Chaos, Solitons and Fractals 165 (2022) 112770

Contents lists available at ScienceDirect

Chaos, Solitons and Fractals

journal homepage: www.elsevier.com/locate/chaos

AEA-NCS: An audio encryption algorithm based on a nested chaotic system

Rui Wu [a], Suo Gao [a,*], Xingyuan Wang [b], Songbo Liu [a], Qi Li [b], Uğur Erkan [c], Xianglong Tang [a]

[a] School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China
[b] School of Information Science and Technology, Dalian Maritime University, Dalian 116026, China
[c] Department of Computer Engineering, Faculty of Engineering, Karamanoglu Mehmetbey University, 70200 Karaman, Turkey

ARTICLE INFO

Keywords:
Chaos
Chaotic cryptography
Audio encryption
Bifurcation

ABSTRACT

Audio information strongly correlates in adjacent times, and the data type of the audio is float, so the traditional encryption algorithms for the image are unsuitable for audio encryption. This paper proposes an audio encryption algorithm based on Chaos, named AEA-NCS. Most 1D maps have a control parameter, and the parameter space in the chaotic state is small. Therefore, a 2D-Logistic-nested-infinite-collapse (2D-LNIC) is proposed by combining an infinite collapse map (1D-ICM) and a logistic map. There are two control parameters in 2D-LNIC, and it exhibits good chaotic performance through the Lyapunov exponent and attractor phase diagram. In the audio encryption algorithm, 2D-LNIC generates the keystream, and the encryption algorithm is a process of scrambling and diffusion simultaneously. This structure increases the security of the algorithm. We evaluate AEA-NCS in ESC-50, and the evaluation results show that AEA-NCS exhibits good performance, significantly reducing the correlation of audio information in adjacent times.

1. Introduction

With the rapid development of Internet technology, multimedia information such as images, audio, and texts can be exchanged frequently in an open and shared environment, which also exposes many information security problems [1–4]. Many multimedia information protection methods have been proposed, such as watermarking technology, encryption technology, steganography technology, etc. [5–8]. Among them, encryption technology is one of the most widely used technologies [9–11].

Chaos is widely used in cryptography due to its pseudo-randomness, sensitivity to initial values, etc. [12–15]. Nowadays, multimedia information encryption algorithms combined with chaos theory have been widely used and achieved good results [16–19]. For example, Yahi et al. proposed an Enhanced chaotic map inspired by the cubic map [20]. They analyzed the dynamic behavior of this system and showed good performance in image encryption. Midoun et al. proposed a 1-DFCS and used 1-DFCS to generate the keystream required by the cryptosystem [21]. Most one-dimensional chaotic systems have one parameter, and the parameter space in the chaotic state is discontinuous, resulting in small available parameter space in cryptosystems. In addition, as reported in Ref. [22], the trajectory of some one-dimensional systems can be predicted. In this paper, we combine two existing one-dimensional chaotic systems [23,24] and propose a two-dimensional chaotic system named 2D-Logistic-nested-infinite-collapse (2D-LNIC), this system has two control parameters, and the parameter space in the chaotic state is larger and continuous.

Image is considered the most intuitive multimedia tool to convey information [25–28]. However, in many scenarios, audio information occupies a more critical position. For example, it is possible to study the laws of auroral activity using the infrasound waves produced by the aurora. Ensuring the safe transmission of this audio information on the Internet is an urgent problem to be solved [29–31]. Gnanajeyaraman et al. constructed a chaotic lookup table and applied it to audio encryption using the blockchain model. The algorithm is difficult to implement and has many limitations [32]. Dai et al. proposed a Chen Memristor chaotic system. They analyzed its dynamic behavior and used this system for audio encryption. In the encryption system, scrambling and diffusion were used separately. The encryption effect is good, but the key space of the cryptosystem is small (only three initial keys), so it is easy to crack the algorithm using brute force attacks [33]. El et al. [34] and Abdelfatah [35] applied DNA encoding technology to audio encryption. Although this technology improves the algorithm's security, the efficiency is slow. Wang and Su proposed an audio encryption algorithm using PWLCM to generate a keystream, in which DNA encoding and decoding are used [36]. Although the experimental results are good, PWLCM has only one control parameter and needs to use PWLCM multiple times to generate the keystream. In addition, the scrambling and diffusion separation encryption algorithm

* Corresponding author.
E-mail address: gaosuo@stu.hit.edu.cn (S. Gao).

https://doi.org/10.1016/j.chaos.2022.112770
Received 28 July 2022; Received in revised form 22 September 2022; Accepted 30 September 2022
Available online 18 October 2022

proposed by Feistel [37] is considered to have security flaws. Solak et al. cracked this separate scrambling, and diffusion structure using the chosen ciphertext attack method utilizing an influence network [38]. Then Xie et al. pointed out the shortcomings in Sorak's algorithm, and they improved the attack algorithm [39]. Naskar et al. proposed a new audio encryption algorithm using DNA Encoding and a logistic map, and the same problem occurs in their algorithm, which requires multiple uses of a logistic map to generate a keystream [40]. In this paper, we propose an audio encryption algorithm based on 2D-LNIC. The scrambling and diffusion of AEA-NCS are performed simultaneously. This structure increases the security of the algorithm. The algorithm is very efficient with a large key space.

In summary, we make the following three significant contributions:

1. A 2D-LNIC is proposed, and its dynamic behavior is analyzed.

2. An audio encryption algorithm named AEA-NCS is proposed based on 2D-LNIC.

3. Experimental analysis shows that AEA-NCS exhibits good performance.

The remaining organizational structure of this paper is described as follows. In the second section, 2D-LNIC is introduced, and the parameter space in a hyperchaotic state is analyzed. The third section describes the proposed audio encryption algorithm based on 2D-LNIC. The fourth section uses indicators to evaluate the AEA-NCS and to compare it with existing algorithms. The fifth section concludes this paper.

2. 2D-Logistic-nested-infinite-collapse (2D-LNIC)

There is only one control parameter in the 1D-ICM and Logistic map, and the chaotic system's parameter space determines the cryptosystem's parameter space. To increase the parameter space of chaotic systems, a 2D-Logistic-nested-infinite-collapse (2D-LNIC) is proposed by combining 1D-ICM and a Logistic map. Compared with 1D-ICM and Logistic Map, 2D-LNIC has two parameters, so the parameter space of 2D-LNIC is larger. Besides, 2D-LNIC is a hyperchaotic system that has better dynamic behavior. The mathematical expression of the 1D-ICM is,

$$f(\mu_1, x_n) = x_{n+1} = \sin(\frac{\mu_1}{x_n}). \tag{1}$$

The mathematical expression of the Logistic map is,

$$g(\mu_2, y_n) = y_{n+1} = \mu_2 y_n(1 - y_n). \tag{2}$$

The mathematical expression of the 2D-LNIC is,

$$L_{2D-LNIC}(\mu_1, \mu_2, x_n, y_n) = \begin{cases} x_{n+1} = \mu_2 \sin(\frac{\mu_1}{y_n})(1 - \sin(\frac{\mu_1}{x_n})) \\ y_{n+1} = \sin(\frac{\mu_1}{\mu_2 x_n(1-y_n)}) \end{cases}. \tag{3}$$

where μ_1 ($\mu_1 > 0$) and μ_2 ($\mu_2 > 0$) are control parameters, the nth iteration states are x_n and y_n. x_0 and y_0 are the initial values of 2D-LNIC.

2.1. Lyapunov exponent (LE)

The Lyapunov exponent is a common method to test whether a nonlinear dynamical system is in a chaotic state. Lyapunov exponents of 2D-LNIC are shown in Fig. 1.

As shown in Fig. 1, when $\mu_2 = 1$, 2D-LNIC presents a periodic state at $\mu_1 \in (0, 0.86)$, and a hyperchaotic state at $\mu_1 \in (0.86, +\infty)$ which is shown in Fig. 1(a). When $\mu_2 = 2$, the three states appear alternately (chaos state, hyperchaotic state, periodic state) at $\mu_1 \in (0, 0.51)$, and at $\mu_1 \in (0.51, +\infty)$, 2D-LNIC presents a stable hyperchaotic state which is shown in Fig. 1(b). When $\mu_2 = 2.7$, 2D-LNIC presents a stable hyperchaotic state at $\mu_1 \in (0, +\infty)$ which are shown in Fig. 1(e). With the gradual increase of μ_2, the 2D-LNIC always maintains a stable hyperchaotic state at $\mu_1 \in (0, +\infty)$ which are shown in Figs. 1(f), 1(g) and 1(h).

Table 1
Description of audio information.

