frontiers | Frontiers in Physics

TYPE Original Research
PUBLISHED 30 September 2022
DOI 10.3389/fphy.2022.1006324

OPEN ACCESS

EDITED BY
Karthikeyan Rajagopal,
Chennai Institute of Technology, India

REVIEWED BY
Hongjun Liu,
University of Jinan, China
Junwei Sun,
Zhengzhou University of Light Industry, China

*CORRESPONDENCE
Yongsheng Hu,
huys1208@bzu.edu.cn

SPECIALTY SECTION
This article was submitted to Interdisciplinary Physics, a section of the journal Frontiers in Physics

RECEIVED 29 July 2022
ACCEPTED 09 September 2022
PUBLISHED 30 September 2022

CITATION
Hu Y, Wang X and Zhang L (2022), 1D Sine-Map-Coupling-Logistic-Map for 3D model encryption.
Front. Phys. 10:1006324.
doi: 10.3389/fphy.2022.1006324

1D Sine-Map-Coupling-Logistic-Map for 3D model encryption

Yongsheng Hu[1,2]*, Xiaolin Wang[1,2] and Liyi Zhang[2]

[1]School of Information Engineering, Binzhou University, Binzhou, China, [2]School of Information Engineering, Tianjin University of Commerce, Tianjin, China

With the rise of technologies of VR technology, AR technology, and 3D printing, the application of 3D models has become more and more extensive. The data of the 3D model is the floating point and has a unique storage format, and the traditional 2D image encryption algorithms are unsuitable for 3D models. Therefore, based on 1D Sine-Map-Coupling-Logistic-Map (1D-SMCLM), a 3D model encryption algorithm is designed in this paper. The 1D-SMCLM is a new chaotic system with large parameter space and good chaotic characteristics. The keystream generated by the 1D-SMCLM has good randomness and is very suitable for cryptographic systems. In the new encryption algorithm (SMCLM-3ME), the vertices of the 3D models are divided into integer and decimal vertices. The integer part is encrypted by the strategy of simultaneous scrambling and diffusion. The 3D ciphertext model is obtained by combining the integer and fractional parts. Experimental results show that the SMCLM-IE exhibits excellent performance.

KEYWORDS

chaotic image encryption, chaos theory, 3D model, cryptography, 1D-SMCLM

1 Introduction

With the rapid development of network communication and big data applications, information security has become a critical hot issue [1–5]. The amount of image data on the Internet continues to grow, and most plaintext images are stored in plaintext, which poses a significant security risk [6–8]. Protecting the secure transmission of images on the Internet is an urgent security issue [9–12].

The adjacent pixels of the image has a very strong correlation [13–17], and the traditional DES, AES and other algorithms [18] cannot eliminate this correlation, and the efficiency of these algorithms is very low. Currently, many image protection algorithms have been proposed, such as image watermarking technology, image encryption technology, and image steganography technology [19–24]. Among them, image encryption technology is one of the most widely used technologies [25, 26]. Image encryption technology can convert plaintext images into ciphertext images with random noise according to specific rules, which has high-security [27, 28].

Chaos, as a nonlinear system, has seemingly random irregular motions [29–31], and the behavior of chaos is uncertain, unrepeatable, and unpredictable, which makes chaos and

cryptography have many natural connections [32–36]. Therefore, many image encryption algorithms are proposed based on chaos. For example, the chaotic image encryption algorithm based on DNA [37–39], the chaotic image encryption algorithm based on RNA [40, 41], the chaotic image encryption algorithm based on matrix semi-tensor product [42–45], and the chaotic image encryption algorithm based on compressed sensing [46, 47].

With the rise of technologies of VR technology, AR technology, and 3D printing, the application of 3D models has become more and more extensive. The 2D image encryption algorithm based on chaos has matured, and the 3D model encryption algorithm based on chaos is less studied. Unlike 2D images, the data type of 3D models is a floating point and has a unique storage format. Therefore, the 2D image encryption algorithm cannot be transplanted into the 3D model encryption algorithm. Although a few 3D model encryption algorithms have been proposed, they all have some disadvantages [48, 49]. For example, Xu et al. proposed a CTBCS hyperchaotic system, which uses Arnold scrambling and DNA diffusion to encrypt 3D models. The CTBCS generates the keystream required by the cryptosystem. However, the Arnold mapping has certain limitations, and the scrambled image will result in a plaintext image after a finite number of iterations [48]. In order to improve the defects of this algorithm, Chu et al. used the 3D Arnold algorithm to scramble the plaintext image and used RNA in the diffusion. The memristive chaotic system generated the keystream required by the cryptosystem, and the effect of the algorithm seemed to be good. However, the time of the algorithm is prolonged. They are sacrificing time to improve the security of the algorithm [49]. Unlike traditional scrambling and diffusing algorithms, the 3D model encryption algorithm (SMCLM-3ME) proposed in this paper is scrambling and diffusing simultaneously, which is fast and has high security.

Although high-dimensional chaotic systems have high dynamic behavior, the cost is that the generation speed of the key stream is plodding, and their complex structure makes them difficult to be applied in industrial production [50–54]. Therefore, making a low-dimensional chaotic system generate complex dynamic behavior is essential to increasing a cryptographic system's security. This paper proposes a new one-dimensional chaotic system 1D Sine-Map-Coupling-Logistic-Map (1D-SMCLM) based on Sin Map [55] and Logistic Map [56]. Compared with Sin and Logistic maps, 1D-SMCLM has a larger parameter space. As well as better kinetic behavior, the resulting sequences have good randomness and are therefore very suitable for cryptography. In SMCLM-3ME, the 1D-SMCLM is used to generate a random keystream.

The remaining chapters of this paper are organized as follows. Section 2 introduces the 1D-SMCLM and analyzes its chaotic behavior. Section 3 introduces the SMCLM-3ME algorithm. Section 4 simulates and analyzes the security of the SMCLM-3ME. Finally, the whole paper is concluded in Section 5.

2 1D-SMCLM

The 1D-SMCLM is the coupling of two classical one-dimensional chaotic maps (Sin Map and Logistic Map). The Sin Map is defined as,

$$f_{n+1} = \varphi \sin(\pi f_n). \tag{1}$$

where φ is the control parameter of the Sin Map. The Logistic Map is defined as,

$$f_{n+1} = \gamma f_n(1 - f_n). \tag{2}$$

where γ is the control parameter of the Logistic Map.

The simple structure of Sin Map and Logistic Map can produce complex chaotic behavior, so they are widely used in chaotic image encryption. However, they have some defects, the space of their control parameters is small, and the parameter space in the chaotic state is discontinuous, which will reduce the security of the cryptosystem. Therefore, we propose a new one-dimensional chaotic system (1D-SMCLM), which is defined as,

$$x_{n+1} = \varphi \sin\left(\sin(\pi x_n) \cdot \gamma x_n(1 - x_n) + 1\right). \tag{3}$$

where φ and γ are the control parameters of the 1D-SMCLM, $\gamma \in R^+$ and $\varphi \in R^+$. x_0 is the initial value of the 1D-SMCLM.

2.1 Trajectory analysis

The trajectory of a nonlinear dynamical system describes the iterative changes. The larger the area of the image space occupied by the trajectory of the nonlinear dynamical system, the better the performance of the sequence generated by this system. The trajectory analysis of the 1D-SMCLM is shown in Figure 1 and Figure 2 in different parameter spaces. The trajectory analysis in this paper includes two-dimensional trajectory analysis and three-dimensional trajectory analysis. The initial value of the 1D-SMCLM is $x_0 = 0.32498324654$.

Consists of 2D trajectory and 3D trajectory of the 1D-SMCLM. When φ is small, the sequences generated by the 1D-SMCLM have weak performance, and as φ gradually increases, the performance of sequences generated by the 1D-SMCLM gradually increases. In addition, the trajectories of Sin Map and Logistic Map are shown in Figure 3 and Figure 4.

Under the same parameters, the 1D-SMCLM exhibits better performance compared to Sin Map and Logistic Map. The trajectory of the 1D-SMCLM fills almost the entire phase space. Therefore, it can be shown that the sequences generated by the 1D-SMCLM have better performance than Sin Map and Logistic Map.

2.2 Lyapunov exponent analysis

Lyapunov exponents is an important index to evaluate whether the nonlinear dynamic system is in a chaotic state.

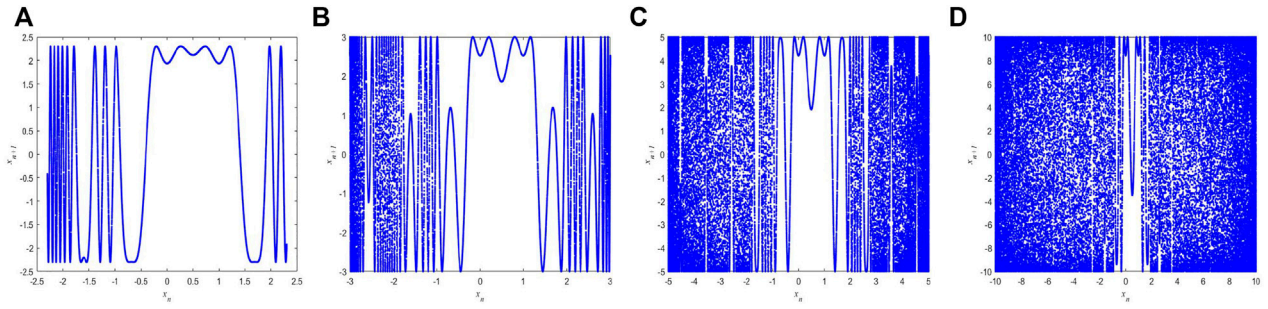

FIGURE 1
2D trajectory analysis of 1D-SMCLM. **(A)** φ = 2.3, γ = 3.9. **(B)** φ = 3, γ = 5.9. **(C)** φ = 5, γ = 7. **(D)** φ = 10, γ = 10.

