Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.036652
Article

Tech Science Press

A Cross-Plane Color Image Encryption Algorithm Based on 1D-SLM

Xiaohong Wang, Huiqing Wu, Yuying Ma and Shuzhen Huang*

School of Artificial Intelligence, Shandong Vocational and Technical University of Engineering, Jinan, 250200, China
*Corresponding Author: Shuzhen Huang. Email: sdgc_whq@suet.edu.cn

Received: 08 October 2022; Accepted: 15 November 2022

Abstract: With the rapid development of 5G technology, it has become fast and easy for people to transmit information on the Internet. Digital images can express information more intuitively, so transmitting information through images has excellent applications. This paper uses a new chaotic system called 1D-Sin-Logistic-Map (1D-SLM). 1D-SLM has two control parameters, which can provide larger parameter space, and the parameter space in the chaotic state is continuous. Through Lyapunov exponent analysis (LE), bifurcation diagrams analysis, spectral entropy analysis (SE), and 0-1 test, it is verified that 1D-SLM has complex dynamic behavior and is very suitable for cryptography. Compared with other 1D chaotic systems, the 1D-SLM has a larger Lyapunov exponent (LE) and spectral entropy (SE). For color image encryption algorithms, only relying on chaotic mapping is not enough to ensure security. So combined with 1D-SLM, we design a color image encryption algorithm, which is implemented by plane expansion, which reduces the correlation between the three channels of color images. The experimental results show that the proposed cross-plane color image encryption algorithm is safe and resistant to common attack methods.

Keywords: Chaos theory; chaotic system; 1D-SLM; image encryption; information security

1 Introduction

Digital images can express information more intuitively, so the transmission of information through images has great applications [1–3]. The ensuing transmission process brings many security risks. Many image protection algorithms have been proposed nowadays [4–8]. Chaos and cryptography have many similarities and connections [9–11]. A chaotic system can generate a pseudo-random key stream with good performance, which is unpredictable and very suitable for cryptography [12–14].

In order to design efficient and secure cryptosystems, image encryption algorithms combined with chaos have gradually become a hot field [15,16]. Kang et al. used two identical 4D chaotic systems to couple into an 8D chaotic system. The system has eight initial values and eight control parameters. The key stream of the cryptosystem is generated by this 8D chaotic system, and combined with 2D-VMD, a new image encryption method is proposed [17]. Yu et al. proposed a 6D fractional-order chaotic system called 6D-FMHNN. They studied this system's coexistence attractor characteristics and applied it to image encryption. The designed algorithm is secure and sensitive to secret keys [18]. Although high-dimensional chaotic systems have more control parameters and can provide a larger parameter space for cryptosystems, their keystream generation efficiency is not high [19–21]. The low-dimensional chaotic system has smaller control parameters, and its key stream generation is efficient. However, the low-dimensional chaotic system has fewer control parameters. The cryptosystem is challenging to resist brute force attacks. This paper designs a new one-dimensional chaotic system called 1D-SLM. This chaotic system has two control parameters, an improvement on the Logistic map. The parameters corresponding to the chaotic region of 1D-SLM are continuous, and the chaotic region is wide, which is very suitable for the design of cryptographic systems.

For color image encryption algorithms, only relying on chaotic mapping is not enough to ensure security [22]. Zhou et al. used a one-dimensional chaotic system to generate multiple different key streams, using different signals to encrypt the three channels of the color image separately. The proposed encryption algorithm is simple and efficient [23]. Wang et al. used the hyperchaotic Lorenz system to generate the key stream of the cryptographic system. In order to enhance the security of the algorithm, they introduced the matrix semi-tensor product diffusion strategy. The encryption algorithm showed promising results on grayscale images. They extended this algorithm to color image encryption [24]. These algorithms encrypt the three channels of the plaintext image simultaneously, ignoring the correlation between the three channels. The attacker can obtain all the plaintext information by deciphering the content of one channel [25,26]. This paper proposes an encryption algorithm for the cross-plane, which treats the three channels as a whole, and the three channels interact with each other during encryption. This design structure increases the algorithm's security, can resist common attack methods, and ensures the security of color images during transmission.

2 Performance Analysis of the New Chaos System

2.1 Existing One-Dimensional Chaotic Systems

Table 1 gives some one-dimensional chaotic systems, including the analytic formulas and control parameters. In Table 1, f_0 is the initial value, f_n is the iterative value. p and q are the control parameters.

Table 1: Existing one-dimensional chaotic systems

Name	Expressions	Parameters
Logistic map [27]	$f_{n+1} = p \cdot f_n(1 - f_n)$	p
Cubic map [28]	$f_{n+1} = p \cdot f_n^3 + (1 - p)f_n$	p
Sin map [29]	$f_{n+1} = p\sin(\pi f_n)$	p
1D-SMCLM [30]	$f_{n+1} = p\sin(q \cdot \sin(\pi f_n) \cdot f_n(1 - f_n) + 1)$	p and q

2.2 New Chaos System 1D-Sin-Logistic-Map

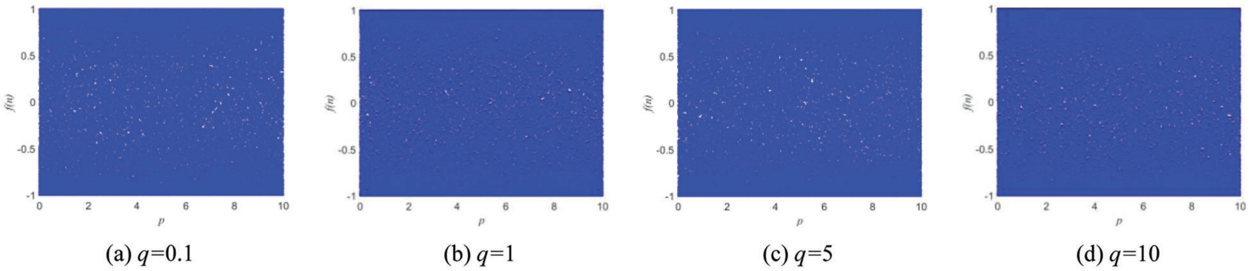
The Logistic map has only one control parameter, the mapping range of the chaotic state is narrow, and the parameters are discontinuous. Therefore, we designed a new chaotic system named 1D-Sin-Logistic-Map (1D-SLM). The 1D-SLM is defined as,

$$f_{n+1} = \sin(\sqrt{q} \cdot (1 - p \cdot f_n \cdot (1 - f_n)) \times 100^2 + 1). \tag{1}$$

In Eq. (1), f_0 is the initial value, $f_0 \in (0,\ 1)$. f_n is the iterative value, $f_n \in (0,\ 1)$. p and q are control parameters, $p \in (0, +\infty)$ and $q \in (0, +\infty)$.