Filename	Category	FS	The length of audio
1-97392-A-0.wav	dog	44 100	220 500
1-110389-A-0.wav	dog	44 100	220 500
1-115920-A-22.wav	clapping	44 100	220 500
1-11687-A-47.wav	airplane	44 100	220 500
1-119125-A-45.wav	train	44 100	220 500
1-121951-A-8.wav	sheep	44 100	220 500
1-12654-A-15.wav	water_drops	44 100	220 500
1-208757-A-2.wav	pig	44 100	220 500
1-34094-A-5.wav	cat	44 100	220 500

It can be seen from Fig. 1 that with the increase of μ_1, LE1 and LE2 show an upward trend, and their values are always greater than 0. Therefore, the system presents a hyperchaotic state at this time . For the convenience of illustration, we only show the Lyapunov exponents of 2D-LNIC in the interval $[0, 20]$.

The bifurcation diagram corresponds to the Lyapunov exponent, but the bifurcation diagram cannot show the hyperchaotic behavior of the system. The bifurcation diagram of 2D-LNIC is shown in Fig. 2. To avoid the appearance of the period window, in the cryptosystem, the parameter range for selecting 2D-LNIC are $\mu_2 \in (2.7, 100]$ and $\mu_1 \in (0, 100]$.

2.2. Attractor phase diagram

The attractor phase diagram is a description of the trajectory produced by a nonlinear dynamical system. The attractor phase diagrams of 2D-LNIC are shown in Fig. 3.

As shown in Fig. 3, the attractor trajectories of 2D-LNIC is uniformly distributed throughout the phase space. Therefore, the new system has good chaotic properties.

2.3. 0–1 Test

The 0–1 test can determine both regular and chaotic motion by computing a parameter K that is asymptotically close to zero or one. The 0–1 test graph of chaotic motion presents Brownian motion. The 0–1 test results of 2D-LNIC are shown in Fig. 4.

As shown in Figs. 4(a) and 4(b), when the parameter $\mu_2 = 1$ and $\mu_1 = 0.5$, the 2D-LNIC presents a regular motion state, and their motion trajectory is a ring, which verifies the Lyapunov exponent under this parameter state (Fig. 1(a)). The rest of the diagrams show the Brownian motion state presented by the system, where the system is chaotic and can produce unpredictable random sequences.

3. Description of the ESC-50 dataset

We evaluate AEA-NCS on the ESC-50 dataset (github.com/karolpiczak/ESC-50), and the audio files are in .wav format. The reason for mapping the ciphertext value of the audio to the interval $[0, 255]$ is that the distribution of the image pixel value is $[0, 255]$, and the performance of AEA-NCS can be evaluated by the evaluation index of the image. The description of the audio information are shown in Table 1 and Fig. 5.

4. Description of AEA-NCS

4.1. Description of encryption algorithm

AEA-NCS is a symmetric encryption algorithm. The secret key is generated by Hash256 and the scrambling and diffusion algorithms are carried out at the same time. This structure increases the security of the algorithm. The attacker needs to crack the scrambling and diffusion algorithms at the same time. AEA-NCS is described as follow,

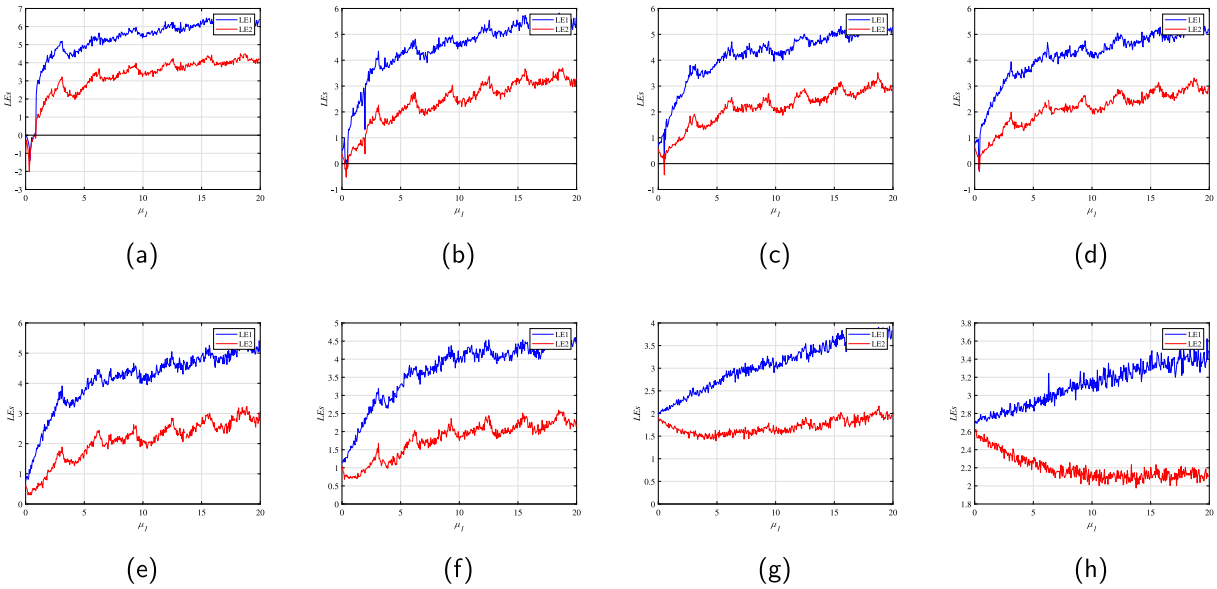

Fig. 1. Lyapunov exponents of 2D-LNIC. (a) $\mu_2 = 1$. (b) $\mu_2 = 2$. (c) $\mu_2 = 2.5$. (d) $\mu_2 = 2.6$. (e) $\mu_2 = 2.7$. (f) $\mu_2 = 4$. (g) $\mu_2 = 10$. (h) $\mu_2 = 20$.

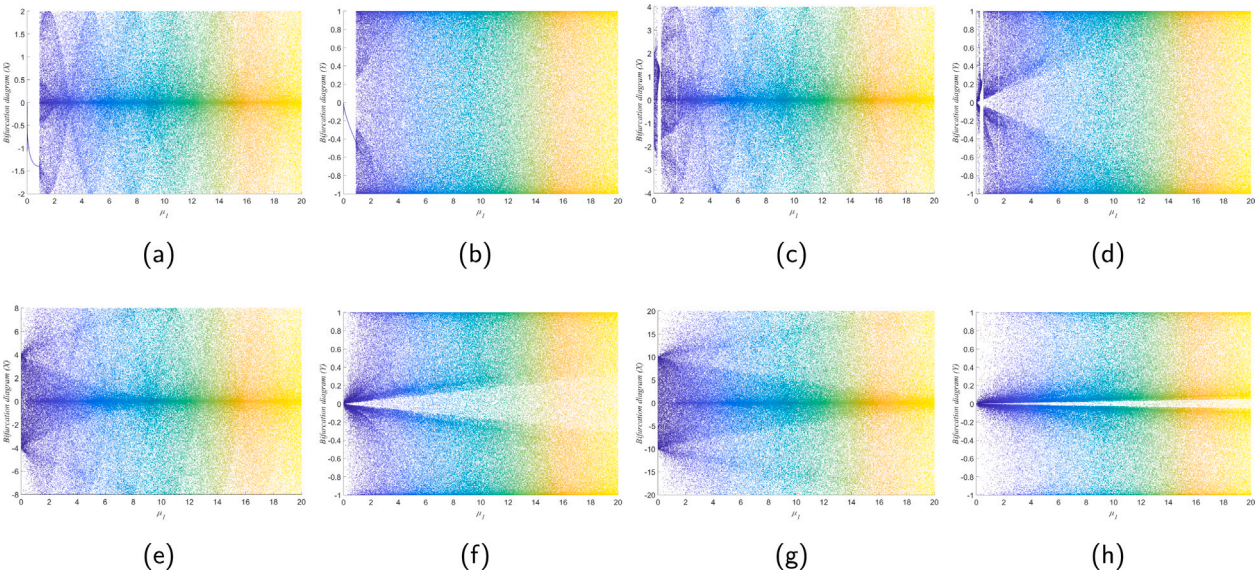

Fig. 2. Bifurcation diagrams of 2D-LNIC. (a) $\mu_2 = 1$ (Sequence X). (b) $\mu_2 = 1$ (Sequence Y). (c) $\mu_2 = 2$ (Sequence X). (d) $\mu_2 = 2$ (Sequence Y). (e) $\mu_2 = 4$ (Sequence X). (f) $\mu_2 = 4$ (Sequence Y). (g) $\mu_2 = 10$ (Sequence X). (h) $\mu_2 = 10$ (Sequence Y).