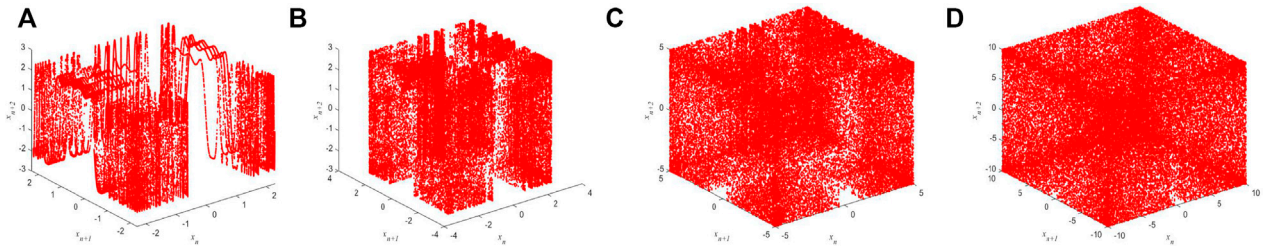

FIGURE 2
3D trajectory analysis of 1D-SMCLM. **(A)** φ = 2.3, γ = 3.9. **(B)** φ = 3, γ = 5.9. **(C)** φ = 5, γ = 7. **(D)** φ = 10, γ = 10.

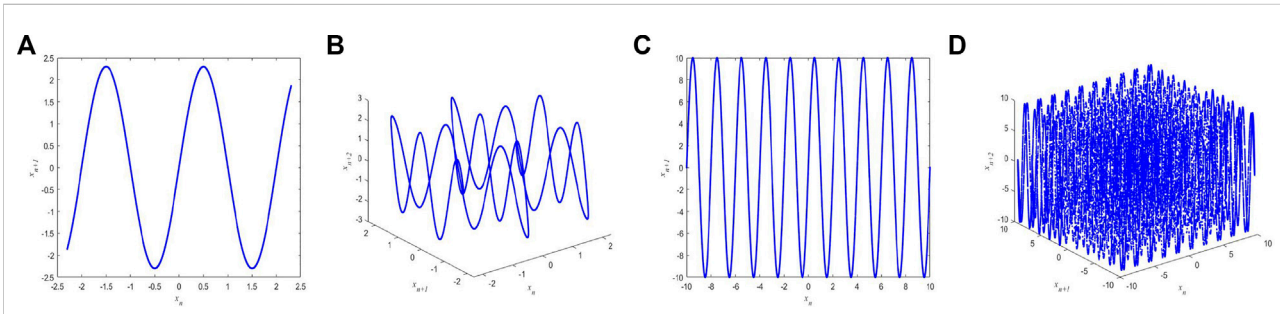

FIGURE 3
Trajectory analysis of Sin Map. **(A)** 2D trajectory analysis with φ = 2.3. **(B)** 3D trajectory analysis with φ = 2.3. **(C)** 2D trajectory analysis with φ = 10. **(D)** 3D trajectory analysis with φ = 10.

When LE is greater than 0, it indicates that the nonlinear dynamical system is chaotic at this time. LE is defined as,

$$\lambda = \lim_{T\to+\infty} \frac{1}{T} \sum_{t=0}^{T} |f'(x_t)|. \tag{4}$$

The LE analysis of 1D-SMCLM is shown in Figure 5.

When φ = 2.3, at γ = 0.5501, γ = 1.4001, and γ = 7.001, the 1D-SMCLM is in a non-chaotic state, with the φ gradual increase of, this non-chaotic phenomenon gradually disappears. When φ = 5, the 1D-SMCLM is almost global chaotic, which means that the parameter of 1D-SMCLM can be selected is $\gamma \in R^{+}$. In addition, the LE analysis of Sin Map and Logistic Map are shown in Figure 6. The parameter space of the Sin Map in chaotic state is discontinuous, while the parameter space of the Logistic Map in chaotic state is very small. The 1D-SMCLM addresses the advantages of both systems and exhibits excellent performance. 1D-SMCLM addresses the shortcomings of these two systems and exhibits excellent performance. The 1D-SMCLM can generate better random sequences.

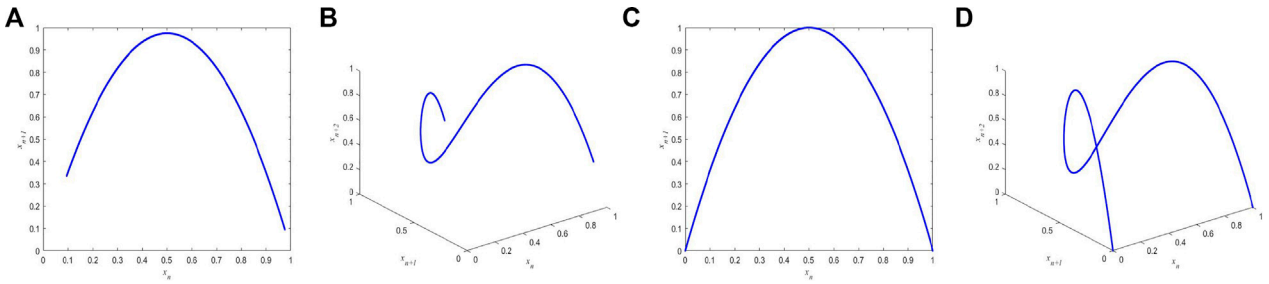

FIGURE 4
Trajectory analysis of Logistic Map. **(A)** 2D trajectory analysis with $\gamma = 3.9$. **(B)** 3D trajectory analysis with $\gamma = 3.9$. **(C)** 2D trajectory analysis with $\gamma = 10$. **(D)** 3D trajectory analysis with $\gamma = 10$.

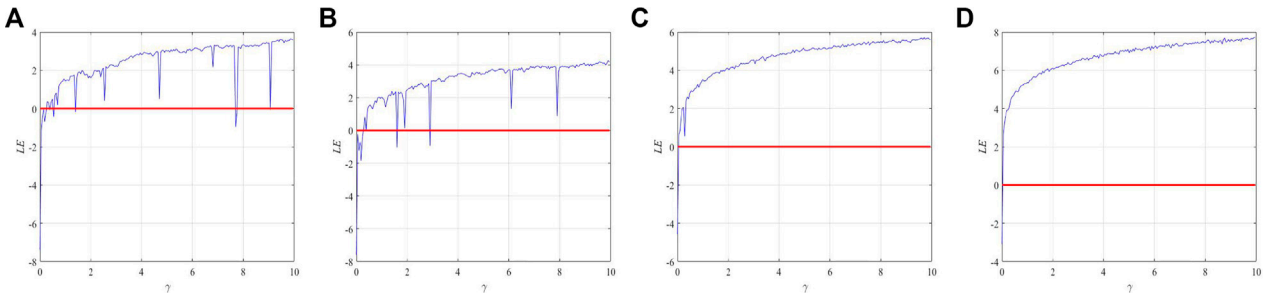

FIGURE 5
LE analysis of 1D-SMCLM. **(A)** $\varphi = 2.3$. **(B)** $\varphi = 3$. **(C)** $\varphi = 5$. **(D)** $\varphi = 10$.

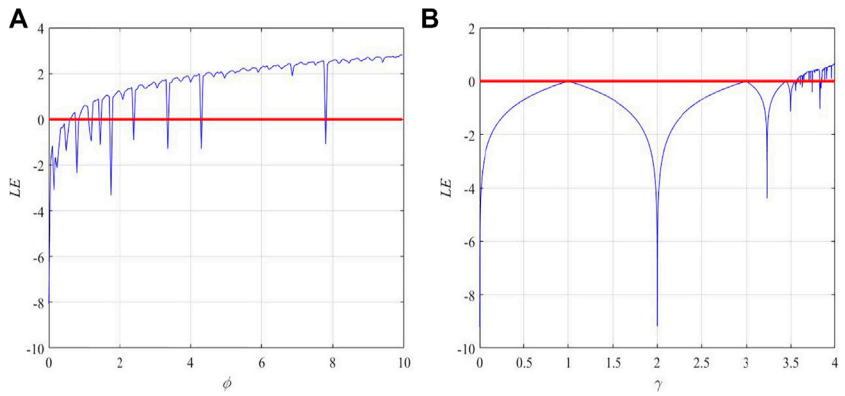

FIGURE 6
LE analysis of Sin Map and Logistic Map. **(A)** LE of Sin Map. **(B)** LE of Logistic Map.

2.3 NIST statistical test suite

National Institute of Standards and Technology (NIST) suit is used to test the random performance of the chaotic sequence generated by chaos. NIST statistical test of the 1D-SMCLM is shown in Table 1. The test results show that the 1D-SMCLM can generate chaotic sequences with good randomness.

2.4 0–1 test

The 0–1 test is another random number test, the 0–1 test is defined as,

$$R(n) = \sum_{j=1}^{n} x(j)\cos(\phi(j)), S(n) = \sum_{j=1}^{n} x(j)\sin(\phi(j)). \quad (5)$$

When a sequence has good randomness, its 0–1 test graph exhibits a Boolean motion state. When the sequence has no randomness, its 0–1 test graph is clustered. The 0–1 test of the 1D-SMCLM is shown in Figure 7.