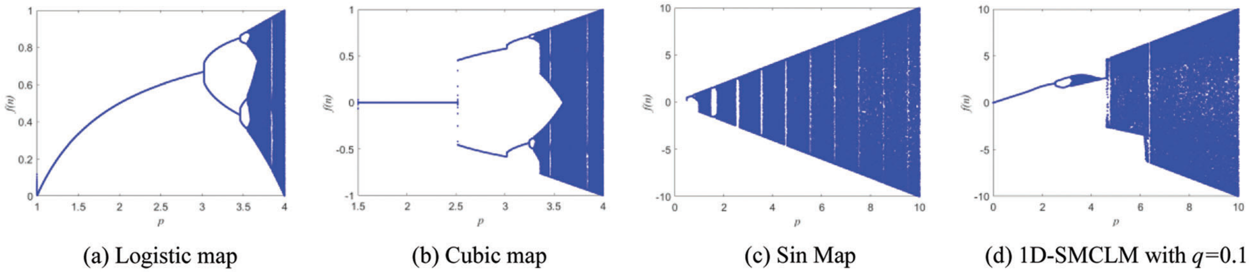
2.3 Bifurcation Diagram of 1D-SLM

The bifurcation diagram reflects the trajectory of the nonlinear dynamic system from the periodic motion state to the chaotic motion state. The Bifurcation diagrams of 1D-SLM are shown in Fig. 1 under different parameter spaces. The Bifurcation diagrams of existing one-dimensional chaotic systems in Table 1 are shown in Fig. 2. Compared with the Logistic map, Cubic map, Sin Map, and 1D-SMCLM, the 1D-SLM has a larger chaotic interval and more complex chaotic behavior.



(a) q=0.1 (b) q=1 (c) q=5 (d) q=10

Figure 1: Bifurcation diagrams of 1D-SLM



(a) Logistic map (b) Cubic map (c) Sin Map (d) 1D-SMCLM with q=0.1

Figure 2: Bifurcation diagrams of existing one-dimensional chaotic systems

2.4 Lyapunov Exponents Analysis

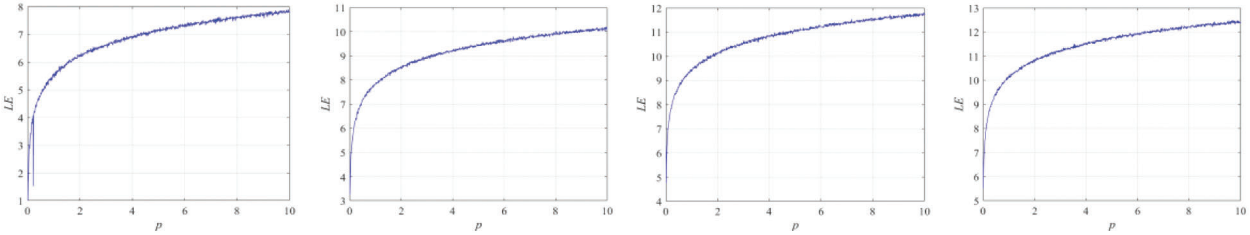
Lyapunov exponents analysis is one of the most effective means of evaluating the dynamic behavior of nonlinear dynamical systems. The LE is defined as [31,32],

$$LE = \lim_{t \to +\infty} \frac{1}{t} \sum_{i=1}^{n-1} \ln|f'(x_i)|. \tag{2}$$

When the Lyapunov exponent is greater than 0, it means that in this parameter space, the system is in a chaotic state. The Lyapunov exponents of 1D-SLM are shown in Fig. 3. The Lyapunov exponents of existing one-dimensional chaotic systems are shown in Fig. 4. It can be seen from Figs. 3 and 4 that the 1D-SLM shows the chaotic global state. Therefore, 1D-SLM can produce a keystream with excellent performance. Compared with other 1D chaotic systems, the 1D-SLM has a larger Lyapunov exponent, and the parameter space in the chaotic state is continuous.

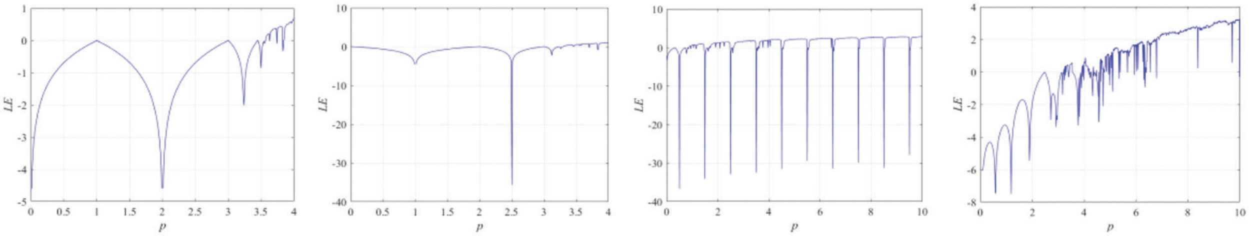
2.5 0–1 Test

The 0–1 test is a test algorithm that measures the presence of chaos in a time series. The 0–1 test of 1D-SLM is shown in Fig. 5. The 0–1 test of existing one-dimensional chaotic systems is shown in Fig. 6. Figs. 5 and 6 show the motion state of 1D-SLM is a Boolean motion state. The Logistic map, Cubic map, Sin map, and 1D-SMCLM exhibit regular motion states in the same parameters. It shows that 1D-SLM can provide sequences with more complex dynamical behavior.



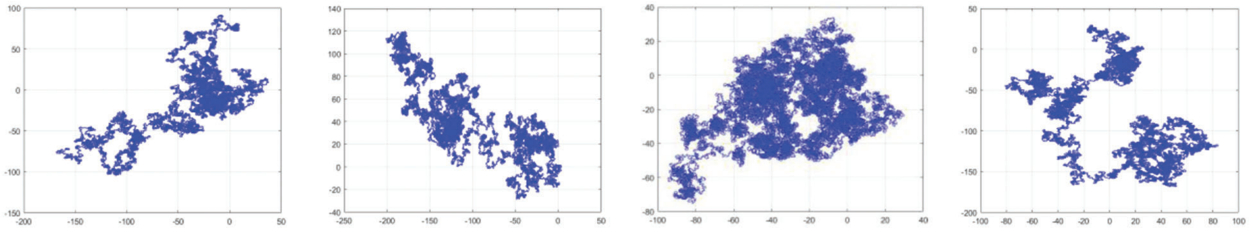
(a) q=0.1 (b) q=1 (c) q=5 (d) q=10

Figure 3: Lyapunov exponents analysis of 1D-SLM



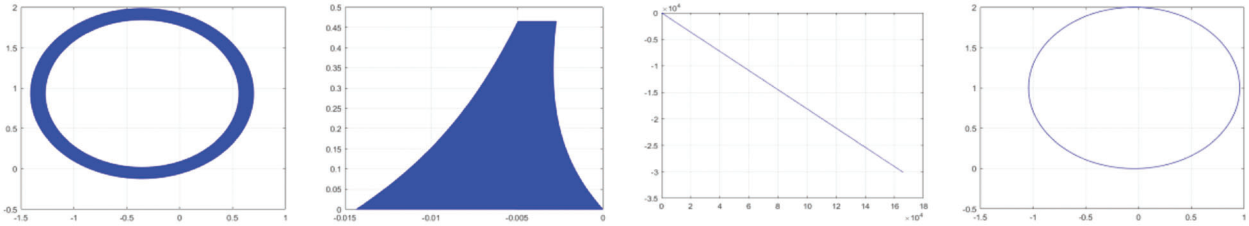
(a) Logistic map (b) Cubic map (c) Sin Map (d) 1D-SMCLM with q=0.1