Input: A (A is an audio information, and the length of A is L)

Step 1: The value range of A is $[\min A, \max A]$, obtain the new A by

$$NA = A \times \frac{255}{\max A - \min A} + \min A \times \frac{255}{\min A - \max A}. \tag{4}$$

The value range of NA is $[0, 255]$.

Step 2: Integer part of the audio is NA_1 ($NA_1 = floor(NA)$), fractional part of the audio is NA_2 ($NA_2 = NA - NA_1$).

Step 3: Obtain the key K of AEA-NCS by Hash256, A is the input of Hash256, K is 256bits. Divide K into 8 equal parts, each containing 32 bits, and convert to decimal. The secret keys of the cryptosystem are

$$\begin{cases} k_1 = K(1:32) \oplus K(33:64)/2^{32}, \\ k_2 = K(65:96) \oplus K(97:128)/2^{32}, \\ k_3 = K(129:160) \oplus K(161:192)/2^{32} \times 100 + 4, \\ k_4 = K(193:224) \oplus K(225:256)/2^{32} \times 100. \end{cases} \tag{5}$$

Step 4: Obtain the keystreams X and Y by 2D-LNIC,

$$\begin{cases} X: x_{n+1} = \mu_2 \sin(\mu_1/y_n)(1 - \sin(\mu_1/x_n)) \\ Y: y_{n+1} = \sin(\mu_1/\mu_2 x_n(1 - y_n)) \end{cases} \tag{6}$$

where $x_0 = k_1$, $y_0 = k_2$, $\mu_1 = k_4$, and $\mu_2 = k_3$. The length of X is L and the length of Y is L.

Step 5: Obtain the interference matrix S by

$$S = \mathrm{mod}(floor(X \times 10^{10}), 256). \tag{7}$$

Step 6: Obtain the sort matrix G, where G_i meets the condition that $G_i < G_{i+1}$ and $G_i \in Y$ $(i = 1, 2, 3, \ldots, L)$.

Step 7: The first three values of the ciphertext are

$$\begin{cases} C[G(1)] = NA_1(1) + S(1) \bmod 256, \\ C[G(2)] = NA_1(2) + S(1) + C[G(1)] \bmod 256, \\ C[G(3)] = NA_1(3) + S(1) + C[G(1)] + C[G(2)] \bmod 256. \end{cases} \tag{8}$$

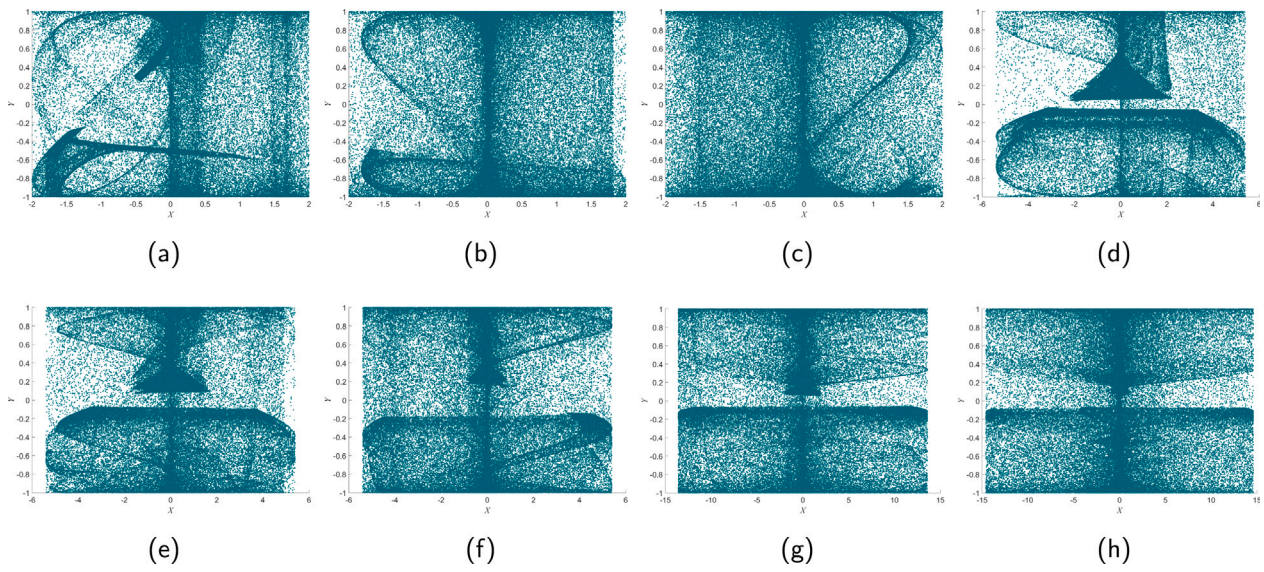

Fig. 3. Attractor phase diagram of 2D-LNIC. (a) $\mu_1 = 1$ and $\mu_2 = 1$. (b) $\mu_1 = 2$ and $\mu_2 = 1$. (c) $\mu_1 = 4$ and $\mu_2 = 1$. (d) $\mu_1 = 1$ and $\mu_2 = 2.7$. (e) $\mu_1 = 2$ and $\mu_2 = 2.7$. (f) $\mu_1 = 4$ and $\mu_2 = 2.7$. (g) $\mu_1 = 10.9$ and $\mu_2 = 6.8$. (h) $\mu_1 = 15.4$ and $\mu_2 = 7.3$.

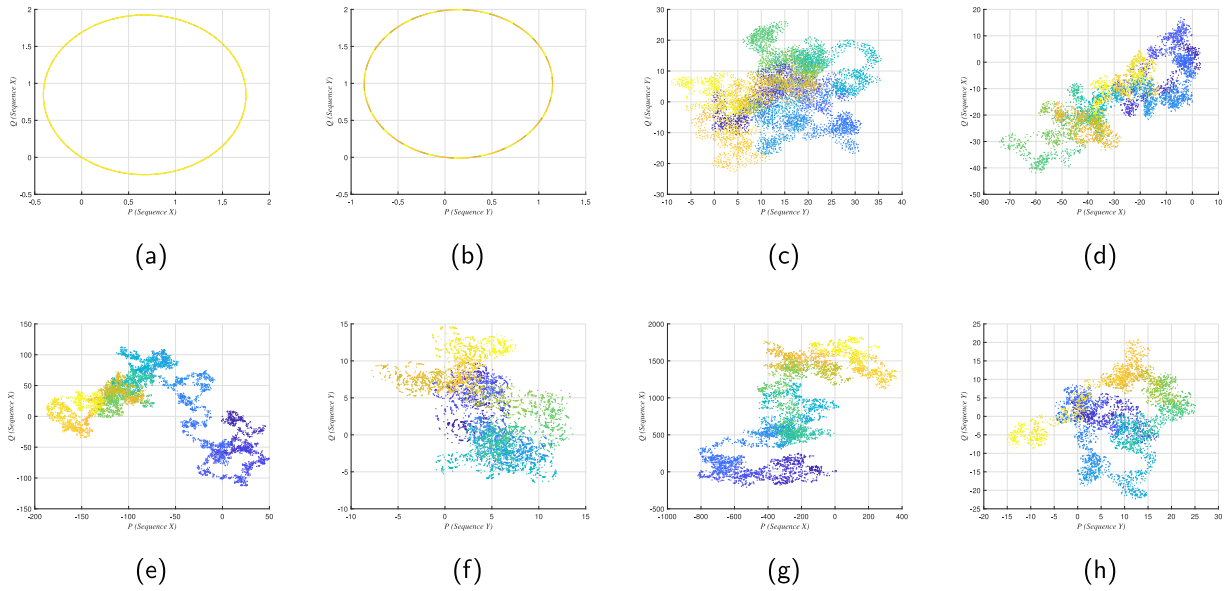

Fig. 4. 0-1 test. (a) $\mu_2 = 1$ and $\mu_1 = 0.5$ (Sequence X). (b) $\mu_2 = 1$ and $\mu_1 = 0.5$ (Sequence Y). (c) $\mu_2 = 1$ and $\mu_1 = 2$ (Sequence X). (d) $\mu_2 = 1$ and $\mu_1 = 2$ (Sequence Y). (e) $\mu_2 = 2.7$ and $\mu_1 = 0.5$ (Sequence X). (f) $\mu_2 = 2.7$ and $\mu_1 = 0.5$ (Sequence Y). (g) $\mu_2 = 20$ and $\mu_1 = 20$ (Sequence X). (h) $\mu_2 = 20$ and $\mu_1 = 20$ (Sequence Y).

