, K. An Audio Encryption Scheme Based on Fast Walsh Hadamard Transform and Mixed Chaotic Keystreams. *Appl. Comput. Informatics* **2020**, ahead-of-print. [\[CrossRef\]](#)
13. Naskar, P.K.; Paul, S.; Nandy, D.; Chaudhuri, A. DNA Encoding and Channel Shuffling for Secured Encryption of Audio Data. *Multimed. Tools Appl.* **2019**, *78*, 25019–25042. [\[CrossRef\]](#)
14. Noshadian, S.; Ebrahimzade, A.; Kazemitabar, S.J. Breaking a Chaotic Image Encryption Algorithm. *Multimed. Tools Appl.* **2020**, *79*, 25635–25655. [\[CrossRef\]](#)
15. Deng-Wei, Y.; Li-Dan, W.; Shu-Kai, D. Memristor-based multi-scroll chaotic system and its pulse synchronization control. *Acta Phys. Sin.* **2018**, *67*, 110502. [\[CrossRef\]](#)
16. Bo-Cheng, B.; Jian-Ping, X.; Zhong, L. Initial State Dependent Dynamical Behaviors in a Memristor Based Chaotic Circuit. *Chin. Phys. Lett.* **2010**, *27*, 070504. [\[CrossRef\]](#)
17. Ma, X.; Mou, J.; Liu, J.; Ma, C.; Yang, F.; Zhao, X. A Novel Simple Chaotic Circuit Based on Memristor-Memcapacitor. *Nonlinear Dyn.* **2020**, *100*, 2859–2876. [\[CrossRef\]](#)
18. Chen, J.-J.; Yan, D.-W.; Duan, S.-K.; Wang, L.-D. Memristor-Based Hyper-Chaotic Circuit for Image Encryption. *Chin. Phys. B* **2020**, *29*, 110504. [\[CrossRef\]](#)
19. Peng, G.; Min, F. Multistability Analysis, Circuit Implementations and Application in Image Encryption of a Novel Memristive Chaotic Circuit. *Nonlinear Dyn.* **2017**, *90*, 1607–1625. [\[CrossRef\]](#)
20. Kamal, F.M.; Elsonbaty, A.; Elsaid, A. A Novel Fractional Nonautonomous Chaotic Circuit Model and Its Application to Image Encryption. *Chaos Solitons Fractals* **2021**, *144*, 110686. [\[CrossRef\]](#)
21. Akgul, A.; Rajagopal, K.; Durdu, A.; Pala, M.A.; Boyraz, Ö.F.; Yildiz, M.Z. A Simple Fractional-Order Chaotic System Based on Memristor and Memcapacitor and Its Synchronization Application. *Chaos Solitons Fractals* **2021**, *152*, 111306. [\[CrossRef\]](#)
22. Yan, D.; Wang, L.; Duan, S.; Chen, J.; Chen, J. Chaotic Attractors Generated by a Memristor-Based Chaotic System and Julia Fractal. *Chaos Solitons Fractals* **2021**, *146*, 110773. [\[CrossRef\]](#)
23. Xu, X.; Li, G.; Dai, W. Multi-direction Chain and Grid Chaotic System based on Julia Fractal. *Fractals* **2021**. [\[CrossRef\]](#)
24. Wang, L.; Drakakis, E.; Duan, S.; He, P.; Liao, X. Memristor Model and Its Application for Chaos Generation. *Int. J. Bifurcation Chaos* **2012**, *22*, 1250205. [\[CrossRef\]](#)
25. Chen, G.R.; Ueta, T. Yet Another Chaotic Attractor. *Int. J. Bifurcation Chaos* **1999**, *9*, 1465–1466. [\[CrossRef\]](#)
26. Benettin, G.; Galgani, L.; Strelcyn, J.-M. Kolmogorov Entropy and Numerical Experiments. *Phys. Rev. A* **1976**, *14*, 2338–2345. [\[CrossRef\]](#)
27. Chun-Ling, F.; Ning-De, J.; Xiu-Ting, C.; Zhong-Ke, G. Multi-Scale Permutation Entropy: A Complexity Measure for Discriminating Two-Phase Flow Dynamics. *Chin. Phys. Lett.* **2013**, *30*, 090501. [\[CrossRef\]](#)
28. Ghasemzadeh, A.; Esmaili, E. A Novel Method in Audio Message Encryption Based on a Mixture of Chaos Function. *Int. J. Speech Technol.* **2017**, *20*, 829–837. [\[CrossRef\]](#)
29. Babu, N.R.; Kalpana, M.; Balasubramaniam, P. A Novel Audio Encryption Approach via Finite-Time Synchronization of Fractional Order Hyperchaotic System. *Multimed. Tools Appl.* **2021**, *80*, 18043–18067. [\[CrossRef\]](#)
30. Kordov, K. A Novel Audio Encryption Algorithm with Permutation-Substitution Architecture. *Electronics* **2019**, *8*, 530. [\[CrossRef\]](#)
31. Parvees, M.Y.M.; Samath, J.A.; Bose, B.P. Audio Encryption—A Chaos-Based Data Byte Scrambling Technique. *Int. J. Appl. Syst. Stud.* **2018**, *8*, 51–75.
32. Wang, X.; Su, Y. An Audio Encryption Algorithm Based on DNA Coding and Chaotic System. *IEEE Access* **2020**, *8*, 9260–9270. [\[CrossRef\]](#)
33. Li, X.; Yu, H.; Zhang, H.; Jin, X.; Sun, H.; Liu, J. Video Encryption Based on Hyperchaotic System. *Multimed. Tools Appl.* **2020**, *79*, 23995–24011. [\[CrossRef\]](#)
34. Naskar, P.K.; Bhattacharyya, S.; Chaudhuri, A. An Audio Encryption Based on Distinct Key Blocks along with PWLCM and ECA. *Nonlinear Dyn.* **2021**, *103*, 2019–2042. [\[CrossRef\]](#)