Figures 7A–C are Boolean motion states, and the corresponding the 1D-SMCLM is a chaotic state at this time. Figure 7D is the Boolean motion state, corresponding to the periodic state of the 1D-SMCLM. The 0–1 test shows that the 1D-SMCLM has good performance and can generate random sequences.

3 SMCLM-3ME

Unlike 2D images, the data type of 3D images is a floating point type. Traditional 2D image encryption algorithms cannot be ported to 3D model encryption. Because the 1D-SMCLM has good performance, we propose a new 3D model encryption algorithm based on the 1D-SMCLM, called SMCLM-3ME. The structure diagram of the SMCLM-3ME is shown in Figure 8.

3.1 3D model processing

The encrypted objects of SMCLM-3ME are in Stereolithography (STL) format. A 3D model in STL format is composed of multiple triangular faces. The vertex coordinates in

TABLE 1 NISTtest of 1D-SMCLM.

Number	Statistical test	$\varphi = 2.3, \gamma = 3.9$		$\varphi = 3, \gamma = 5.9$	
		p-value	Result	*p*-value	Result
1	Longest run of ones	0.883171	Pass	0.419021	Pass
2	Overlapping template matching	0.534146	Pass	0.494392	Pass
3	Random excursions variant	0.888137	Pass	0.739918	Pass
4	Rank	0.013569	Pass	0.657933	Pass
5	Frequency	0.494392	Pass	0.319084	Pass
6	Universal	0.289667	Pass	0.122325	Pass
7	Random excursions	0.964295	Pass	0.671779	Pass
8	Block frequency	0.883171	Pass	0.455937	Pass
9	Cumulative sums	0.574903	Pass	0.911413	Pass
10	Runs	0.699313	Pass	0.779188	Pass
11	Serial	0.739918	Pass	0.616305	Pass
12	Spectral	0.657933	Pass	0.289667	Pass
13	Approximate entropy	0.779188	Pass	0.236810	Pass
14	Non-overlapping template matching	0.816537	Pass	0.779188	Pass
15	Linear complexity	0.534146	Pass	0.534146	Pass

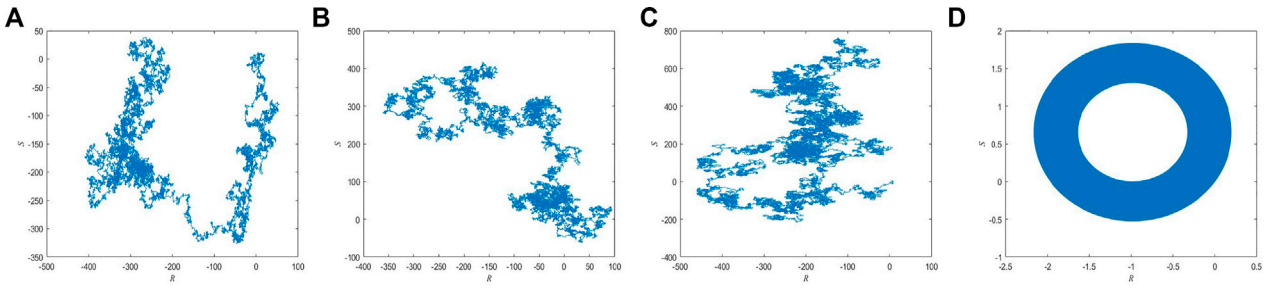

FIGURE 7
0–1 test. **(A)** $\varphi = 2.3$, $\gamma = 3.9$. **(B)** $\varphi = 3$, $\gamma = 5.9$. **(C)** $\varphi = 5$, $\gamma = 7$. **(D)** $\varphi = 2.3\gamma = 0.1$.

10.3389/fphy.2022.1006324

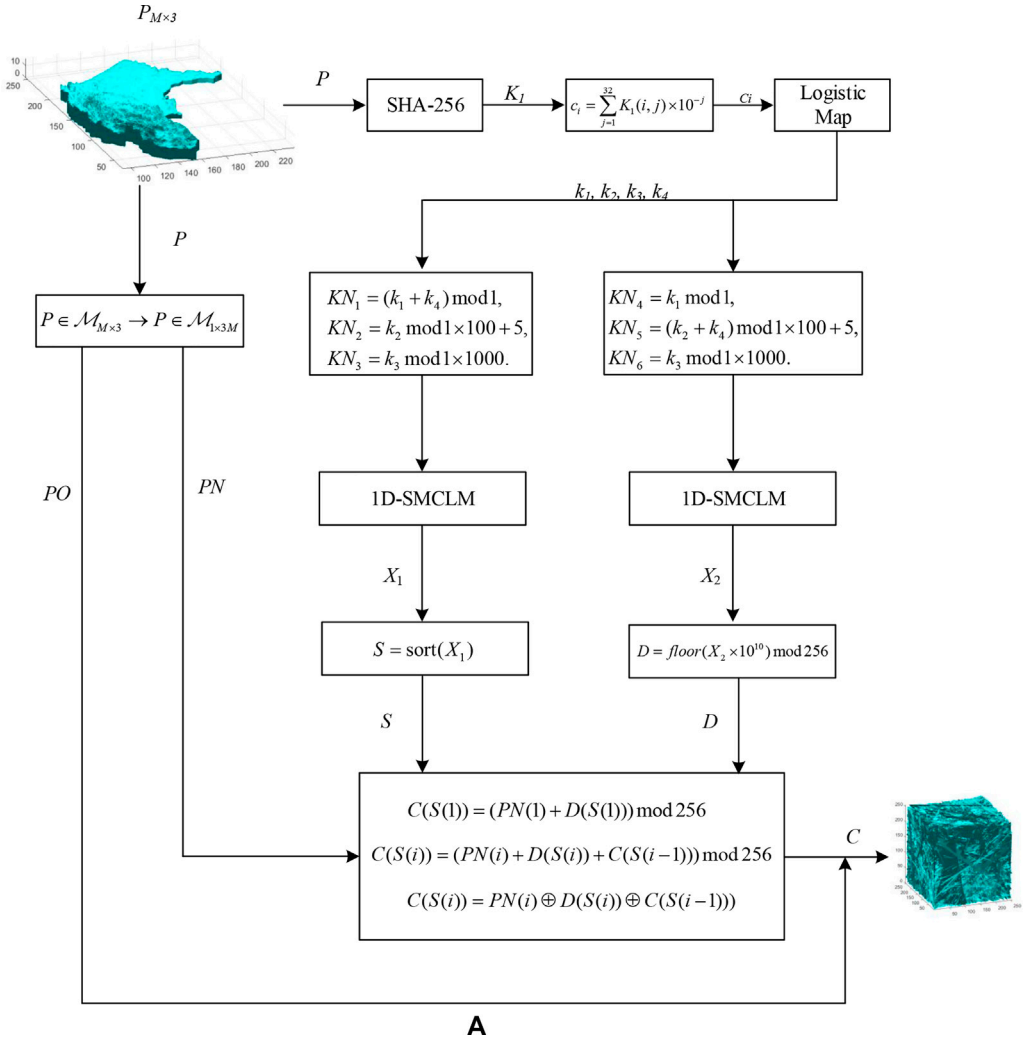

FIGURE 8
Structure diagram of SMCLM-3ME.

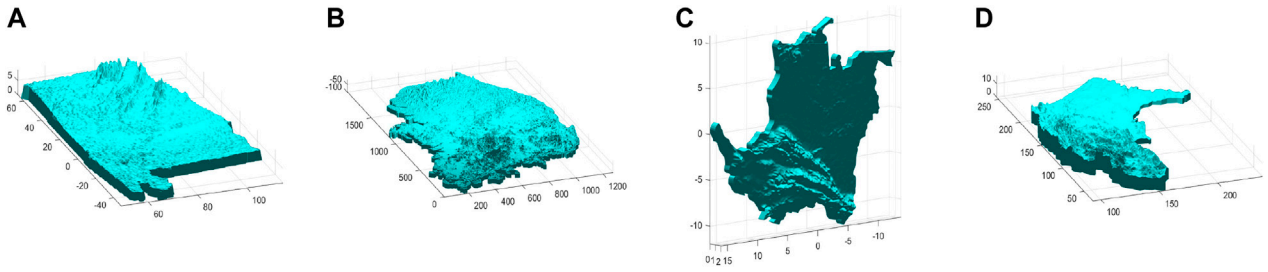

FIGURE 9
3D models. **(A)** Topographic map of the United States. **(B)** Topographic map of South Korea. **(C)** Topographic map of Colombia. **(D)** Topographic map of the capital of Australia.

3D space determine the shape of the 3D model. The vertex coordinates of the 3D model are represented as, $P_i = \{x_i, y_i, z_i\}$.

In SMCLM-3ME, the 3D model is first normalized, so that the vertex coordinates are mapped to between [0, 255], and the normalization method is shown in Eq. 6,

$$P = \frac{P - \min P}{\max P - \min P} \times 255. \tag{6}$$

The 3D model dataset is selected from http://www.3dwhere.com. The 3D model is normalized as shown in Figure 9.

3.2 Key generation

The key of the SMCLM-3ME is generated by a hash function, and the normalized plaintext is used as the input of the hash function. The key generation process is described as follows.

Input: P. ($P \in \mathcal{M}_{M\times3}$)

Step 1 : The plaintext P is the input of the hash function. The hash-256 function is used to generate a 256-bit secret key K. The other secret key of the SMCLM-3ME is generated by the secret key K.