Step 8: The rest values of the ciphertext are

$$f_1 = floor((3.999 + k_1/10^5) \times C[G(i-1)]/256 \times (1 - C[G(i-1)]/256) \times 10^{10}) \bmod 256.$$

$$f_2 = floor((3.999 + k_2/10^6) \times C[G(i-1)]/256 \times (1 - C[G(i-2)]/256) \times 10^{10}) \bmod 256.$$

$$C[G(i)] = NA_1(i) + f_1 + f_2 + S(i) \bmod 256.$$

Step 9: Obtain the ciphertext C ($C = C + NA_2$).

Output: C

4.2. Description of decryption algorithm

The decryption algorithm is shown in Algorithm 1.

5. Performance analysis

5.1. Simulation experiments

The encryption results and decryption results of audios are shown in Figs. 6 and 7. Visually, AEA-NCS shows good performance, the ciphertext becomes random noise, and the amplitude distribution is uniform.

5.2. Differential attack analysis

The attacker observes the difference between the original ciphertext and the new ciphertext by changing the information of the original audio (minor changes). This type of attack is called a differential attack. In data encryption, NSCR and UACI are used to evaluate the ability of the encryption algorithm to resist differential attacks. Their calculation

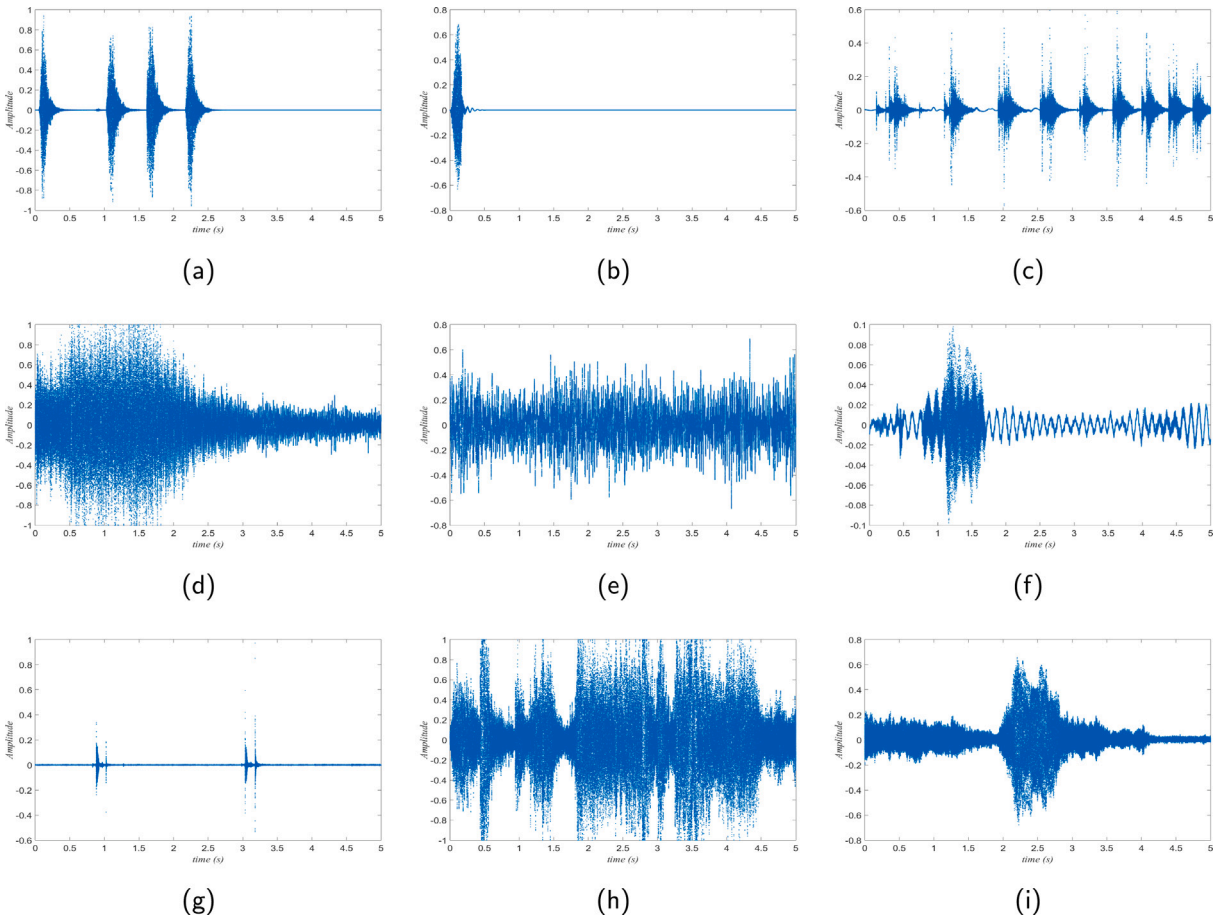

Fig. 5. Description of audio information. (a) 1-97392-A-0.wav. (b) 1-110389-A-0.wav. (c) 1-115920-A-22.wav. (d) 1-11687-A-47.wav. (e) 1-119125-A-45.wav. (f) 1-121951-A-8.wav. (g) 1-12654-A-15.wav. (h) 1-208757-A-2.wav. (i) 1-34094-A-5.wav.

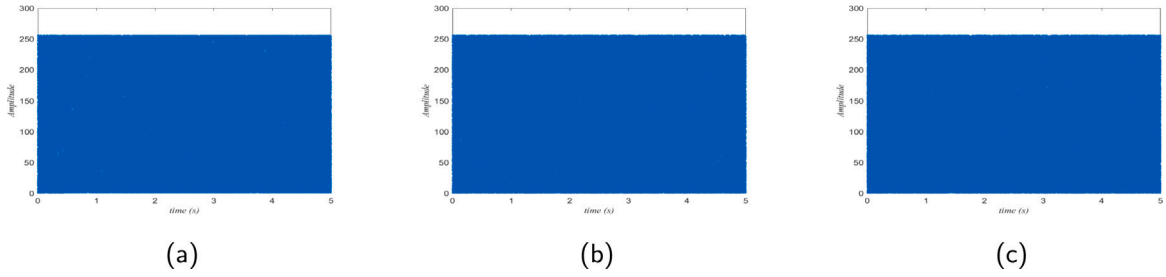

Fig. 6. Ciphered audio information. (a) Ciphered 1-110389-A-0.wav. (b) Ciphered 1-119125-A-45.wav. (c) Ciphered 1-208757-A-2.wav.

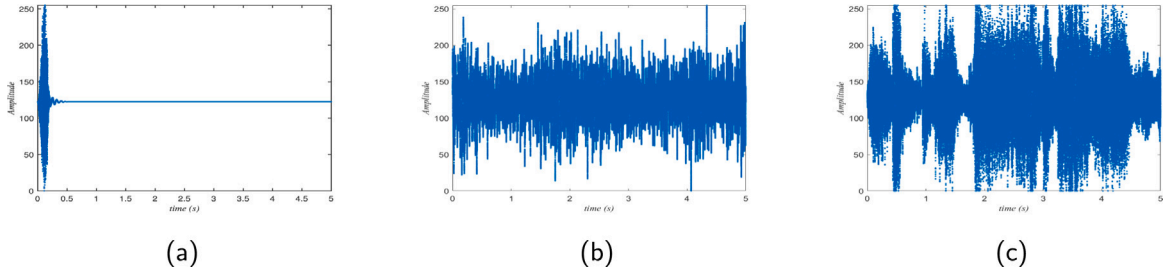

Fig. 7. Decrypted audio information. (a) Decrypted 1-110389-A-0.wav. (b) Decrypted 1-119125-A-45.wav. (c) Decrypted 1-208757-A-2.wav.