Figure 4: Lyapunov exponents analysis of existing one-dimensional chaotic systems



(a) q=0.1 and p=0.1 (b) q=2 and p=2 (c) q=3 and p=3.5 (d) q=10 and p=10

Figure 5: 0–1 test analysis of 1D-SLM



(a) Logistic map with p=3.5 (b) Cubic map with p=2 (c) Sin map with p=3.5 (d) 1D-SMCLM with q=0.1

Figure 6: 0–1 test analysis of existing one-dimensional chaotic systems

2.6 Spectral Entropy Analysis

Spectral entropy reflects the energy of the signal. The greater the spectral entropy, the greater the signal's energy and the more complex the dynamic behavior of the signal. The spectral entropy of 1D-SLM and the Logistic map, Cubic map, Sin map, and 1D-SMCLM are shown in Fig. 7. It can be seen from Fig. 7 that compared with the chaotic sequence generated by the Logistic map, Cubic map, Sin map, and 1D-SMCLM, the chaotic sequence generated by 1D-SLM has more potent energy, which indicates that the key stream generated by 1D-SLM has more complex dynamic behavior.

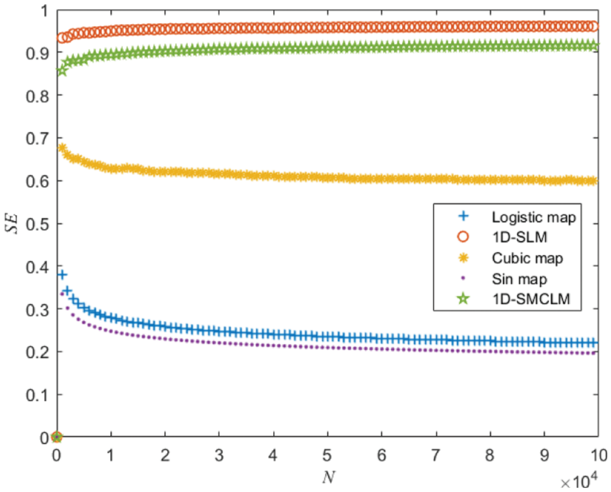


Figure 7: Spectral entropy of 1D-SLM and existing one-dimensional chaotic systems

3 Encryption Algorithm

3.1 Key Generation

The plaintext image is P ($L \times W$), the R channel of the plaintext image is denoted as P_R ($L \times W$), the G channel is denoted as P_G ($L \times W$), and the B channel is denoted as P_B ($L \times W$). Calculate the sum of the plaintext pixel values of each channel by

$$\begin{cases} k_1 = \text{sum}(P_R) \\ k_2 = \text{sum}(P_G) \\ k_3 = \text{sum}(P_B) \end{cases}. \tag{3}$$

The key of the cryptosystem is $K_1 = k_1/k_2,\ K_2 = k_2/k_3,\ K_3 = k_3/k_1$.

3.2 Cross-Plane for Color Images

Given the original initial value v_1 and parameter p_1, q_1 of 1D-SLM. According to the secret key in Section 3.1, the new initial value and parameter are,

$$v_1 = v_1 + K_1,\ p_1 = p_1 + K_2,\ q_1 = q_1 + K_3. \tag{4}$$

The new initial value and parameters are brought into the 1D-SLM iteration to generate the key stream, discard the first 200 iterations of the initial value, denoted as X_1 ($L \times W$), definition

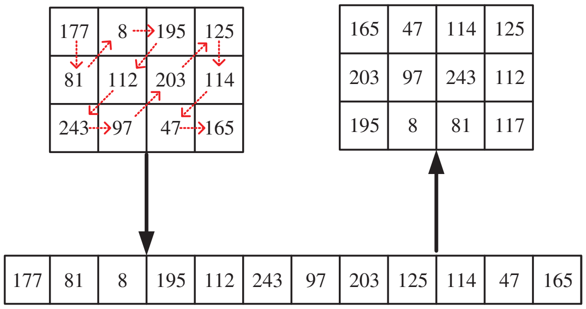
$$U = floor(|X_1 \times 10^{10}|) \bmod 6 + 1. \tag{5}$$

The rule for cross-plane for color images is

$$\begin{cases} P(R_{l,w},\ G_{l,w},\ B_{l,w}) = P(R_{l,w},\ G_{l,w},\ B_{l,w}), & U_{l,w} = 1 \\ P(R_{l,w},\ G_{l,w},\ B_{l,w}) = P(R_{l,w},\ B_{l,w},\ G_{l,w}), & U_{l,w} = 2 \\ P(R_{l,w},\ G_{l,w},\ B_{l,w}) = P(B_{l,w},\ G_{l,w},\ R_{l,w}), & U_{l,w} = 3 \\ P(R_{l,w},\ G_{l,w},\ B_{l,w}) = P(B_{l,w},\ R_{l,w},\ G_{l,w}), & U_{l,w} = 4 \\ P(R_{l,w},\ G_{l,w},\ B_{l,w}) = P(G_{l,w},\ R_{l,w},\ B_{l,w}), & U_{l,w} = 5 \\ P(R_{l,w},\ G_{l,w},\ B_{l,w}) = P(G_{l,w},\ B_{l,w},\ R_{l,w}), & U_{l,w} = 6 \end{cases}. \tag{6}$$

3.3 Zigzag Scrambling

Concatenate the plaintext processed by cross-planes in Section 3.2 into a new plaintext P ($L \times 3W$), in the order of P_R, P_G, and P_B. Perform zigzag scrambling on the new plaintext P to obtain the scrambled matrix S. The zigzag scrambling is shown in Fig. 8.