Step 2 : Convert K to array K_1, $K \in \mathcal{M}_{1\times256} \rightarrow K_1 \in \mathcal{M}_{16\times16}$.

Step 3 : Convert $K_1 \in \mathcal{M}_{16\times16}$ to $K_2 \in \mathcal{M}_{16\times1}$ by Eq. 7,

$$K_2 = \{c_i | i = 1, 2, 3, 4, \ldots, 16\}, c_i = \sum_{j=1}^{16} K_1(i, j) \times 10^{-j}. \tag{7}$$

Step 4 : K_2 as the initial value of Logistic Map, the Logistic Map is iterated 30 times to produce the sequence K_3 by Eq. 8,

$$\begin{aligned} &K_3(j, i+1) = (3.999 + K_2(j)/10^5) \times K_3(j, i) \times (1 - K_3(j, i)) \\ &K_3(j, 1) = K_2(j), \quad j = 1, 2, 3, \ldots, 16, i = 1, 2, 3, \ldots, 30 \end{aligned}. \tag{8}$$

Step 5 : The initial key eventually evolves into

$$\begin{cases} k_1 = (K_3(1, 30) + K_3(2, 30) + K_3(3, 30) + K_3(4, 30))/4, \\ k_2 = (K_3(5, 30) + K_3(6, 30) + K_3(7, 30) + K_3(8, 30))/4, \\ k_3 = (K_3(9, 30) + K_3(10, 30) + K_3(11, 30) + K_3(12, 30))/4, \\ k_4 = (K_3(13, 30) + K_3(14, 30) + K_3(15, 30) + K_3(16, 30))/4. \end{cases} \tag{9}$$

Output: k_1, k_2, k_3 and k_4 ($k_1 \in (0, 1)$, $k_2 \in (0, 1)$, $k_3 \in (0, 1)$], and $k_4 \in (0, 1)$)

3.3 Encryption algorithm

Different from the traditional image encryption algorithm of scrambling and then diffusing. The Encrypt for 3D model proposed in this paper is scrambling and diffusing at the same time, which increases the security of the algorithm. The encryption process is described as follow.

Input: P. ($P \in \mathcal{M}_{M\times3}$)

Step 1 : Convert the plaintext P to a new one, that $P \in \mathcal{M}_{M\times3} \rightarrow P \in \mathcal{M}_{1\times3M}$. Divide the floating point number into two parts, the fractional part PO ($PO = P \bmod 1$) and the integer part PN ($PN = P - PO$).

Step 2 : Generate the secret key of the first keystream by Eq. 10,

$$\begin{cases} KN_1 = (k_1 + k_4) \bmod 1, \\ KN_2 = k_2 \bmod 1 \times 100 + 5, \\ KN_3 = k_3 \bmod 1 \times 1000. \end{cases} \tag{10}$$

Step 3 : Generate the first key stream of the cryptosystem by the 1D-SMCLM,

$$X_1: x_{n+1} = \varphi \sin\left(\sin(\pi x_n) \cdot \gamma x_n (1 - x_n) + 1\right) \tag{11}$$

where $x_0 = KN_1$, $\varphi = KN_2$, and $\gamma = KN_3$. When the keystream is generated, the initial point of the iteration needs to be discarded, which is set to 500 in this paper. Then the first keystream is generated which is $X_1 \in \mathcal{M}_{1\times3M}$.

Step 4 : Generate the secret key of the second keystream by Eq. 12

$$\begin{cases} KN_4 = k_1 \bmod 1, \\ KN_5 = (k_2 + k_4) \bmod 1 \times 100 + 5, \\ KN_6 = k_3 \bmod 1 \times 1000. \end{cases} \tag{12}$$

Step 5 : Generate the second keystream of the cryptosystem by the 1D-SMCLM,

$$X_2: x_{n+1} = \varphi \sin\left(\sin(\pi x_n) \cdot \gamma x_n (1 - x_n) + 1\right). \tag{13}$$

where $x_0 = KN_4$, $\varphi = KN_5$, and $\gamma = KN_6$. Then the second keystream is generated which is $X_2 \in \mathcal{M}_{1\times3M}$.

Step 6 : Generate the ordering matrix s required by the cryptosystem. Sort the keystream X_1 from small to large to generate a new sorted key stream SX_1. Pick elements from SX_1 in turn and find the positions of these elements in X_1, recorded as S. In addition, a cryptographic matrix D is generated for the cryptosystem, where $D = floor(X_2 \times 10^{10}) \bmod 256$.

Step 7 : The encryption process is described as follow,

1) $C(S(1)) = (PN(1) + D(S(1))) \bmod 256$.
2) if $i \bmod 2 = 0$, then $C(S(i)) = (PN(i) + D(S(i)) + C(S(i-1))) \bmod 256$, $i = 2, 3, 4, \ldots, 3M$.
3) if $i \bmod 2 = 1$, then $C(S(i)) = PN(i) \oplus D(S(i)) \oplus C(S(i-1)))$, $i = 2, 3, 4, \ldots, 3M$.

Step 8 : Convert the ciphertext to vertex coordinates in STL format, $C = C + PO$ and $C \in \mathcal{M}_{1\times3M} \rightarrow C \in \mathcal{M}_{M\times3}$.

Output: C. ($C \in \mathcal{M}_{M\times3}$)

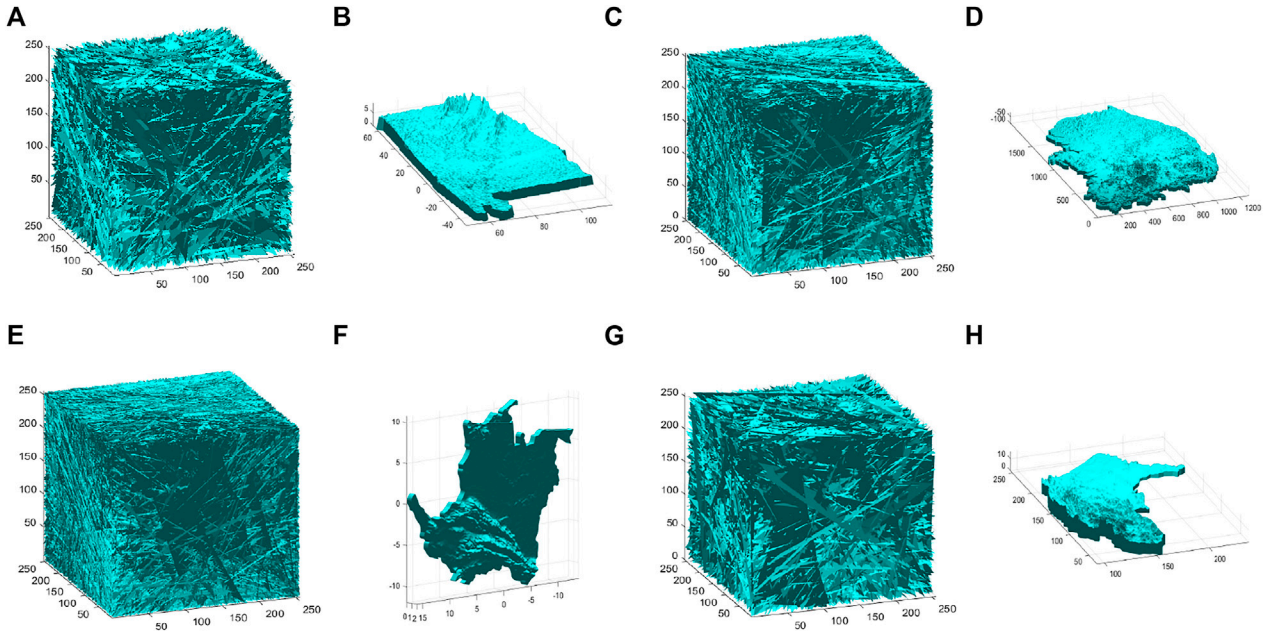

FIGURE 10
Visualization of SMCLM-3ME. **(A)** Encrypted topographic map of the United States. **(B)** Decrypted topographic map of the United States. **(C)** Encrypted topographic map of South Korea. **(D)** Decrypted topographic map of South Korea. **(E)** Encrypted topographic map of Colombia. **(F)** Decrypted topographic map of Colombia. **(G)** Encrypted topographic map of the capital of Australia. **(H)** Decrypted topographic map of the capital of Australia.

The SMCLM-3ME is a symmetric cryptosystem, and the decryption process is the reverse process of encryption. This paper omits the decryption process.

4 Performance analysis

This section analyzes the security of the SMCLM-3ME, including visualization analysis, key analysis, information entropy analysis, statistical analysis, NIST, time analysis, etc.

4.1 Visualization

The visualization analysis results of the SMCLM-3ME are shown in Figure 10. The 3D model selected for visual analysis is shown in Figure 9. Visual analysis includes 3D model encryption and 3D model decryption. Visual analysis results show that SMCLM-3ME has good encryption effect visually and can decrypt without error.

4.2 Key analysis

Key analysis includes key space analysis and key sensitivity analysis. The original key of the SMCLM-3ME is generated by a hash function, and the key space is 2^{256}. When the key space is larger than 2^{100}, the algorithm can resist brute force attacks. Therefore, the SMCLM-3ME has better resistance to brute force attacks.