Algorithm 1: Description of decryption algorithm

Input: C (Ciphertext), and K (Secret key, 256 bits)
Output: A (Plaintext)

$NA_2 \leftarrow C - floor(C)$, $C = floor(C)$
$k_1 \leftarrow K(1:32) \oplus K(33:64)/2^{32}$ $//k_1 \in (0,1)$
$k_2 \leftarrow K(65:96) \oplus K(97:128)/2^{32}$ $//k_2 \in (0,1)$
$k_3 \leftarrow K(129:160) \oplus K(161:192)/2^{32} \times 100 + 4$ $//k_3 \in (4,104)$
$k_4 \leftarrow K(193:224) \oplus K(225:256)/2^{32} \times 100$ $//k_4 \in (0,100)$
$X, Y \leftarrow L_{2D-LNIC}(k_4, k_3, k_1, k_2)$
$S \leftarrow floor(X \times 10^{10})$, $S \leftarrow S \bmod 256$
$G \leftarrow$ meet the conditions that $G_i < G_{i+1}$ and $G_i \in Y$
$NA_1(1) \leftarrow C[G(1)] - S(1) \bmod 256$
$NA_1(2) \leftarrow C[G(2)] - S(1) - C[G(1)] \bmod 256$
$NA_1(3) \leftarrow C[G(3)] - S(1) - C[G(1)] - C[G(2)] \bmod 256$
for $i \leftarrow 4$ **to** L **do**
  $f_1 \leftarrow floor((3.999 + k_1/10^5) \times C[G(i-1)]/256 \times (1 - C[G(i-1)]/256) \times 10^{10}) \bmod 256$ $f_2 \leftarrow floor((3.999 + k_2/10^6) \times C[G(i-1)]/256 \times (1 - C[G(i-2)]/256) \times 10^{10}) \bmod 256$
  $NA_1(i) \leftarrow C[G(i)] - f_1 - f_2 - S(i) \bmod 256$
end
$A \leftarrow NA_1 + NA_2$

Table 2
NSCR and UACI of AEA-NCS.

Audios	NSCP (%)	Pass/Fail	UACI (%)	Pass/Fail
1-97392-A-0.wav	99.6052	Pass	33.4860	Pass
1-110389-A-0.wav	99.6063	Pass	33.4709	Pass
1-115920-A-22.wav	99.6109	Pass	33.4280	Pass
1-11687-A-47.wav	99.6070	Pass	33.4904	Pass
1-119125-A-45.wav	99.6071	Pass	33.4581	Pass
1-121951-A-8.wav	99.6055	Pass	33.4531	Pass
1-12654-A-15.wav	99.6079	Pass	33.4487	Pass
1-208757-A-2.wav	99.6082	Pass	33.4580	Pass
1-34094-A-5.wav	99.6073	Pass	33.4581	Pass
Average	99.6072	Pass	33.4612	Pass

formulas are,

$$\begin{cases} NSCR = \frac{1}{L}\sum_{i=1}^{L} \left| Sign(\lfloor C_1(i) \rfloor - \lfloor C_2(i) \rfloor) \right| \times 100\% \\ UACI = \frac{1}{L}\sum_{i=1}^{L} \frac{|\lfloor C_1(i) \rfloor - \lfloor C_2(i) \rfloor|}{255} \times 100\% \end{cases}, \tag{9}$$

where C_1 is the original ciphertext, C_2 is the new ciphertext, $\lfloor x \rfloor$ is the function of round-to-zero, $sign(x)$ is the sign function, and L is the length of the audio.

The acceptable ranges of NSCR and UACI corresponding to the plaintext of different lengths are given in Ref. [41]. When the length of the audio is 220 500, the range of NSCP is 99.5875% to 100%, and the range of UACI is 33.3648% to 33.5623%. At this point, it shows that the algorithm can resist differential attacks.

The values of NSCR and UACI are shown in Table 2. Experimental analysis results show that AEA-NCS has a strong ability to resist differential attacks.

5.3. Key analysis

The secret key of AEA-NCS is generated by Hash256, so the key space of AEA-NCS is 2^{256}. It is reported in Ref. [42] that if the key space is more than 2^{100}, the algorithm is resistant to brute force attacks. So the AEA-NCS has a strong ability to resist brute force attacks.

In addition, the key should be sensitive in a secure cryptosystem. To test the key sensitivity of AEA-NCS, the audio "1-121951-A-8.wav" is selected for key sensitivity analysis. The original secret key is K, the new keys with minor changes are K_1, K_2, K_3, K_4, and K_5.

$K = 640d4faae551e06b7f8f9e46580a720ec8bde6c32d4fa78c74f96534b4c226de,$

$K_1 = 640d4faae551e06b7f8f9e46580a720ec8bde6c32d4fa78c74f96534b4c226dc,$

$K_2 = 640d4faae551e06b7f8f9e46580a720ec8bde6c32d4fa78c74f96534b4c226df,$

$K_3 = 740d4faae551e06b7f8f9e46580a720ec8bde6c32d4fa78c74f96534b4c226de,$

$K_4 = 540d4faae551e06b7f8f9e46580a720ec8bde6c32d4fa78c74f96534b4c226de,$

$K_5 = 640d4faae551e06b7f8f9e46580a721ec8bde6c32d4fa78c74f96534b4c226de,$

The key sensitivity analysis of AEA-NCS is shown in Fig. 8.

Using NSCR and UACI to evaluate the subplots in Fig. 8 is different, and the evaluation results are shown in the Table 3.

The evaluation results show that the decrypted audio image is messy using the wrong key, and the attacker cannot identify the useful information, so the key of AEA-NCS is sensitive.

5.4. Classic attack analysis

Ciphertext only attack, known plaintext attack, chosen plaintext attack, and chosen ciphertext attack are the four classic attacks. Among them, the chosen plaintext attack is the most powerful attack. If an algorithm can resist the chosen plaintext attack, then this algorithm can resist four classic attack [4].

A_1 and A_2 are the original audios, and C_1 and C_2 are the encrypted audios. If $\lfloor A_1(i,j) \rfloor \oplus \lfloor A_2(i,j) \rfloor \neq \lfloor C_1(i,j) \rfloor \oplus \lfloor C_2(i,j) \rfloor$, it shows the encryption algorithm has the ability to resist chosen-plaintext attacks. The chosen-plaintext attacks analysis of AEA-NCS are shown in Fig. 9.

The NSCR is used to evaluate the difference between two audios. The NSCR between the audio in Fig. 9(a) and the audio in Fig. 9(d) is 99.5963%, that between the audio in Fig. 9(b) and the audio in Fig. 9(e) is 99.6485%, and that between the audio in Fig. 9(c) and the audio in Fig. 9(f) is 99.6235%. It is evident that $\lfloor A_1(i,j) \rfloor \oplus \lfloor A_2(i,j) \rfloor \neq \lfloor C_1(i,j) \rfloor \oplus \lfloor C_2(i,j) \rfloor$. So this the AEA-NCS can resist chosen plaintext attack and four classic attack.

5.5. Robustness analysis

When the information is transmitted over the Internet, the attacker usually uses noise attacks to interfere with the information, and the quality of the decrypted information will be degraded at this time. When the ciphertext is attacked by noise, the more information of the original audio recovered after decryption, the stronger the ability of the algorithm to resist noise attack. The robustness analysis results of AEA-NCS are shown in Fig. 10.

The NSCR is used to evaluate the robustness of AEA-NCS. The NSCR between the audio in Fig. 10(d) and the original audio is 0.03%, that between the audio in Fig. 10(e) and the original audio is 0.07%, and that between the audio in Fig. 10(f) and the original audio is 1.43%. The experimental results show that even if the ciphertext is attacked by noise during transmission, most of the original audio information can still be obtained through the decryption algorithm. AEA-NCS exhibits excellent robustness.

5.6. Information entropy analysis

Information entropy indicates the chaotic degree of information distribution. The more chaotic the information distribution, the closer the information entropy is to 8. The information entropy of AEA-NCS is shown in Table 4.

The information entropy analysis shows that the information entropy of the ciphertext is close to the theoretical value, indicating that AEA-NCS has a good encryption effect and can cover up the plaintext information. It is difficult for an attacker to obtain the plaintext information from the ciphertext (produced by AEA-NCS).