177	8	195	125
81	112	203	114
243	97	47	165

165	47	114	125
203	97	243	112
195	8	81	117

177	81	8	195	112	243	97	203	125	114	47	165

Figure 8: Zigzag scrambling of 3 × 4

3.4 Diffusion

Given the original initial value v_2 and parameter p_2, q_2 of 1D-SLM. According to the secret key in Section 3.1, the new initial value and parameter are,

$$v_2 = v_2 + K_3,\ p_2 = p_2 + K_1,\ q_2 = q_2 + K_2. \tag{7}$$

The new initial value and parameters are brought into the 1D-SLM iteration to generate the key stream, discard the first 200 iterations of the initial value, denoted as X_2 ($L \times 3W$), definition

$$T = floor(|X_2 \times 10^{10}|) \bmod 256. \tag{8}$$

The diffusion process is

$$\begin{cases} C[1,\ 1] = T[1,\ 1] \oplus S[1,\ 1], \\ C[1,\ u] = T[1,\ u] \oplus S[1,\ u] \oplus C[1,\ u-1],\ u = 2{:}3W, \\ C[v,\ 1] = T[v,\ 1] \oplus S[v,\ 1] \oplus C[v-1,\ 1],\ v = 2{:}L, \\ C[v,\ u] = T[v,\ u] \oplus C[v-1,\ u] \oplus S[v,\ u] \oplus C[v,\ u-1]. \end{cases} \tag{9}$$

Output the ciphertext C, and synthesize the ciphertext color image.

3.5 Decryption Algorithm

The decryption algorithm is shown in Algorithm 1.

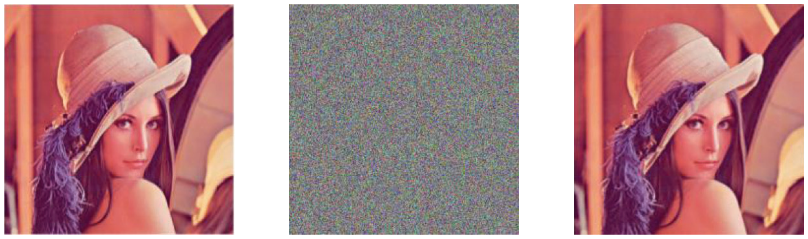
Algorithm 1. Decryption algorithm

```
Input: $C, K_1, K_2, K_3, v_1, p_1, q_1, v_2, p_2, q_2$
Output: $P$
1. $v_1 = v_1 + K_1,\ p_1 = p_1 + K_2,\ q_1 = q_1 + K_3,\ v_2 = v_2 + K_3,\ p_2 = p_2 + K_1,\ q_2 = q_2 + K_2$
2. $X_1 = SLM(v_1, p_1, q_1),\ X_2 = SLM(v_2, p_2, q_2)$
3. $U = floor(abs(X_1 \times 10^{10}))mod6 + 1,\ T = floor(abs(X_2 \times 10^{10}))mod256$
4. for $u = 2:3 \times W$
        $S(1,u) = bitxor(bitxor(T(1,u),C(1,u)),C(1,u-1));$
   end
5. for $v = 2:L$
        $S(v,1) = bitxor(bitxor(T(v,1),C(v,1)),C(v-1,1))$
   end
6. for $u = 2:3 \times W$
      for $v = 2:L$
        $S(v, u) = bitxor(bitxor(T(v,u),C(v-1,u)),bitxor(C(v,u),C(v,u-1)))$
      end
    end
7. $P = iZTransform(S)$ %The inverse process of Scrambling
8. If $U(l,w) = 1,\ P(R(l,w),G(l,w),B(l,w)) = P(R(l,w),G(l,w),B(l,w))$
9. If $U(l,w) = 2,\ P(R(l,w),G(l,w),B(l,w)) = P(R(l,w),B(l,w),G(l,w))$
10. If $U(l,w) = 3,\ P(R(l,w),G(l,w),B(l,w)) = P(B(l,w),G(l,w),R(l,w))$
11. If $U(l,w) = 4,\ P(R(l,w),G(l,w),B(l,w)) = P(B(l,w),R(l,w),G(l,w))$
12. If $U(l,w) = 5,\ P(R(l,w),G(l,w),B(l,w)) = P(G(l,w),R(l,w),B(l,w))$
13. If $U(l,w) = 6,\ P(R(l,w),G(l,w),B(l,w)) = P(G(l,w),B(l,w),R(l,w))$
```

4 Performance Analysis

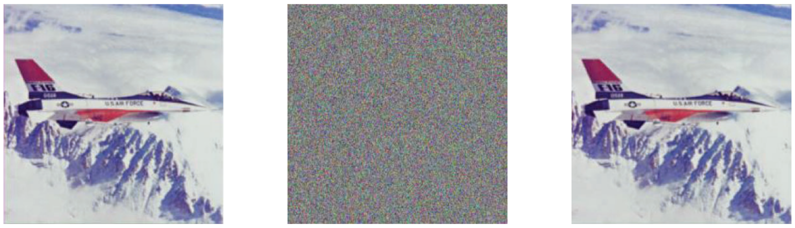
4.1 Simulation Experiments

The visual analysis of the proposed algorithm is shown in Figs. 9–11. Visual analysis shows that, visually, the proposed algorithm is safe.



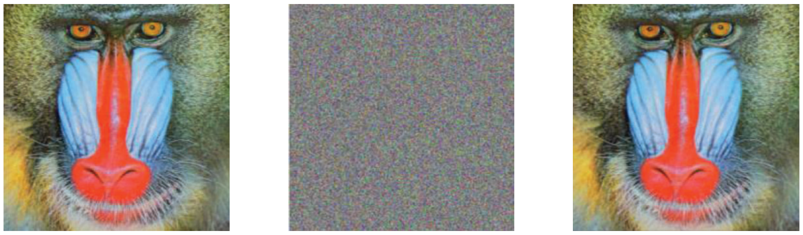
(a) Lena (b) Encrypted Lena (c) Decrypted Lena

Figure 9: Visual analysis of Lena with the size of 512 × 512



(a) Airplane (b) Encrypted Airplane (c) Decrypted Airplane

Figure 10: Visual analysis of Airplane with the size of 512 × 512

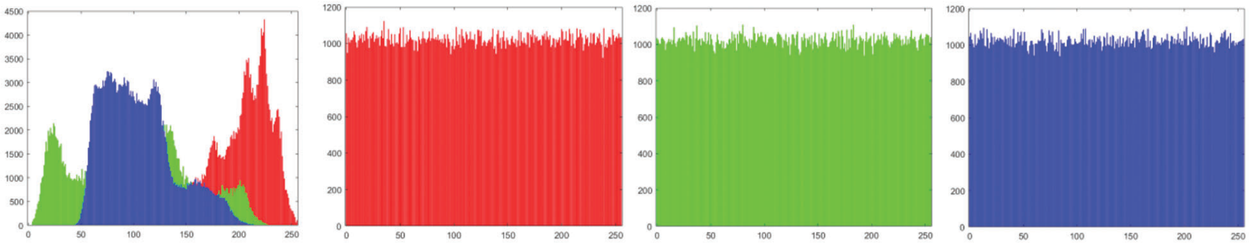


(a) Baboon (b) Encrypted Baboon (c) Decrypted Baboon

Figure 11: Visual analysis of Baboon with the size of 512 × 512

4.2 Histogram Analysis

The histogram analysis of the proposed algorithm is shown in Fig. 12 [33]. Histogram analysis shows that the distribution of pixel values obtained by the proposed algorithm is uniform, and the algorithm has excellent security.