A secure encryption algorithm cannot decrypt an encrypted image with a wrong key that differs very little from the correct key. The key sensitivity analysis of the SMCLM-3ME is shown in Figure 11. The original key is ψ, and the wrong keys are ψ_1, ψ_2, ψ_3, ψ_4 and ψ_5. ψ = 3159*a*982400*f*77436326*b*3*ebb*3*c*7*c*5*ce*844151*ef* 4*a*89503*b*0*e*77136*fd*6*e*0*f*947.ψ_1 = 3159*a*982400*f*77436326*b*3*ebb* 3*c*7*c*5*ce*844151*ef*4*a*89503*b*0*e*77136*fd*6*e*0*f*948.ψ_2 = 3159*a* 982400 *f*77436326*b*3*ebb*3*c*7*c*5*ce*844151*ef*4*a*89503*b*0*e*77136*fd*6*e*0*f*946.ψ_3= 4159*a*982400*f*77436326*b*3*ebb*3*c*7*c*5*ce*844151*ef*4*a*89503 *b*0*e*7713 6*fd*6*e*0*f*947.ψ_4 = 2159*a*982400*f*77436326*b*3*ebb*3*c*7*c*5*ce*844151*ef* 4*a*89503*b*0*e*77136*fd*6*e*0*f*947.ψ_5 = 3159*a*982400*f*77436326*b*3*ebb* 3*c*7*c*5*ce*844251*ef*4*a*89503*b*0*e*77136*fd*6*e*0*f*947.

The key sensitivity analysis shows that the key of the encryption algorithm is very sensitive. When one bit of the key changes, the obtained encrypted image and decrypted image have a big gap.

4.3 Information entropy analysis

Information entropy is a measure of the chaotic degree of an image. The more chaotic the image, the greater the information entropy. The calculation formula of information entropy is,

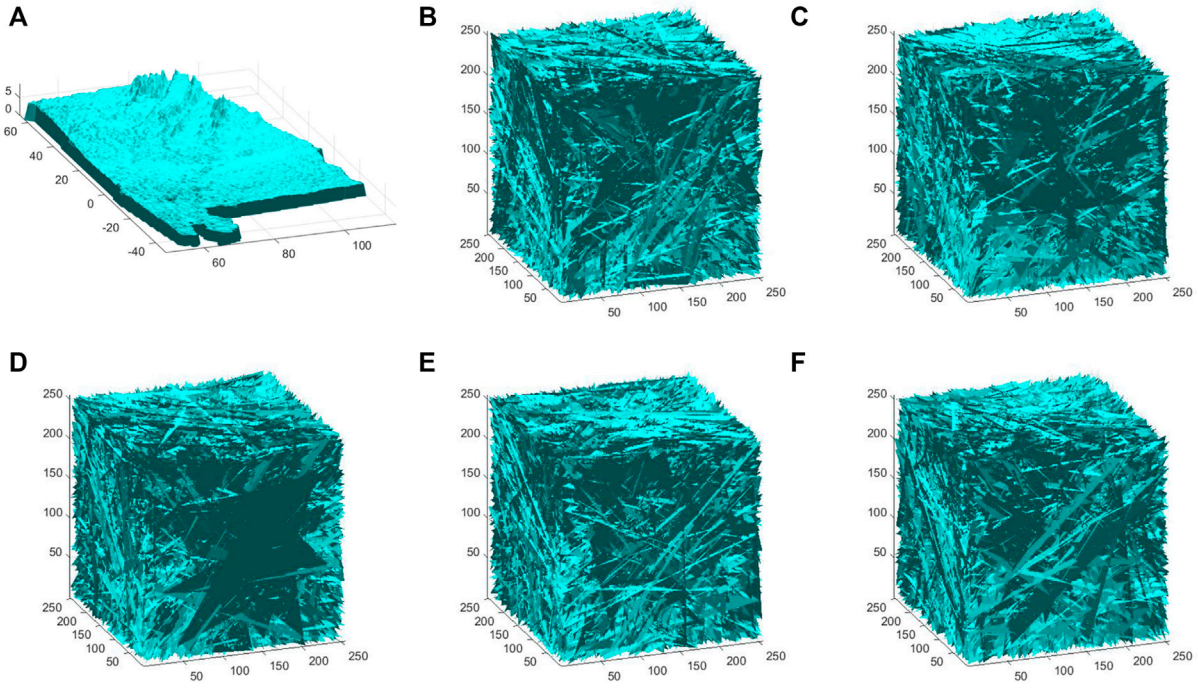

FIGURE 11
Key sensitivity analysis of SMCLM-3ME. **(A)** Decrypted by ψ. **(B)** decrypted by ψ_1. **(C)** Decrypted by ψ_2. **(D)** Decrypted by ψ_3. **(E)** Decrypted by ψ_4. **(F)** Decrypted by ψ_5.

$$H = \sum_{i=0}^{255} p(g_i)\log_2 \frac{1}{p(g_i)}.$$

The information entropy analysis of the SMCLM-3ME is shown in Table 2. In addition, the information entropy of the SMCLM-3ME is compared with some algorithms (Refs. [49, 59, 60]), the comparison results are shown in Table 3. The information entropy comparison shows that the ciphertext information entropy value of the SMCLM-3ME is closer to the theoretical value than the algorithms in Refs. [49, 59, 60], so the ciphertext of the SMCLM-3ME has better randomness, attackers cannot obtain useful information from the ciphertext.

TABLE 2 Information entropy of SMCLM-3ME.

3D models	Plaintext	Ciphertext
Topographic map of the United States	6.7782	7.9994
Topographic map of South Korea	6.6313	7.9999
Topographic map of Colombia	6.4975	7.9999
Topographic map of the capital of Australia	7.0754	7.9994
Average	6.7456	7.9997

4.4 Correlation analysis

A plaintext image has a strong correlation between adjacent pixels, and the purpose of encryption is to eliminate this correlation. The adjacent pixel correlation is defined as,

$$r_\rho = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x) \cdot D(y)}}.$$

In the 3D model, correlation analysis is divided into X-direction correlation, Y-direction correlation, and Z-direction correlation. Taking the Topographic map of Colombia as an example, the correlation analysis of the SMCLM-3ME is shown in Figure 12.

TABLE 3 Information entropy comparison.

Algorithms	SMCLM-3ME	Algorithm [49]	Algorithm [59]	Algorithm [60]
Information entropy	7.9997	7.9988	7.9980	7.9959

Taking the Topographic map of South Korea as an example, the correlation analysis of the SMCLM-3ME is shown in Figure 13.

The quantitative analysis results of the correlation are shown in Table 4, and the correlation comparison with some algorithms (Refs. [48, 49, 59]) are shown in Table 5.

The correlation analysis results show that the SMCLM-3ME can eliminate the strong correlation between the coordinates of the plaintext, and the correlation of the ciphertext becomes very low. This shows that an attacker cannot use a statistical attack to obtain useful information from the ciphertext to crack the algorithm. The correlation comparison results show that the SMCLM-3ME has lower correlations in all three directions, which indicates that the SMCLM-3ME has better resistance to statistical attacks than the algorithm in Refs. [48, 49, 59].

4.5 NIST statistical test suite

In order to verify whether the ciphertext generated by the SMCLM-3ME is random, the NIST test is used on the ciphertext. When the ciphertext passes the NIST test, it indicates that the distribution of ciphertext values is random. The NIST test results of SMCLM-3ME are shown in Table 6. The test results show that the plaintext is not random, while the ciphertext has passed all 15 tests, indicating that the ciphertext has good randomness. The attacker cannot obtain useful information from the ciphertext, so the SMCLM-3ME has high security.

4.6 Robustness analysis

During the transmission process, the image will lose some information or be disturbed by some noise. This section analyzes the ability of the algorithm to resist clipping attacks and noise attacks which are shown in Figure 14.

It can be seen from Figure 14 that SMCLM-3ME has good robustness. Even if part of the image data is lost or interfered by some noise during the transmission process, part of the plaintext information can still be obtained through the decryption algorithm.

4.7 Time analysis

The running environment of the SMCLM-3ME is Windows 10, matlab 2020, i3-10105F. The running time of the SMCLM-3ME is shown in Table 7.