5.7. Correlation analysis

For a secure cryptosystem, the correlation between adjacent elements of the obtained ciphertext should be low, otherwise, the attacker

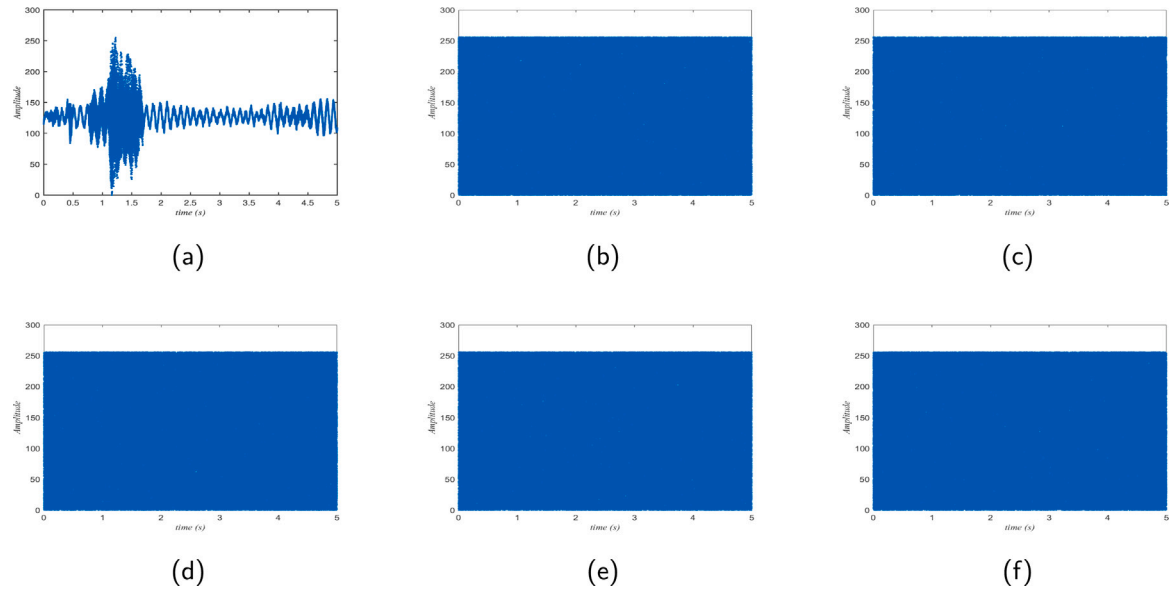

Fig. 8. Key sensitivity analysis of AEA-NCS. (a) Decrypted audio with K. (b) Decrypted audio with K_1. (c) Decrypted audio with K_2. (d) Decrypted audio with K_3. (e) Decrypted audio with K_4. (f) Decrypted audio with K_5.

Table 3
Key sensitivity analysis of AEA-NCS.

NPCR(%100)/UACI(%100)	Fig. 8(a)	Fig. 8(b)	Fig. 8(c)	Fig. 8(d)	Fig. 8(e)	Fig. 8(f)
Fig. 8(a)	–	99.6158	99.6072	99.6213	99.6072	99.6136
Fig. 8(b)	25.4013	–	99.6131	99.6140	99.5909	99.6163
Fig. 8(c)	25.4937	33.5150	–	99.6181	99.6009	99.6258
Fig. 8(d)	25.4295	33.5445	33.4751	–	99.6117	99.5968
Fig. 8(e)	25.4254	33.5306	33.4584	33.4601	–	99.6095
Fig. 8(f)	25.4014	33.3733	33.5059	33.4234	33.4617	–

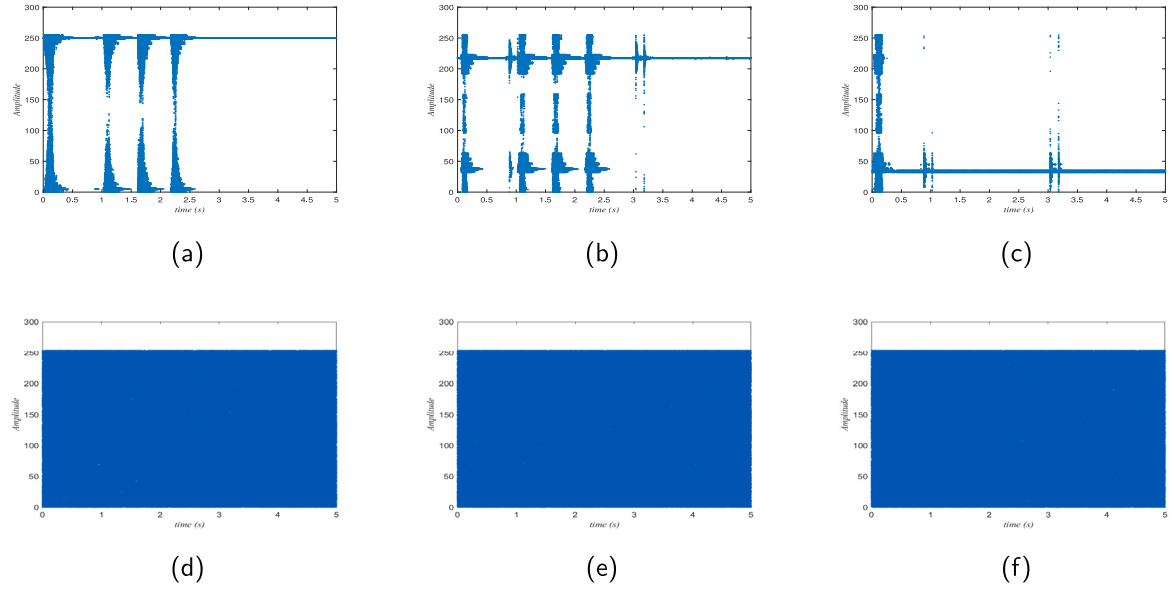

Fig. 9. Chosen-plaintext attacks of AEA-NCS. (a) Audio of 1-97392-A-0.wav XOR 1-110389-A-0.wav. (b) Audio of 1-97392-A-0.wav XOR 1-12654-A-15.wav. (c) Audio of 1-110389-A-0.wav XOR 1-12654-A-15.wav. (d) Audio of encrypted 1-97392-A-0.wav XOR encrypted 1-110389-A-0.wav. (e) Audio of encrypted 1-97392-A-0.wav XOR encrypted 1-12654-A-15.wav. (f) Audio of encrypted 1-110389-A-0.wav XOR encrypted 1-12654-A-15.wav.

will crack the algorithm by means of statistical attacks. The correlation calculation formula is

$$r(p,q) = \frac{\mathrm{cov}(p,q)}{\sigma(p)\sigma(p)},$$

where, q is the adjacent pixel value of p. The correlation analysis of AEA-NCS is shown in Table 5, Table 6 and Fig. 11.

As shown in Table 5, Table 6, and Fig. 11, A_n is the nth element of the audio, A_{n+1} is the $(n+1)^{th}$ element of the audio, A_{n+2} is the $(n+2)^{th}$ element of the audio. Correlation analysis shows that AEA-NCS can not only eliminate the correlation between adjacent elements of audio, but also eliminate the correlation between elements that are not adjacent in a short time.

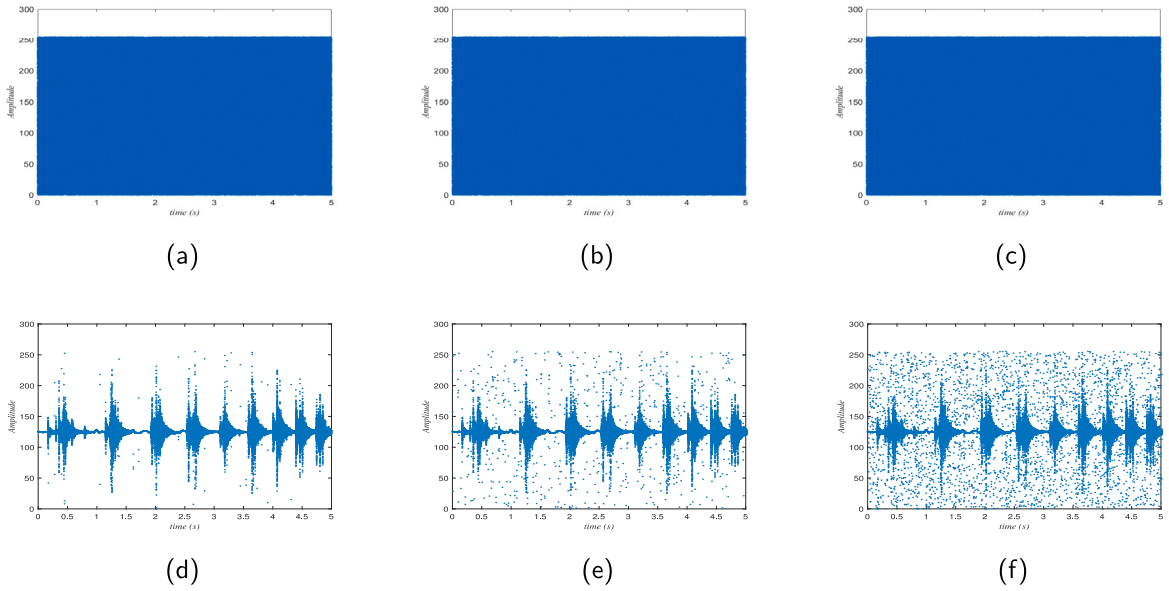

Fig. 10. Robustness analysis of audio 1-115920-A-22.wav. (a) Ciphered audio with 0.0001 salt & pepper noise. (b) Ciphered audio with 0.001 salt & pepper noise. (c) Ciphered audio with 0.005 salt & pepper noise. (d) Decrypted audio of (a). (e) Decrypted audio of (b). (f) Decrypted audio of (c).