(a) Plaintext (b) Encrypted R-channel (c) Encrypted G-channel (d) Encrypted B-channel

Figure 12: Histogram analysis

4.3 Differential Attack Analysis

A secure algorithm is sensitive to plaintext, and NPCR and UACI are two metrics for detecting plaintext sensitivity [34].

$$\begin{cases} NPCR = \dfrac{\sum_{i,j} \begin{cases} 1, & c_1(i, j) \neq c_2(i, j) \\ 0, & c_1(i, j) = c_2(i, j) \end{cases}}{L \times W} \\ UACI = \dfrac{1}{L \times W} \sum_{i,j} \dfrac{|c1(i, j) - c2(i, j)|}{255} \end{cases} . \tag{10}$$

For a image with the size of 512 × 512, when the value of NPCR is $[99.5893\%,\ 100\%]$, and the value of UACI is $[33.3730\%,\ 33.5541\%]$, at this point, it indicates that the algorithm is sensitive to plaintext. The test results of NPCR and UACI are shown in Table 2. The results of the differential attack show that the algorithm is sensitive to plaintext.

Table 2: Differential attack analysis

Image		NPCR (%)	Pass (Y/N)	UACI (%)	Pass (Y/N)
Lena	R	99.6059	Y	33.4427	Y
	G	99.5914	Y	33.4700	Y
	B	99.6120	Y	33.4747	Y
Airplane	R	99.5960	Y	33.4068	Y
	G	99.6219	Y	33.4579	Y
	B	99.6158	Y	33.4020	Y
Baboon	R	99.6025	Y	33.4966	Y
	G	99.6070	Y	33.4701	Y
	B	99.6120	Y	33.5190	Y
Peppers	R	99.6082	Y	33.6462	Y
	G	99.5964	Y	33.4047	Y
	B	99.6067	Y	33.5091	Y

4.4 NIST for Ciphertext and Plaintext

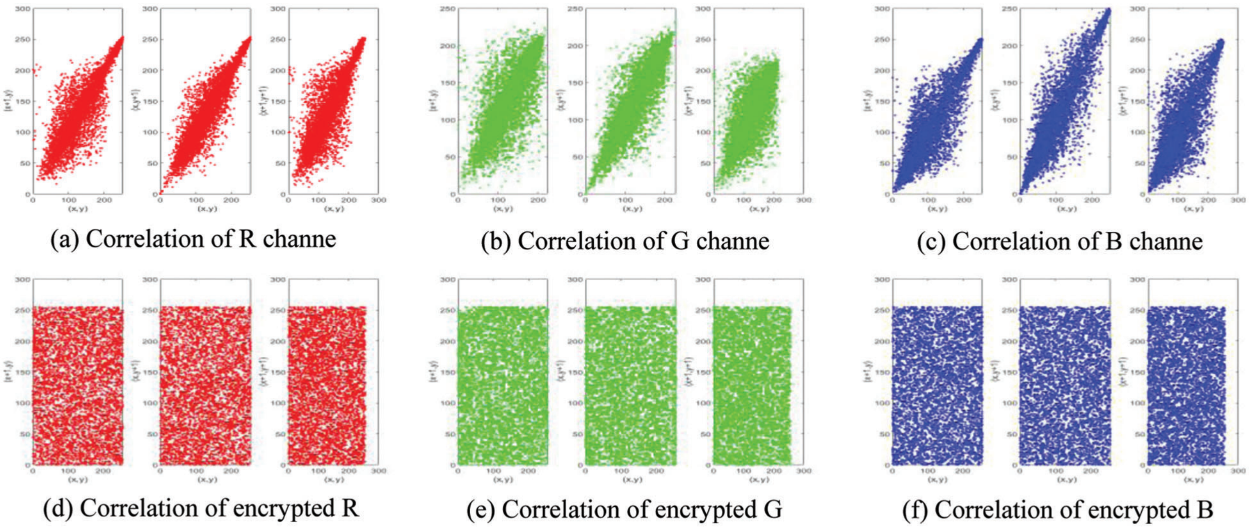
The NIST effectively checks whether the data has randomness [35–37]. The NIST test results of ciphertext and plaintext are shown in Table 3. NIST test results show that the ciphertext has terrific randomness.

Table 3: NIST for ciphertext and plaintext

Sub-tests	Plaintext	Pass (Y/N)	Ciphertext	Pass (Y/N)
Frequency	0	N	0.2932	Y
FFT	0	N	0.0027	Y
Block Frequency	0	N	0.0164	Y
Longest Run	0	N	0.0618	Y
Overlapping Template	0	N	0.1995	Y
Approximate Entropy	0	N	0.2589	Y
Rank	0	N	0.1137	Y
Non-Overlapping Template	0	N	0.5595	Y
Cumulative Sums	0	N	0.4145	Y
Random Excursions	0	N	0.3504	Y
Linear Complexity	0	N	0.3711	Y
Runs	0	N	0.2277	Y
Serial	0	N	0.1516	Y
Random Excursions Variant	0	N	0.5341	Y
Universal	0	N	0.2589	Y

4.5 Adjacent Pixel Correlation Analysis

A secure encryption algorithm can reduce ciphertext's horizontal, vertical, and diagonal adjacent pixel correlations. Otherwise, the algorithm can be easily cracked by statistical attacks. The adjacent pixel correlation analysis of the algorithm is shown in Fig. 13.



(a) Correlation of R channe

(b) Correlation of G channe

(c) Correlation of B channe

(d) Correlation of encrypted R

(e) Correlation of encrypted G

(f) Correlation of encrypted B

Figure 13: Correlation analysis of Baboon

The quantitative results of the correlation analysis of the proposed algorithm are shown in Table 4. The correlation analysis shows that the correlation of the plaintext image in the three directions is very high. The correlation of the ciphertext image in the three directions is very high, close to 0 (theoretical value). Therefore, the proposed encryption algorithm has good security.