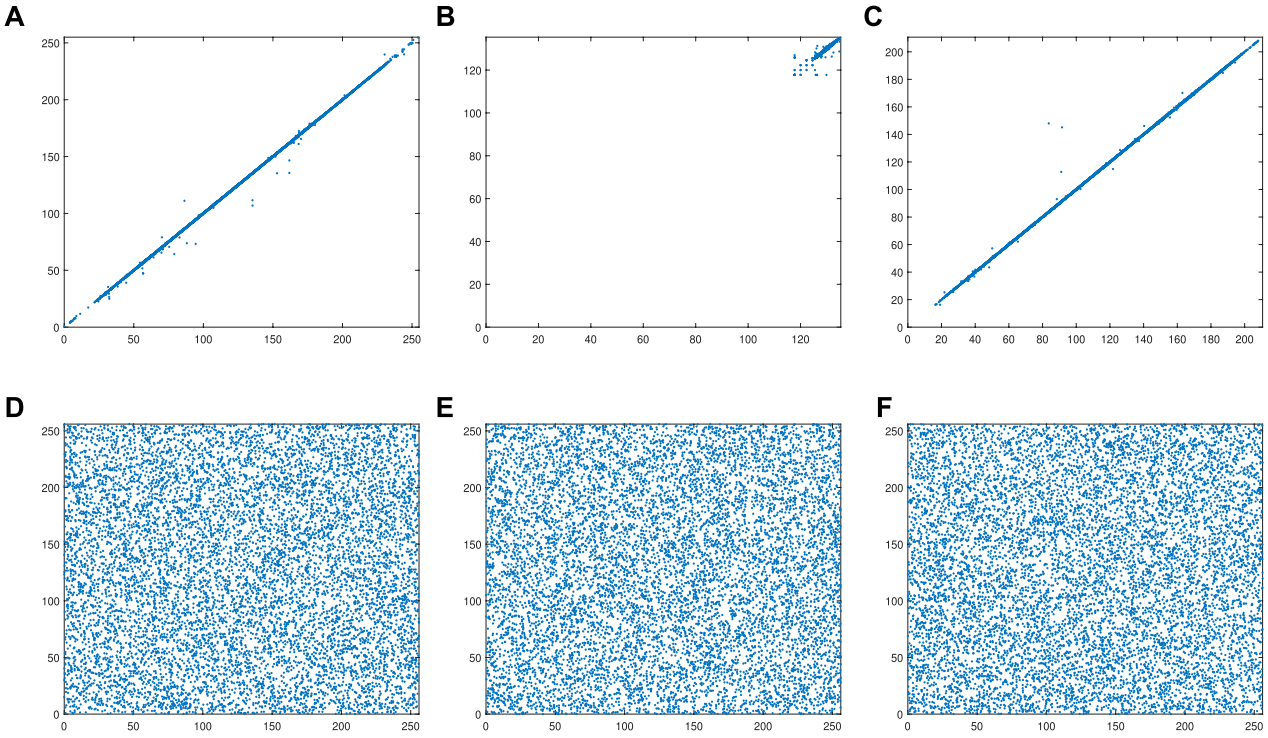

FIGURE 12
Correlation analysis of Topographic map of Colombia. **(A)** X-direction of plaintext. **(B)** Y-direction of plaintext. **(C)** Z-direction of plaintext. **(D)** X-direction of ciphertext. **(E)** Y-direction of ciphertext. **(F)** Z-direction of ciphertext.

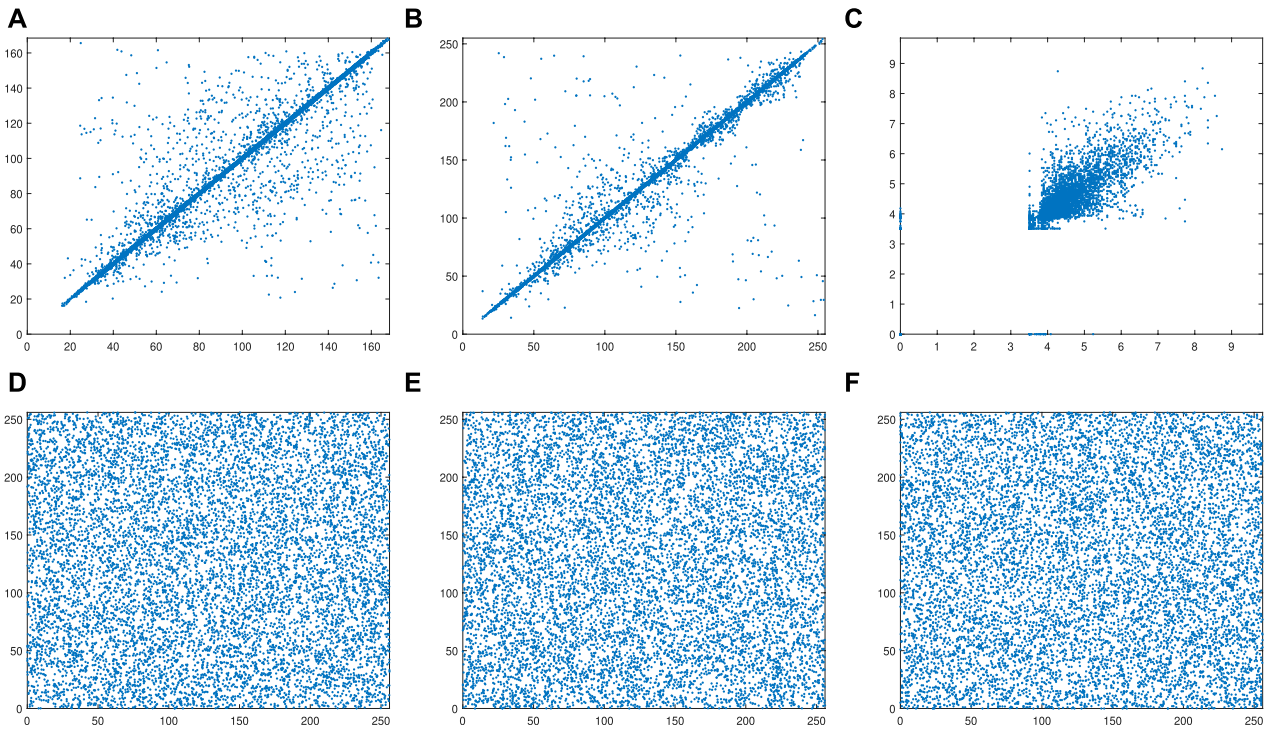

FIGURE 13
Correlation analysis of Topographic map of South Korea. **(A)** X-direction of plaintext. **(B)** Y-direction of plaintext. **(C)** Z-direction of plaintext. **(D)** X-direction of ciphertext. **(E)** Y-direction of ciphertext. **(F)** Z-direction of ciphertext.

TABLE 4 Correlation coefficients of SMCLM-3ME.

Image	Plaintext			Ciphertext		
	X-direction	Y-direction	Z-direction	X-direction	Y-direction	Z-direction
United States	0.9914	0.9999	0.8449	−0.0050	−0.0029	−0.0008
South Korea	0.9462	0.9621	0.9737	0.0022	0.0008	−0.0011
Colombia	0.9996	0.9880	0.9989	0.0010	0.0008	0.00009
Capital of Australia	0.9639	0.9254	0.7848	−0.0024	0.0003	0.0006
Average	0.9753	0.9689	0.9006	−0.0010	−0.0002	−0.0003

TABLE 5 Correlation coefficients comparison.

Algorithms	SMCLM-3ME	Algorithm [48]	Algorithm [49]	Algorithm [59]
X-direction	−0.0010	0.0118	−0.0055	−0.0254
Y-direction	−0.0002	0.0062	0.0081	−0.0097
Z-direction	−0.0003	0.0004	0.0115	0.0049

TABLE 6 Correlation coefficients comparison.

Number	Statistical test	Plaintext		Ciphertext	
		p-value	Result	*p*-value	Result
1	Longest run of ones	0	Fail	0.657933	Pass
2	Overlapping template matching	0	Fail	0.616305	Pass
3	Random excursions variant	0	Fail	0.931952	Pass
4	Rank	0	Fail	0.911413	Pass
5	Frequency	0	Fail	0.319084	Pass
6	Universal	0	Fail	0.122325	Pass
7	Random excursions	0	Fail	0.964295	Pass
8	Block frequency	0	Fail	0.739918	Pass
9	Cumulative sums	0	Fail	0.971699	Pass
10	Runs	0	Fail	0.236810	Pass
11	Serial	0	Fail	0.574903	Pass
12	Spectral	0	Fail	0.699313	Pass
13	Approximate entropy	0	Fail	0.108791	Pass
14	Non-overlapping template matching	0	Fail	0.616305	Pass
15	Linear complexity	0	Fail	0.739918	Pass

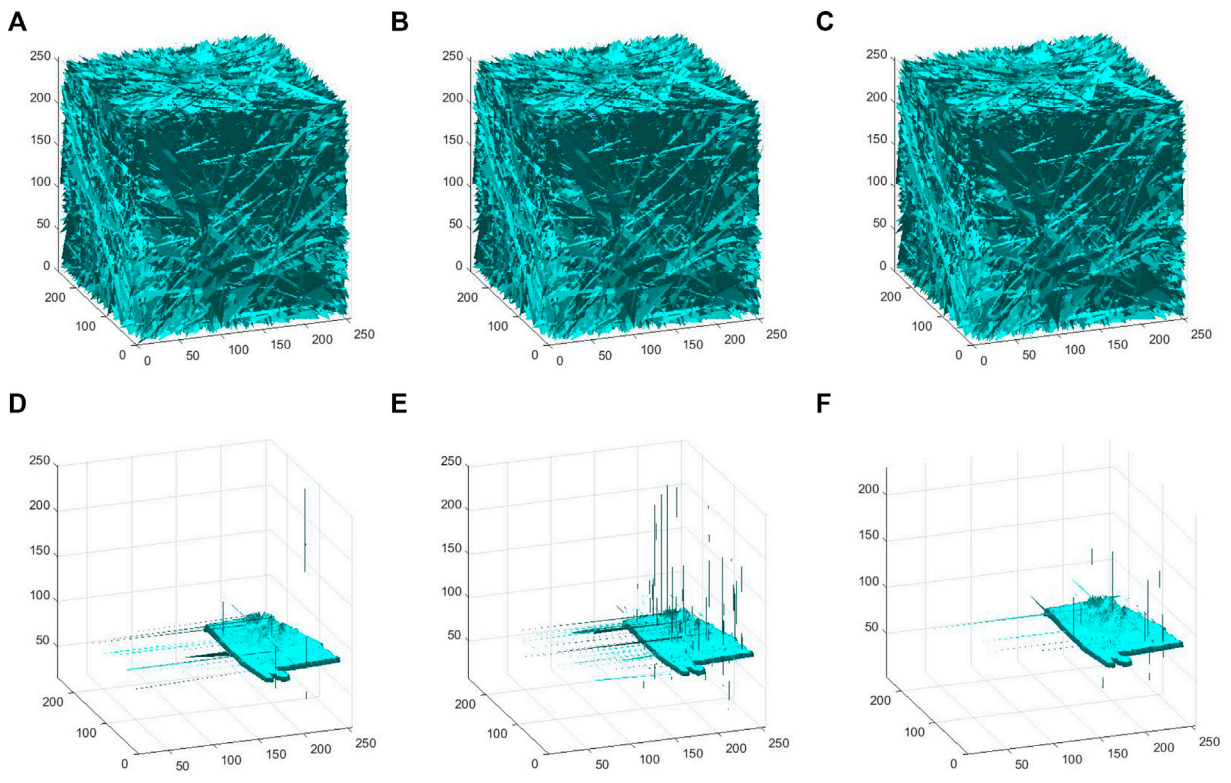

FIGURE 14
Robustness analysis of United States. **(A)** Ciphertext of data loss 10 groups. **(B)** Ciphertext of data loss 50 groups. **(C)** Ciphertext of 0.0001 salt and pepper. **(D)** Decrypted image of **(A)**. **(E)** Decrypted image of **(B)**. **(F)** Decrypted image of **(C)**.