Table 4
Information entropy of AEA-NCS.

Audios	Plaintext	Ciphertexts
1-97392-A-0.wav	2.305996	7.999197
1-110389-A-0.wav	0.789470	7.999169
1-115920-A-22.wav	3.944677	7.999032
1-11687-A-47.wav	6.667425	7.999206
1-119125-A-45.wav	6.918204	7.999212
1-121951-A-8.wav	5.749949	7.999177
1-12654-A-15.wav	1.333441	7.999189
1-208757-A-2.wav	7.160781	7.999026
1-34094-A-5.wav	5.784559	7.999215
Average	4.517166	7.999158

Table 5
Correlation coefficients of Plaintexts.

Audios	Plaintext		
	$A_n,\ A_{n+1}$	$A_n,\ A_{n+2}$	$A_n,\ A_{n+3}$
1-97392-A-0.wav	0.984303	0.938678	0.866471
1-110389-A-0.wav	0.986346	0.946290	0.881931
1-115920-A-22.wav	0.921015	0.764834	0.625231
1-11687-A-47.wav	0.907603	0.736946	0.654457
1-119125-A-45.wav	0.999348	0.997687	0.995575
1-121951-A-8.wav	0.969731	0.884306	0.758527
1-12654-A-15.wav	0.865871	0.688808	0.622361
1-208757-A-2.wav	0.988971	0.958375	0.913855
1-34094-A-5.wav	0.936340	0.757929	0.496745
Average	0.841525	0.748710	0.660963

In addition, the correlation comparison with other algorithms (KK [29], DXS [33], ARI [35], WS [36], RM [43], SGV [44], NPN [45], and NBC [46]) is shown in Table 7. The values in Table 7 are the mean values of the correlations. As shown in Table 7, the ciphertext obtained by AEA-NCS has lower correlation, which means that AEA-NCS has stronger ability to resist statistical attacks.

5.8. Efficiency analysis

The system environment is described as follows: win10 system, CPU: I5-4210, and MATLAB R2019a. The efficiency analysis of AEA-NCS is shown in Table 8. Compared with other algorithms (KK [29], DXS [33], ARI [35], WS [36], NPN [45], and NBC [46]), AEA-NCS is more efficient as shown in Table 9.

Table 6
Correlation coefficients of Ciphertexts.

Audios	Ciphertexts		
	$A_n,\ A_{n+1}$	$A_n,\ A_{n+2}$	$A_n,\ A_{n+3}$
1-97392-A-0.wav	−0.001459	0.001582	0.000651
1-110389-A-0.wav	0.002247	−0.000160	−0.001872
1-115920-A-22.wav	−0.000689	0.002165	0.0016217
1-11687-A-47.wav	−0.001711	0.003079	−0.001214
1-119125-A-45.wav	0.000995	0.001099	0.001790
1-121951-A-8.wav	−0.001207	−0.001457	0.0010471
1-12654-A-15.wav	0.003268	0.001185	0.003467
1-208757-A-2.wav	−0.000070	−0.003556	−0.000523
1-34094-A-5.wav	−0.001496	0.003218	−0.000007
Average	−0.000013	0.000795	0.000551

6. Conclusion

In some specific scenarios, acquiring image information is expensive and time-consuming, and acquiring audio information becomes a better choice at this time. This paper provides a secure encryption algorithm based on 2D-LNIC for transmitting audio information on the Internet. 2D-LNIC is a combination of two classical mappings. Through Lyapunov exponent, bifurcation graph, attractor, and other methods, it is verified that 2D-LNIC has good dynamic behavior and has a large parameter space in a chaotic state, which is very suitable for cryptography. Therefore, the keystream of AEA-NCS is generated using 2D-LNIC. In cryptosystems, the audio information is mapped to $[0, 255]$ so that we can evaluate the audio ciphertext using the same method used to evaluate the image ciphertext. Then a hash function is used to generate the secret key of the cryptosystem. Finally, combined with 2D-LNIC, the audio information is encrypted using the encryption algorithm of scrambling and diffusion simultaneously. Correlation analysis, visual analysis, and other methods have verified that AEA-NCS has good performance and can complete the task of audio encryption.

Table 7
Comparison with other algorithms.

Algorithm	AEA-NCS	KK [29]	DXS [33]	ARI [35]	WS [36]	RM [43]	SGV [44]	NPN [45]	NBC [46]
Correlation	**−0.00001**	−0.0006	0.0010	0.00005	0.0004	−0.1578	0.0133	0.0002	0.0002

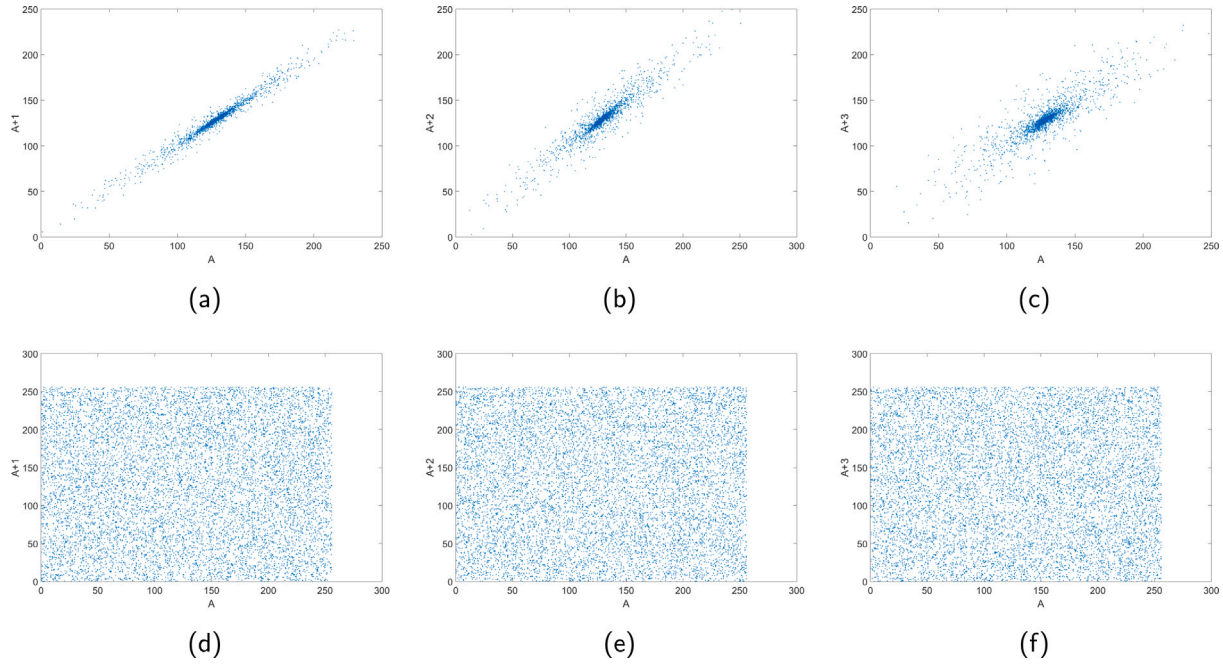

Fig. 11. Correlation coefficients of 1-97392-A-0.wav. (a) Plaintext between A_n and A_{n+1}. (b) Plaintext between A_n and A_{n+2}. (c) Plaintext between A_n and A_{n+3}. (d) Ciphertext between A_n and A_{n+1}. (e) Ciphertext between A_n and A_{n+2}. (f) Ciphertext between A_n and A_{n+3}.

Table 8
Efficiency analysis.

Audios	Sizes (KB)	Encryption time (s)	Speed (s/KB)
1-97392-A-0.wav	430	0.234232	0.000544
1-110389-A-0.wav	430	0.230509	0.000536
1-115920-A-22.wav	430	0.233298	0.000542
1-11687-A-47.wav	430	0.227486	0.000529
1-119125-A-45.wav	430	0.226902	0.000527
1-121951-A-8.wav	430	0.234685	0.000545
1-12654-A-15.wav	430	0.233517	0.000543
1-208757-A-2.wav	430	0.232537	0.000540
1-34094-A-5.wav	430	0.233659	0.000543
Average	430	0.231869	0.000539

Table 9
Encryption time comparison.