Table 4: Correlation coefficients analysis

Image		Plaintext			Ciphertext		
		H	V	D	H	V	D
Lena	R	0.9797	0.9893	0.9696	−0.0001	−0.0012	−0.0019
	G	0.9689	0.9823	0.9554	0.0014	−0.0003	−0.0004
	B	0.9325	0.9574	0.9180	−0.0027	−0.0005	−0.00006
Airplane	R	0.9726	0.9568	0.9343	−0.00009	−0.0006	0.0017
	G	0.9576	0.9676	0.9324	0.0025	−0.0038	0.0005
	B	0.9639	0.9352	0.9145	−0.0010	−0.0015	0.0017
Baboon	R	0.9230	0.8659	0.8543	0.0008	−0.0013	0.0030
	G	0.8654	0.7650	0.7347	−0.0009	−0.0024	0.0025
	B	0.9072	0.8807	0.8397	−0.0016	0.0008	−0.0020
Peppers	R	0.9635	0.9663	0.9563	0.0022	−0.0013	−0.0006
	G	0.9810	0.9817	0.9685	0.0009	−0.0027	0.0022
	B	0.9663	0.9662	0.9476	−0.0013	0.0002	−0.0005

4.6 R, G, B Correlation Analysis

A safe algorithm requires a slight correlation between adjacent pixels and a small correlation between the three channels. The correlation analysis between the three channels of the proposed algorithm is shown in Tables 5 and 6. The results of correlation analysis show that the proposed algorithm can reduce not only the correlation of adjacent pixels but also the correlation between different channels, and the attacker cannot obtain the information of the remaining channels from one channel.

Table 5: Plaintext correlation between R, G, and B

Image	(R, G)	(R, B)	(G, B)
Lena	0.8785	0.6763	0.9104
Airplane	0.9211	0.8410	0.9378
Baboon	0.3565	0.1236	0.8071
Peppers	0.2748	0.3951	0.8377

Table 6: Ciphertext correlation between R, G, and B

Image	(R, G)	(R, B)	(G, B)
Lena	−0.0013	0.0006	0.0031
Airplane	0.0005	0.0007	−0.0007
Baboon	0.0010	0.0004	−0.0041
Peppers	−0.0026	−0.0004	0.0006

4.7 Information Entropy Analysis

The information entropy is defined as

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

Information entropy is an index to analyze the randomness of image information distribution. The higher the information entropy, the more chaotic the information.

The information entropy analysis of the proposed algorithm is shown in Table 7. The local information entropy reflects the degree of local confusion of the image [38]. When the value of local information entropy is between 7.9015 and 7.9034, it indicates that the local information of the image has good randomness. The local information entropy is shown in Table 7. The information entropy analysis results show that the information entropy of the ciphertext is close to the theoretical value, indicating that the algorithm has a good encryption effect.

4.8 Key Analysis

The key space of a cryptographic system is at least greater than 2^{100} that to meet the conditions for resisting brute force attacks. The keys in this paper include v_1, p_1, q_1, v_2, p_2, q_2, K_1, K_2, K_3. If the computational precision of the computer is 10^{14}, the size of the key space of the proposed algorithm is,

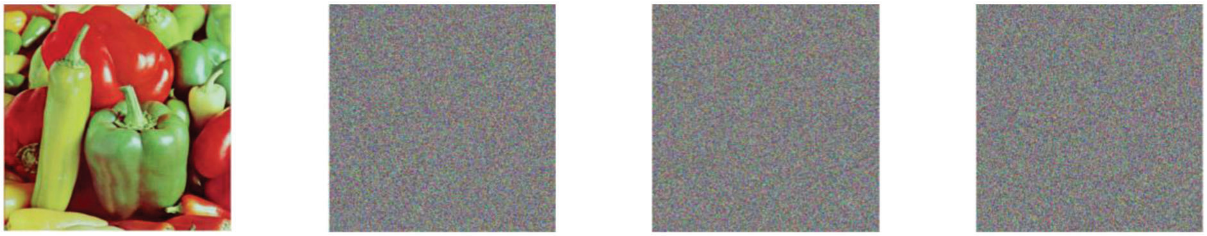
$$K = 10^{14} \times 10^{28} \times 10^{28} \times 10^{14} \times 10^{28} \times 10^{28} \times 10^{14} \times 10^{14} = 10^{168} \approx 2^{558}.$$

The designed algorithm is strong enough to resist brute-force attacks.

Table 7: Information entropy analysis and Local information entropy

Image		IE of plaintext	IE of ciphertext	Local information entropy	Pass or No Pass
Lena	R	7.2530	7.9993	7.9021	Pass
	G	7.5951	7.9993	7.9026	Pass
	B	6.9685	7.9994	7.9022	Pass
Airplane	R	6.7177	7.9992	7.9019	Pass
	G	6.8055	7.9993	7.9030	Pass
	B	6.2139	7.9993	7.9026	Pass
Baboon	R	7.7066	7.9993	7.9025	Pass
	G	7.4752	7.9993	7.9029	Pass
	B	7.7522	7.9993	7.9018	Pass
Peppers	R	7.3388	7.9994	7.9023	Pass
	G	7.5183	7.9993	7.9031	Pass
	B	7.0583	7.9993	7.9023	Pass

A highly sensitive key is a necessary condition for an encryption algorithm. This section tests the key sensitivity of the proposed algorithm, with the initial key set to $v_2 = 0.985612$, $p_2 = 10.36985$, $q_2 = 11.23654$. The key sensitivity analysis is shown in Fig. 14. Key sensitivity analysis shows that the key of the proposed algorithm is sensitive. Calculate the difference between the images in Fig. 14 using NPCR and UACI shown in Table 8 [35,36].



(a) Decrypted with correct key (b) Decrypted with $v_2 + 10^{-14}$ (c) Decrypted with $p_2 + 10^{-14}$ (d) Decrypted with $q_2 + 10^{-14}$

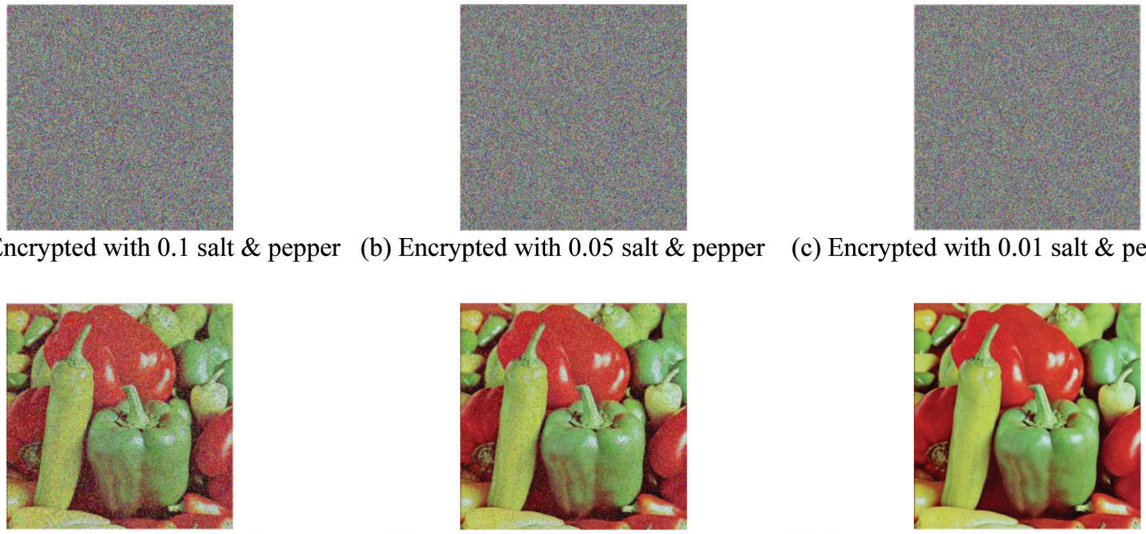
Figure 14: Key sensitivity analysis

Table 8: NPCR and UACI of key sensitivity analysis

NPCR (%) and UACI (%)	Fig. 14a	Fig. 14b	Fig. 14c	Fig. 14d
Fig. 14a	0	32.2304	32.2352	32.2123
Fig. 14b	99.5924	0	33.4445	33.4585
Fig. 14c	99.6063	99.6138	0	33.4996
Fig. 14d	99.6081	99.6105	99.6200	0