TABLE 7 Time analysis of SMCLM-3ME.

Name of 3D models	Number of coordinate	Time/s
Topographic map of the United States	1,24,407	1.059190
Topographic map of South Korea	7,23,432	6.519195
Topographic map of Colombia	2,461,824	21.201624
Topographic map of the capital of Australia	1,08,396	0.945507

The encryption time in Ref. [49] is 30.1795 s with 348,282 vertex coordinates, where the encryption time in the SMCLM-3ME is 6.519195 s with 723,432 vertex coordinates. The encryption time in Ref. [57] is 7.59 s with 65,536 pixel values, where the encryption time in the SMCLM-3ME is 0.945507s with 108,396 vertex coordinates. The encryption time in Ref. [58] is 21.5 s with 7,86,432 pixel values, where the encryption time in the SMCLM-3ME is 21.201624 s with 2,461,824 vertex coordinates. The encryption time comparison shows that the SMCLM-3ME has a faster running speed.

4.8 Influence analysis of 1D-SMCLM in SMCLM-3ME

In this section, the influence of 1D-SMCLM in SMCLM-3ME is analyzed. In SMCLM-3ME, Logistic Map and Sin Map are used to replace 1D-SMCLM, respectively, and the performance of the obtained ciphertext is analyzed, as shown in Tables 8, 9, 10.

As shown in Tables 8, 9, 10, 1D-SMCLM improves the coding quality of the cryptosystem. On the indicators of the information entropy of the ciphertext and the correlation

TABLE 8 Replace 1D-SMCLM with logistic map in SMCLM-3ME.

Image	X-direction	Y-direction	Z-direction	Information entropy
United States	−0.0032	−0.0024	−0.0031	7.9995
South Korea	0.0016	0.0020	0.0009	7.9999
Colombia	0.0004	0.0005	−0.0001	7.99997
Capital of Australia	−0.0066	−0.0026	−0.0005	7.9994
Average	−0.0019	−0.0006	−0.0007	7.9996

TABLE 9 Replace 1D-SMCLM with sin map in SMCLM-3ME.

Image	X-direction	Y-direction	Z-direction	Information entropy
United States	−0.0011	−0.0006	0.0017	7.9995
South Korea	0.0023	−0.0002	−0.0006	7.9999
Colombia	0.0003	−0.0002	−0.0009	7.9998
Capital of Australia	−0.0013	−0.0024	0.0027	7.9994
Average	0.0005	−0.0008	0.0007	7.9997

TABLE 10 Influence analysis of 1D-SMCLM in SMCLM-3ME.

SMCLM-3ME	X-direction	Y-direction	Z-direction	Information entropy
SMCLM-3ME with 1D-SMCLM	−0.0010	−0.0002	−0.0003	7.9997
SMCLM-3ME with Logistic Map	−0.0019	−0.0006	−0.0007	7.9996
SMCLM-3ME with Sin Map	**0.0005**	**−0.0008**	**0.0007**	**7.9997**

Bold values are the best value among the three methods.

between the adjacent pixels of the ciphertext, using 1D-SMCLM will make the values of these indicators closer to the theoretical values. It is shown that using 1D-SMCLM in the cryptosystem has better security. In addition, 1D-SMCLM has a larger parameter space, and the parameter space in the chaotic state is continuous, which makes 1D-SMCLM a better choice in cryptosystems.

5 Conclusion

This paper proposes a 3D model encryption algorithm based on the 1D-SMCLM to ensure the network's safe transmission of 3D models. A 1D-SMCLM is proposed. Through 2D trajectory analysis, 3D trajectory analysis, Lyapunov exponent, NIST statistical test suite, and 0–1 test, it is verified that the 1D-SMCLM has good performance, the parameter space in the chaotic state is continuous, and the sequence has good randomness, which is very suitable for generating the key stream of the cryptosystem. In the encryption phase, the secret key of the cryptosystem is generated by a hash function, which ensures that the algorithm can resist chosen-plaintext attacks. The 3D model is encrypted by the strategy of scrambling and diffusion simultaneously, and the 1D-SMCLM generates the keystream in the encryption stage. Through visual analysis, key analysis, statistical analysis, time analysis, and ciphertext NIST analysis, it is verified that the SMCLM-3ME has good security. The SMCLM-3ME can resist standard attack methods.

The encryption algorithm in this paper is only for 3D models in STL format. Due to the different storage principles of 3D models in different storage formats, in future work, we will try to propose 3D image encryption algorithms in other formats.

Data availability statement

The raw data supporting the conclusion of this article will be made available by the authors, without undue reservation.

Author contributions

YH: Writing—original draft, Writing—review and editing. XW: Conceptualization, Investigation, Visualization LZ: Methodology, Software.

Funding

Funds for New Generation Information Technology of the Industry-University-Research Innovation Foundation of China University (No. 2020ITA03022).

Conflict of interest

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

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

1. Farah MAB, Guesmi R, Kachouri A, Samet M. A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. *Opt Laser Technol* (2020) 121:105777. doi:10.1016/j.optlastec.2019.105777

2. Gao S., Wu R., Wang X., Wang J., Li Q., Wang C., et al. A 3D model encryption scheme based on a cascaded chaotic system. *Signal Process* (2022) 202:108745. doi:10.1016/j.sigpro.2022.108745

3. Huang X, Dong Y, Zhu H, Ye G. Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image. *Alexandria Eng J* (2022) 61(10): 7637–47. doi:10.1016/j.aej.2022.01.015

4. Gao X, Miao M, Chen X. Multi-image encryption algorithm for 2D and 3D images based on chaotic system. *Front Phys* (2022) 10:498. doi:10.3389/fphy.2022.901800

5. Sha Y, Bu F, Jahanshahi H, Wang L. A chaos-based image encryption scheme using the hamming distance and DNA sequence operation. *Front Phys* (2022) 10:421. doi:10.3389/fphy.2022.911156

6. Toktas A, Erkan U, Toktas F, Yetgin Z. Chaotic map optimization for image encryption using triple objective differential evolution algorithm. *IEEE Access* (2021) 9:127814–32. doi:10.1109/access.2021.3111691

7. Yang F, Mou J, Ma C, Cao Y. Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. *Opt Lasers Eng* (2020) 129:106031. doi:10.1016/j.optlaseng.2020.106031

8. Chai X, Fu X, Gan Z, Lu Y, Chen Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.* (2019) 155:44–62. doi:10.1016/j.sigpro.2018.09.029

9. Liu B, Ye X, Chen Q. Generating infinitely many coexisting attractors via a new 3D cosine system and its application in image encryption. *IEEE Access* (2021) 9:136292–301. doi:10.1109/access.2021.3117570

10. Wang X, Gao S, Yu L, Sun Y, Sun H. Chaotic image encryption algorithm based on bit-combination scrambling in decimal system and dynamic diffusion. *IEEE Access* (2019) 7:103662–77. doi:10.1109/access.2019.2931052

11. Yao X, Chen X, Liu H, Sun L, He L. Adaptive sliding-mode synchronization of the memristor-based sixth-order uncertain chaotic system and its application in image encryption. *Front Phys* (2022) 10:269. doi:10.3389/fphy.2022.863668

12. Yu F, Kong X, Chen H, Yu Q, Cai S, Huang Y, et al. A 6D fractional-order memristive hopfield neural network and its application in image encryption. *Front Phys* (2022) 10:109. doi:10.3389/fphy.2022.847385

13. Mirzaei O, Yaghoobi M, Irani H. A new image encryption method: Parallel sub-image encryption with hyper chaos. *Nonlinear Dyn* (2012) 67(1):557–66. doi:10.1007/s11071-011-0006-6

14. Pourasad Y, Ranjbarzadeh R, Mardani A. A new algorithm for digital image encryption based on chaos theory. *Entropy* (2021) 23(3):341. doi:10.3390/e23030341

15. Si Y, Liu H, Chen Y. Constructing keyed strong S-Box using an enhanced quadratic map. *Int J Bifurcation Chaos* (2021) 31(10):2150146. doi:10.1142/s0218127421501467

16. Si Y, Liu H, Chen Y. Constructing a 3D exponential hyperchaotic map with application to PRNG. *Int J Bifurcation Chaos* (2022) 32(07):2250095. doi:10.1142/s021812742250095x

17. Sun J, Han G, Wang Y. Dynamical analysis of memcapacitor chaotic system and its image encryption application. *Int J Control Autom Syst* (2020) 18(5):1242–9. doi:10.1007/s12555-019-0015-7

18. Hsiao FH. Applying 3DES to chaotic synchronization cryptosystems. *IEEE Access* (2021) 10:1036–50. doi:10.1109/access.2021.3137356