Algorithms	Sizes	Encryption time (s)	Speed (s/KB)
AEA-NCS	430 KB	0.2318	**0.0005**
KK [29]	544 KB	1.3240	0.0024
DXS [33]	260 KB	0.6364	0.0024
ARI [35]	984 KB	198.26	0.2014
WS [36]	123 KB	14.6000	0.0370
NPN [45]	304 KB	58.6300	0.1928
NBC [46]	439 KB	1.1760	0.0026

CRediT authorship contribution statement

Rui Wu: Project administration, Resources, Writing – original draft. **Suo Gao:** Methodology, Software, Writing – original draft, Writing – review & editing. **Xingyuan Wang:** Funding acquisition, Project administration, Resources. **Songbo Liu:** Conceptualization, Data curation. **Qi Li:** Investigation, Validation, Visualization. **Uğur Erkan:** Supervision, Writing – review & editing. **Xianglong Tang:** Funding acquisition, Resources.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This research is supported by the National Natural Science Foundation of China (Nos: 61672124, and 61672190), the Password Theory Project of the 13th Five-Year Plan National Cryptography Development Fund, China (No. MMJJ20170203), and Key R&D Projects of Liaoning Province, China (No: 2019020105-JH2/103).

References

[1] Liu X, Tong X, Wang Z, et al. A new n-dimensional conservative chaos based on generalized Hamiltonian system and its' applications in image encryption. Chaos Solitons Fractals 2022;154:111693.
[2] Chai X, Fu J, Gan Z, et al. An image encryption scheme based on multi-objective optimization and block compressed sensing. Nonlinear Dynam 2022;108(3):2671–704.
[3] Li X, Mou J, Banerjee S, et al. Design and DSP implementation of a fractional-order detuned laser hyperchaotic circuit with applications in image encryption. Chaos Solitons Fractals 2022;159:112133.
[4] Gao S, Wu R, Wang X, et al. A 3D model encryption scheme based on a cascaded chaotic system. Signal Process 2023;202:108745.

[5] Wang X, Wang X, Ma B, et al. High precision error prediction algorithm based on ridge regression predictor for reversible data hiding. IEEE Signal Process Lett 2021;28:1125–9.
[6] Ma B, Shi YQ. A reversible data hiding scheme based on code division multiplexing. IEEE Trans Inf Forensics Secur 2016;11(9):1914–27.
[7] Li Q, Wang X, Ma B, et al. Concealed attack for robust watermarking based on generative model and perceptual loss. IEEE Trans Circuits Syst Video Technol 2022;32(8):5695–706.
[8] Wang C, Ma B, Xia Z, et al. Stereoscopic image description with trinion fractional-order continuous orthogonal moments. IEEE Trans Circuits Syst Video Technol 2022;32(4):1998–2012.
[9] Wang X, Gao S, Ye X, et al. A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system. Int J Bifurcation Chaos 2021;31(01):2150003.
[10] Chai X, Wu H, Gan Z, et al. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. Inform Sci 2021;556:305–40.
[11] Ma X, Mou J, Xiong L, et al. A novel chaotic circuit with coexistence of multiple attractors and state transition based on two memristors. Chaos Solitons Fractals 2021;152:111363.
[12] Wang X, Liu P. A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Trans Circuits Syst I Regul Pap 2021;69(3):1291–301.
[13] García-Guerrero E, Inzunza-González E, López-Bonilla O, et al. Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels. Chaos Solitons Fractals 2020;133:109646.
[14] Fu X, Liu B, Xie Y, et al. Image encryption-then-transmission using DNA encryption algorithm and the double chaos. IEEE Photonics J 2018;10(3):1–15.
[15] Al-Hazaimeh O, Al-Jamal M, Alhindawi N, et al. Image encryption algorithm based on lorenz chaotic map with dynamic secret keys. Neural Comput Appl 2019;31(7):2395–405.
[16] Wang X, Gao S. A chaotic image encryption algorithm based on a counting system and the semi-tensor product. Multimedia Tools Appl 2021;80(7):10301–22.
[17] Zhou S, Wang X, Zhang Y, et al. A novel image encryption cryptosystem based on true random numbers and chaotic systems. Multimedia Syst 2022;28(1):95–112.
[18] Jain K, Aji A, Krishnan P. Medical image encryption scheme using multiple chaotic maps. Pattern Recognit Lett 2021;152:356–64.
[19] Song W, Fu C, Tie M, et al. A fast parallel batch image encryption algorithm using intrinsic properties of chaos. Signal Process, Image Commun 2022;102:116628.
[20] Yahi A, Bekkouche T, Daachi MEH, et al. A color image encryption scheme based on 1D cubic map. Optik 2022;249:168290.
[21] Midoun MA, Wang X, Talhaoui MZ. A sensitive dynamic mutual encryption system based on a new 1D chaotic map. Opt Lasers Eng 2021;139:106485.
[22] Li C, Lin D, Lü J, et al. Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography. IEEE Multimedia 2018;25(4):46–56.
[23] Zareai D, Balafar M, Feizi Derakhshi MR. A new grayscale image encryption algorithm composed of logistic mapping, arnold cat, and image blocking. Multimedia Tools Appl 2021;80(12):18317–44.
[24] Cao W, Mao Y, Zhou Y. Designing a 2D infinite collapse map for image encryption. Signal Process 2020;171:107457.
[25] Chai X, Fu X, Gan Z, et al. A color image cryptosystem based on dynamic DNA encryption and chaos. Signal Process 2019;155:44–62.
[26] Gao X, Mou J, Xiong L, et al. A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear Dynam 2022;108(1):613–36.
[27] Zhou S, Wang X, Wang M, et al. Simple colour image cryptosystem with very high level of security. Chaos Solitons Fractals 2020;141:110225.
[28] Wang M, Wang X, Wang C, et al. Spatiotemporal chaos in cross coupled map lattice with dynamic coupling coefficient and its application in bit-level color image encryption. Chaos Solitons Fractals 2020;139:110028.
[29] Kordov K. A novel audio encryption algorithm with permutation-substitution architecture. Electronics 2019;8(5):530.
[30] Lima JB, Da Silva Neto EF. Audio encryption based on the cosine number transform. Multimedia Tools Appl 2016;75(14):8403–18.
[31] Parvees MYM, Samath JA, Bose BP. Audio encryption–a chaos-based data byte scrambling technique. Int J Appl Syst Stud 2018;8(1):51–75.
[32] Gnanajeyaraman R, Prasadh K. Audio encryption using higher dimensional chaotic map. Int J Recent Trends Eng 2009;1(2):103.
[33] Dai W, Xu X, Song X, et al. Audio encryption algorithm based on chen memristor chaotic system. Symmetry 2021;14(1):17.
[34] El Hanouti I, El Fadili H. Security analysis of an audio data encryption scheme based on key chaining and DNA encoding. Multimedia Tools Appl 2021;80(8):12077–99.
[35] Abdelfatah RI. Audio encryption scheme using self-adaptive bit scrambling and two multi chaotic-based dynamic DNA computations. IEEE Access 2020;8:69894–907.
[36] Wang X, Su Y. An audio encryption algorithm based on DNA coding and chaotic system. IEEE Access 2019;8:9260–70.
[37] Feistel H. Cryptography and computer privacy. Sci Am 1973;228(5):15–23.
[38] Solak E, Cokal C, Yildiz OT, et al. Cryptanalysis of Fridrich's chaotic image encryption. Int J Bifurcation Chaos 2010;20(05):1405–13.
[39] Xie EY, Li C, Yu S, et al. On the cryptanalysis of Fridrich's chaotic image encryption scheme. Signal Process 2017;132:150–4.
[40] Naskar PK, Paul S, Nandy D, et al. DNA encoding and channel shuffling for secured encryption of audio data. Multimedia Tools Appl 2019;78(17):25019–42.
[41] Wu Y, Noonan JP, Agaian S. NPCR and UACI randomness tests for image encryption. Cyber journals: multidisciplinary journals in science and technology. J Sel Areas Telecommun (JSAT) 2011;1(2):31–8.
[42] Hosny KM, Kamal ST, Darwish MM. A color image encryption technique using block scrambling and chaos. Multimedia Tools Appl 2022;81(1):505–25.
[43] Roy A, Misra AP. Audio signal encryption using chaotic Hénon map and lifting wavelet transforms. Eur Phys J Plus 2017;132(12):1–10.
[44] Sasikaladevi N, Geetha K, Venkata Srinivas KN. A multi-tier security system (SAIL) for protecting audio signals from malicious exploits. Int J Speech Technol 2018;21(2):319–32.
[45] Naskar PK, Paul S, Nandy D, et al. DNA encoding and channel shuffling for secured encryption of audio data. Multimedia Tools Appl 2019;78(17):25019–42.
[46] Naskar PK, Bhattacharyya S, Chaudhuri A. An audio encryption based on distinct key blocks along with PWLCM and ECA. Nonlinear Dynam 2021;103(2):2019–42.