4.9 Robustness Analysis

The image will be interfered with by noise during transmission [39]. A safe algorithm should have good resistance to this attack. The robustness analysis of the algorithm is shown in Fig. 15. The PSNR is generally used to measure the restoring ability of images. The results of MSE are shown in Table 9. The results of PSNR are shown in Table 10.



(a) Encrypted with 0.1 salt & pepper (b) Encrypted with 0.05 salt & pepper (c) Encrypted with 0.01 salt & pepper

(d) Decrypted with 0.1 salt & pepper (e) Decrypted with 0.05 salt & pepper (f) Decrypted with 0.01 salt & pepper

Figure 15: Robustness analysis

Table 9: MSE of robustness analysis

Images	MSE	Images	MSE
Figs. 15a and 15d	11413	Fig. 15d and original image	2750
Figs. 15b and 15e	10789	Fig. 15e and original image	1461
Figs. 15c and 15f	10270	Fig. 15f and original image	305

Table 10: PSNR of robustness analysis

Images	PSNR (dB)	Images	PSNR (dB)
Figs. 15a and 15d	7.5565	Fig. 15d and original image	13.7367
Figs. 15b and 15e	7.8006	Fig. 15e and original image	16.4833
Figs. 15c and 15f	8.0148	Fig. 15f and original image	23.2832

4.10 Time Analysis

Efficiency analysis is an important index to evaluate the practicability of an algorithm [40,41]. The efficiency analysis of the proposed algorithm is shown in Table 11. Experimental environment, Matlab R2019a, Windows 11, Intel i3-10105. Efficiency analysis shows that the proposed algorithm has excellent performance and is more practical.

Table 11: Time analysis

Algorithms	Size	Time (s)
Proposed	512 × 512 × 3	**0.9856**
Algorithm in Ref. [42]	512 × 512 × 3	1.4597
Algorithm in Ref. [43]	512 × 512 × 3	1.3053
Algorithm in Ref. [44]	512 × 512 × 3	1.2122
Algorithm in Ref. [45]	512 × 512 × 3	1.2271

4.11 Comparative Analysis

In this section, the proposed algorithm is compared with some classical algorithms, and the comparison results are shown in Table 6. The values in Table 12 are averages. The comparison results show that our algorithm is more secure than the algorithm in Ref. [42], algorithm in Ref. [43], algorithm in Ref. [44], and algorithm in Ref. [45].

Table 12: Comparative analysis

Algorithms	IE	Horizontal	Vertical	Diagonal	Keyspace
Proposed	**7.9993**	**0.0014**	**0.0007**	**0.0008**	$\mathbf{2^{588}}$
Algorithm in Ref. [42]	7.5618	−0.0107	−0.0079	−0.0014	2^{232}
Algorithm in Ref. [43]	7.9993	0.0034	−0.0008	−0.0010	2^{512}
Algorithm in Ref. [44]	7.9993	0.0038	0.0024	0.0020	2^{512}
Algorithm in Ref. [45]	7.9973	0.0060	0.0146	0.0384	2^{189}

5 Conclusion

In this paper, a new chaotic system, 1D-SLM, is proposed. This system has two control parameters that give the cryptosystem a larger key space. It is verified that the key stream generated by 1D-SLM has strong energy and can generate a key stream with excellent performance that is very suitable for cryptography by the Lyapunov exponent, bifurcation graph analysis, and spectral entropy analysis. We propose a new image encryption algorithm based on 1D-SLM. This encryption algorithm combines the three channels of the color image to encrypt simultaneously. In other words, during the encryption process, the three channels of the color image are interactive. This design structure reduces the correlation between image channels. Through performance analysis, it is verified that the proposed algorithm has good performance. Comparative analysis shows that the proposed algorithm has excellent security.

Funding Statement: This research was supported by the National Natural Science Foundation of China (61802212).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] X. Ga, J. Mou, L. Xiong, Y. W. Sha, H. Z. Yan *et al.,* “A fast and efficient multiple images encryption based on single-channel encryption and chaotic system,” *Nonlinear Dynamics*, vol. 108, no. 1, pp. 613–636, 2022.

[2] D. Jerusha and T. Jaya, “Cryptographic lightweight encryption algorithm with dimensionality reduction in edge computing,” *Computer Systems Science and Engineering*, vol. 42, no. 3, pp. 1121–1132, 2022.

[3] M. A. B. Farah, R. Guesmi, A. Kachouri and M. Samet, “A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation,” *Optics and Laser Technology*, vol. 121, pp. 105777, 2020.

[4] B. Ma and Y. Q. Shi, “A reversible data hiding scheme based on code division multiplexing,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 1914–1927, 2016.

[5] C. Wang, B. Ma, Z. Xia, J. Li, Q. Li *et al.,* “Stereoscopic image description with trinion fractional-order continuous orthogonal moments,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 4, pp. 1998–2012, 2022.

[6] Q. Li, X. Wang, B. Ma, X. Wang, C. Wang *et al.,* “Concealed attack for robust watermarking based on generative model and perceptual loss,” *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 8, pp. 5695–5706, 2022.

[7] X. Wang, X. Wang, B. Ma, Q. Li and Y. Shi, “High precision error prediction algorithm based on ridge regression predictor for reversible data hiding,” *IEEE Signal Processing Letters*, vol. 28, pp. 1125–1129, 2021.

[8] S. Gao, R. Wu, X. Wang, J. Wang, Q. Li *et al.,* “A 3D model encryption scheme based on a cascaded chaotic system,” *Signal Processing*, vol. 202, pp. 108745, 2023.

[9] Z. Hua, Y. Zhou and H. Huang, “Cosine-transform-based chaotic system for image encryption,” *Information Sciences*, vol. 480, pp. 403–419, 2019.

[10] Y. Chen, S. Xie and J. Zhang, “A novel double image encryption algorithm based on coupled chaotic system,” *Physica Scripta*, vol. 97, no. 6, pp. 065207, 2022.