19. Wang C, Ma B, Xia Z, Li J, Li Q, Shi YQ. Stereoscopic image description with trinion fractional-order continuous orthogonal moments. *IEEE Trans Circuits Syst Video Technol* (2021) 32(4):1998–2012. doi:10.1109/tcsvt.2021.3094882

20. Wang X, Liu P. A new full chaos coupled mapping lattice and its application in privacy image encryption. *IEEE Trans Circuits Syst* (2021) 69(3):1291–301. doi:10.1109/tcsi.2021.3133318

21. Wang X, Wang X, Ma B, Li Q, Shi YQ. High precision error prediction algorithm based on ridge regression predictor for reversible data hiding. *IEEE Signal Process Lett* (2021) 28:1125–9. doi:10.1109/lsp.2021.3080181

22. Ma B, Shi YQ. A reversible data hiding scheme based on code division multiplexing. *IEEE Trans Inform Forensic Secur* (2016) 11(9):1914–27. doi:10.1109/tifs.2016.2566261

23. Li Q, Wang X, Ma B, Wang X, Wang C, Gao S, et al. Concealed attack for robust watermarking based on generative model and perceptual loss. *IEEE Trans Circuits Syst Video Technol* (2021) 32:5695–706. doi:10.1109/TCSVT.2021.3138795

24. Erkan U, Toktas A, Toktas F, Alenezi F. 2D e*pi*-map for image encryption. *Inf Sci* (2022) 589:770–89. doi:10.1016/j.ins.2021.12.126

25. Wang Q, Yu S, Li C, Lu J, Fang X, Guyeux C, et al. Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. *IEEE Trans Circuits Syst* (2016) 63(3):401–12. doi:10.1109/tcsi.2016.2515398

26. Hua Z, Zhu Z, Yi S, Zhang Z, Huang H. Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Inf Sci* (2021) 546:1063–83. doi:10.1016/j.ins.2020.09.032

27. Yang F, Mou J, Liu J, Ma C, Yan H. Characteristic analysis of the fractional-order hyperchaotic complex system and its image encryption application. *Signal Process.* (2020) 169:107373. doi:10.1016/j.sigpro.2019.107373

28. Ouannas A, Karouma A, Grassi G, Pham VT, Luong VS. A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. *Alexandria Eng J* (2021) 60(1):1873–84. doi:10.1016/j.aej.2020.11.035

29. Sun J, Zhao X, Fang J, Wang Y. Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization. *Nonlinear Dyn* (2018) 94(4):2879–87. doi:10.1007/s11071-018-4531-4

30. Sun J, Shen Y, Yin Q, Xu C. Compound synchronization of four memristor chaotic oscillator systems and secure communication. *Chaos* (2013) 23(1):013140. doi:10.1063/1.4794794

31. Liu H, Kadir A, Xu C. Color image encryption with cipher feedback and coupling chaotic map. *Int J Bifurcation Chaos* (2020) 30(12):2050173. doi:10.1142/s0218127420501734

32. Wang X, Gao S, Ye X, Shuang Z, Mingxu W. A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system. *Int J Bifurcation Chaos* (2021) 31(01):2150003. doi:10.1142/s0218127421500036

33. Li Y, Li C, Zhang S, Chen G, Zeng Z. A Self-reproduction hyperchaotic map with compound lattice dynamics. *IEEE Trans Ind Electron* (2022) 69(10):10564–72. doi:10.1109/tie.2022.3144592

34. Li X, Mou J, Xiong L, Wang Z, Xu J. Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption. *Opt Laser Technol* (2021) 140:107074. doi:10.1016/j.optlastec.2021.107074

35. Zhang S, Li C, Zheng J, Wang X, Zeng Z, Peng X. Generating any number of initial offset-boosted coexisting chua's double-scroll attractors via piecewise-nonlinear memristor. *IEEE Trans Ind Electron* (2022) 69(7):7202–12. doi:10.1109/tie.2021.3099231

36. Zhang S, Li C, Zheng J, Wang X, Zeng Z, Chen G. Generating any number of diversified hidden attractors via memristor coupling. *IEEE Trans Circuits Syst* (2021) 68(12):4945–56. doi:10.1109/tcsi.2021.3115662

37. Yang Z, Yuan S, Li J, Bai X, Yu Z, Zhou X. An encryption method based on computational ghost imaging with chaotic mapping and DNA encoding. *J Opt* (2022) 24(6):065702. doi:10.1088/2040-8986/ac6597

38. Liu H, Wang X, kadir A. Image encryption using DNA complementary rule and chaotic maps. *Appl Soft Comput* (2012) 12(5):1457–66. doi:10.1016/j.asoc.2012.01.016

39. Sun J, Zang M, Liu P, Wang Y. A secure communication scheme of three-variable chaotic coupling synchronization based on DNA chemical reaction networks. *IEEE Trans Signal Process* (2022) 70:2362–73. doi:10.1109/tsp.2022.3173154

40. Mahmud M, Lee M, Choi JY. Evolutionary-based image encryption using RNA codons truth table. *Opt Laser Technol* (2020) 121:105818. doi:10.1016/j.optlastec.2019.105818

41. Lu Y., Gong M., Huang Z., Zhang J., Chai X., Zhou C. Exploiting compressed sensing (CS) and RNA operations for effective content-adaptive image compression and encryption. *Optik* (2022) 263:169357. doi:10.1016/j.ijleo.2022.169357

42. Wang X, Gao S. Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network. *Inf Sci* (2020) 539:195–214. doi:10.1016/j.ins.2020.06.030

43. Wang X, Gao S. Application of matrix semi-tensor product in chaotic image encryption. *J Franklin Inst* (2019) 356(18):11638–67. doi:10.1016/j.jfranklin.2019.10.006

44. Chai X, Zhi X, Gan Z, Zhang Y, Chen Y, Fu J. Combining improved genetic algorithm and matrix semi-tensor product (STP) in color image encryption. *Signal Process.* (2021) 183:108041. doi:10.1016/j.sigpro.2021.108041

45. Wang X, Gao S. A chaotic image encryption algorithm based on a counting system and the semi-tensor product. *Multimed Tools Appl* (2021) 80(7):10301–22. doi:10.1007/s11042-020-10101-6

46. Zhu L, Jiang D, Ni J, Wang X, Rong X, Ahmad M, et al. A stable meaningful image encryption scheme using the newly-designed 2D discrete fractional-order chaotic map and Bayesian compressive sensing. *Signal Process.* (2022) 195:108489. doi:10.1016/j.sigpro.2022.108489

47. Chai X, Wu H, Gan Z, Han D, Zhang Y, Chen Y. An efficient approach for encrypting double color images into a visually meaningful cipher image using 2D compressive sensing. *Inf Sci* (2021) 556:305–40. doi:10.1016/j.ins.2020.10.007

48. Xu J, Zhao C, Mou J. A 3D image encryption algorithm based on the chaotic system and the image segmentation. *IEEE Access* (2020) 8:145995–6005. doi:10.1109/access.2020.3005925

49. Chu R, Zhang S, Gao X. A novel 3D image encryption based on the chaotic system and RNA crossover and mutation. *Front Phys* (2022) 10:57. doi:10.3389/fphy.2022.844966

50. Wang Y, Yang F. A fractional-order CNN hyperchaotic system for image encryption algorithm. *Phys Scr* (2021) 96(3):035209. doi:10.1088/1402-4896/abd50f

51. Gao X, Yu J, Banerjee S, Yan H, Mou J. A new image encryption scheme based on fractional-order hyperchaotic system and multiple image fusion. *Sci Rep* (2021) 11(1):15737–21. doi:10.1038/s41598-021-94748-7

52. Hosny KM, Kamal ST, Darwish MM. Novel encryption for color images using fractional-order hyperchaotic system. *J Ambient Intell Humaniz Comput* (2022) 13:973–88. doi:10.1007/s12652-021-03675-y

53. Li T, Zhang D. Hyperchaotic image encryption based on multiple bit permutation and diffusion. *Entropy* (2021) 23(5):510. doi:10.3390/e23050510

54. Zhang M, Tong X, Wang Z, Chen P. Joint lossless image compression and encryption scheme based on CALIC and hyperchaotic system. *Entropy* (2021) 23(8):1096. doi:10.3390/e23081096

55. Belazi A, Abd El-Latif AA. A simple yet efficient S-box method based on chaotic sine map. *Optik* (2017) 130:1438–44. doi:10.1016/j.ijleo.2016.11.152

56. May RM. Simple mathematical models with very complicated dynamics. *Nature* (1976) 261(5560):459–67. doi:10.1038/261459a0

57. Chai X, Gan Z, Lu Y, Chen Y, Han D. A novel image encryption algorithm based on the chaotic system and DNA computing. *Int J Mod Phys C* (2017) 28(05):1750069. doi:10.1142/s0129183117500693

58. Wang X, Su Y, Luo C, Nian F, Teng L. Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate. *Multimed Tools Appl* (2022) 81(10):13845–65. doi:10.1007/s11042-022-12220-8

59. Wang X, Xu M, Li Y. Fast encryption scheme for 3D models based on chaos system. *Multimed Tools Appl* (2019) 78(23):33865–84. doi:10.1007/s11042-019-08171-2

60. Joshi AB, Kumar D, Gaffar A, Mishra D. Triple color image encryption based on 2D multiple parameter fractional discrete Fourier transform and 3D Arnold transform. *Opt Lasers Eng* (2020) 133:106139. doi:10.1016/j.optlaseng.2020.106139