[11] R. Wu, S. Gao, X. Wang, S. Liu, Q. Li *et al.,* “AEA-NCS: An audio encryption algorithm based on a nested chaotic system,” *Chaos, Solitons and Fractals*, vol. 165, pp. 112770, 2022.

[12] Y. Xian and X. Wang, “Fractal sorting matrix and its application on chaotic image encryption,” *Information Sciences*, vol. 547, pp. 1154–1169, 2021.

[13] S. Wang, Q. Peng and B. Du, “Chaotic color image encryption based on 4D chaotic maps and DNA sequence,” *Optics and Laser Technology*, vol. 148, pp. 107753, 2022.

[14] J. Arif, M. A. Khan, B. Ghaleb, J. Ahmad, A. Munir *et al.,* “A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution,” *IEEE Access*, vol. 10, pp. 12966–12982, 2022.

[15] Z. Man, J. Li, X. Di, Y. H. Sheng and Z. F. Liu, “Double image encryption algorithm based on neural network and chaos,” *Chaos, Solitons and Fractals*, vol. 152, pp. 111318, 2021.

[16] Q. Wang, S. Yu, C. Li, J. H. Lu, X. L. Fang *et al.,* “Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 63, no. 3, pp. 401–412, 2016.

[17] S. Kang, Y. Liang, Y. Wang and V. I. Mikulovich, “Color image encryption method based on 2D-variational mode decomposition,” *Multimedia Tools and Applications*, vol. 78, no. 13, pp. 17719–17738, 2019.

[18] F. Yu, X. Kong, H. Chen, Q. L. Yu, S. Cai *et al.,* “A 6D fractional-order memristive hopfield neural network and its application in image encryption,” *Frontiers in Physics*, vol. 10, pp. 847385, 2022.

[19] J. Xu, B. Zhao and Z. Wu, “Research on color image encryption algorithm based on bit-plane and chen chaotic system,” *Entropy*, vol. 24, no. 2, pp. 186, 2022.

[20] S. Patel and T. Veeramalai, “Image encryption using a spectrally efficient halton logistics tent (halt) map and DNA encoding for secured image communication,” *Entropy*, vol. 24, no. 6, pp. 803, 2022.

[21] J. Mou, F. Yang, R. Chu and Y. H. Cao, “Image compression and encryption algorithm based on hyper-chaotic map,” *Mobile Networks and Applications*, vol. 26, no. 5, pp. 1849–1861, 2021.

[22] P. Liu, T. Zhang and X. Li, “A new color image encryption algorithm based on DNA and spatial chaotic map,” *Multimedia Tools and Applications*, vol. 78, no. 11, pp. 14823–14835, 2019.

[23] S. Zhou, X. Wang, M. Wang and Y. Zhang, "Simple colour image cryptosystem with very high level of security," *Chaos, Solitons and Fractals*, vol. 141, pp. 110225, 2020.

[24] X. Wang and S. Gao, "Application of matrix semi-tensor product in chaotic image encryption," *Journal of the Franklin Institute*, vol. 356, no. 18, pp. 11638–11667, 2019.

[25] C. L. Li, Y. Zhou, H. M. Li, W. Feng and J. R. Du, "Image encryption scheme with bit-level scrambling and multiplication diffusion," *Multimedia Tools and Applications*, vol. 80, no. 12, pp. 18479–18501, 2021.

[26] H. Zhu, L. Dai, Y. Liu and L. J. Wu, "A three-dimensional bit-level image encryption algorithm with rubik's cube method," *Mathematics and Computers in Simulation*, vol. 185, pp. 754–770, 2021.

[27] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459, 1976.

[28] A. Yahi, T. Bekkouche, M. Daachi and N. Diffellah, "A color image encryption scheme based on 1D cubic map," *Optik*, vol. 249, pp. 168290, 2022.

[29] A. Belazi, A. A. Abd El-Latif, "A simple yet efficient S-box method based on chaotic sine map," *Optik*, vol. 130, pp. 1438–1444, 2017.

[30] Y. Hu, X. Wang and L. Zhang, "1D sine-map-coupling-logistic-map for 3D model encryption," *Frontiers in Physics*, vol. 10, pp. 1006324, 2022.

[31] M. Turkyilmazogl, "An extended epidemic model with vaccination: Weak-immune SIRVI," *Physica A: Statistical Mechanics and its Applications*, vol. 598, pp. 127429, 2022.

[32] M. T. Rosenstein, J. J. Collins and C. J. De Luca, "A practical method for calculating largest lyapunov exponents from small data sets," *Physica D: Nonlinear Phenomena*, vol. 65, no. 1–2, pp. 117–134, 1993.

[33] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[34] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications*, vol. 1, no. 2, pp. 31–38, 2011.

[35] J. Zaman and R. Ghosh, "Review on fifteen statistical tests proposed by NIST," *Journal of Theoretical Physics and Cryptography*, vol. 1, pp. 18–31, 2012.

[36] E. Yavuz, R. Yazici, M. C. Kasapbasi and E. Yamac, "A chaos-based image encryption algorithm with simple logical functions," *Computers and Electrical Engineering*, vol. 54, pp. 471–483, 2016.

[37] Z. Hua, F. Jin, B. X. Xu and H. J. Huang, "2D logistic-sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148–161, 2018.

[38] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan *et al.,* "Local shannon entropy measure with statistical tests for image randomness," *Information Sciences*, vol. 222, pp. 323–342, 2013.

[39] E. Yavuz, "A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme," *Optics and Laser Technology*, vol. 114, pp. 224–239, 2019.

[40] E. Yavuz, "A new parallel processing architecture for accelerating image encryption based on chaos," *Journal of Information Security and Applications*, vol. 63, pp. 103056, 2021.

[41] S. Amina and F. K. Mohamed, "An efficient and secure chaotic cipher algorithm for image content preservation," *Communications in Nonlinear Science and Numerical Simulation*, vol. 60, pp. 12–32, 2018.

[42] Y. G. Yang, B. P. Wang, Y. H. Zhou, W. M. Shi and X. Liao, "Efficient color image encryption by color-grayscale conversion based on steganography," *Multimedia Tools and Applications*, 2022. https://doi.org/10.1007/s11042-022-13689-z.

[43] H. Qiu, X. Xu, Z. Jiang, K. H. Sun and C. W. Xiao, "A color image encryption algorithm based on hyperchaotic map and rubik's cube scrambling," *Nonlinear Dynamics*, 2022. https://doi.org/10.1007/s11071-022-07756-1.

[44] M. Demirtas, "A new RGB color image encryption scheme based on cross-channel pixel and bit scrambling using chaos," *Optik*, vol. 265, pp. 169430, 2022.

[45] M. Xiao, R. Tan, H. Ye, L. H. Gong and Z. Zhu, "Double-color-image compression-encryption algorithm based on quaternion multiple parameter dfrat and feature fusion with preferable restoration quality," *Entropy*, vol. 24, no. 7, pp. 941, 2022.