Computers, Materials & Continua
DOI: 10.32604/cmc.2023.036090
Article

Tech Science Press
check for updates

A Novel 2D Hyperchaotic with a Complex Dynamic Behavior for Color Image Encryption

Yongsheng Hu* **and Liyong Nan**

School of Information Engineering, Binzhou University, Binzhou City, Shandong Province, 256603, China
*Corresponding Author: Yongsheng Hu. Email: huys1208@bzu.edu.cn
Received: 16 September 2022; Accepted: 27 October 2022

Abstract: The generation method of the key stream and the structure of the algorithm determine the security of the cryptosystem. The classical chaotic map has simple dynamic behavior and few control parameters, so it is not suitable for modern cryptography. In this paper, we design a new 2D hyperchaotic system called 2D simple structure and complex dynamic behavior map (2D-SSCDB). The 2D-SSCDB has a simple structure but has complex dynamic behavior. The Lyapunov exponent verifies that the 2D-SSCDB has hyperchaotic behavior, and the parameter space in the hyperchaotic state is extensive and continuous. Trajectory analysis and some randomness tests verify that the 2D-SSCDB can generate random sequences with good performance. Next, to verify the excellent performance of the 2D-SSCDB, we use the 2D-SSCDB to generate a keystream for color image encryption. In the encryption algorithm, the encryption algorithm scrambles and diffuses simultaneously, increasing the cryptographic system's security. The horizontal correlation, vertical correlation, and diagonal correlation of ciphertext are −0.0004, −0.0004 and 0.0007, respectively. The average information entropy of the ciphertext is 7.9993. In addition, the designed encryption algorithm reduces the correlation between the three channels of the color image. Security analysis shows that the color image encryption algorithm designed using 2D-SSCDB has good security, can resist standard attack methods, and has high efficiency.

Keywords: Chaos theory; 2D-SSCDB; cryptography; image encryption

1 Introduction

Image is an essential carrier of information. Due to the openness of the network environment, digital images are inevitably subject to various illegal attacks during the transmission process, and essential information in images will be stolen [1–3]. They are ensuring that privacy is not leaked, and the safe transmission of images in the network has become a significant research problem in the field of information security [4–7]. Many image protection methods have been proposed, such as image steganography, image encryption technology, image watermarking technology, and so on [8–13]. Image encryption technology is one of the most widely used technologies. Image encryption

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

technology converts the original plaintext information into a noise image completely different from the plaintext information, thereby realizing image encryption [14–16].

Because of the large amount of image data and the strong correlation between adjacent pixels, traditional advanced encryption standard (AES), triple data encryption algorithm (3DES), and other methods are not suitable for image encryption, these methods cannot reduce the correlation of adjacent pixels in the image, and the efficiency is very slow [17]. The generation method and algorithm structure of the keystream determine the security of the image encryption algorithm [18–20]. With the introduction of chaos theory, because the sequence generated by a chaotic system has some good characteristics such as pseudo-randomness, initial value sensitivity, secret key sensitivity, ergodicity, etc., the sequence generated by the chaotic system is very suitable for generating the secret of the cryptographic system [21–25]. Therefore, the image encryption algorithm combined with chaos theory has become the mainstream research method in image encryption [26–28].

The chaos system is divided into a one-dimensional chaotic system, a two-dimensional chaotic system, and a high-dimensional chaotic system. A one-dimensional chaotic system has the characteristics of simple structure and fast generation of keystream [29–34]. For example, Li et al. used tent maps to generate keystreams in image encryption [30]. In order to expand the parameter space of the cryptosystem, Chen et al. used a new chaotic system to generate the key stream, composed of a logistic map, sine map, and Chebyshev map [33]. However, a one-dimensional chaotic system has few control parameters and a small parameter space in a chaotic state. Since a one-dimensional chaotic system has only one Lyapunov exponent, it can only exhibit chaotic behavior rather than hyperchaotic behavior. Hyperchaotic behavior is a more complex dynamical behavior compared with chaotic behavior. High-dimensional chaos has the characteristics of complex dynamic behavior and complex structure [35–38]. For example, Liu et al. proposed a new 3D chaotic system and generated an S-box for the encryption algorithm based on this chaotic system [36]. Wang et al. proposed a new spatiotemporal chaotic system, analyzed the performance of this spatiotemporal system, and proposed a new image encryption algorithm combined with this spatiotemporal system, which showed good security properties [38]. Due to the complex structure of the hyperchaotic system, the speed of generating the key stream is very slow, and it is challenging to realize this structure in practical applications.

In order to balance the performance of the high-dimensional and one-dimensional chaotic systems, it is the best choice to use a 2D chaotic system to generate a key stream. Many 2D chaotic systems have been proposed. Although they can exhibit excellent performance, they are pretty complex, and the parameter space in the hyperchaotic state is discontinuous [39,40]. Zheng et al. proposed a 2D logistic sine chaotic map (2D-LSMM), and designed a dynamic image encryption scheme combined with DeoxyriboNucleic Acid (DNA) coding. However, the parameter space of 2D-LSMM is very small which are $\mu_1 \in [0, 4]$ and $\mu_2 \in [0, 4]$ [41]. Teng et al. proposed a 2D cross-logistic-sin-sin (2D-CLSS), and proposed an image encryption strategy based on 2D-CLSS. However, the phase diagram distribution of 2D-CLSS is uneven and there is only one control parameter, which means that the sequences generated by 2D-CLSS will be in an aggregated state [42]. To overcome these shortcomings, this paper proposes a new 2D chaotic system called 2D-SSCDB, which has a simple structure but complex dynamic behavior. The 2D-SSCDB has ample parameter space, and the parameter space in the hyperchaotic state is continuous. These advantages show that the 2D-SSCDB is very suitable for generating keystreams.

Furthermore, to verify the practicality of the 2D-SSCDB, we propose a color image encryption algorithm based on the 2D-SSCDB. In the encryption algorithm, the secret key of the cryptosystem is

generated from the plaintext. In the encryption stage, scrambling and diffusion are carried out simultaneously, which increases the algorithm's security, and the attacker needs to break the scrambling and diffusion operations simultaneously. The experimental results verify that the 2D-SSCDB can be well applied in chaotic image encryption.

2 2D-SSCDB

In this paper, a 2D hyperchaotic system with simple structure, complex dynamic behavior and continuous chaotic parameter space is proposed, called 2D-SSCDB. The 2D-SSCDB is derived from Sine map, Logistic map, the defined of the 2D-SSCDB is shown in Eq. (1),

$$\begin{cases} x_{n+1} = \sin(\mu x_n(1 - y_n) + 1), \\ y_{n+1} = \sin(\eta/(x_n + y_n) + 1) \end{cases} \tag{1}$$

where μ and η are the control parameters of the 2D-SSCDB, $\mu \in R^+$ and $\eta \in R^+$. x_0 and y_0 are the initial values of the 2D-SSCDB.

2.1 Lyapunov Exponent Analysis

The Lyapunov exponent is one of the most effective methods to test whether the nonlinear dynamical system is in chaotic or hyperchaotic state. If a two-dimensional chaotic system has two positive Lyapunov exponents, the system is hyperchaotic in this parameter space. Hyperchaotic behavior has more complex dynamical behavior compared to chaotic behavior. The calculation formula of Lyapunov exponent is shown in Eq. (2),

$$\lambda = \lim_{T \to +\infty} \frac{1}{T} \sum_{t=0}^{T} |f'(x_t)|. \tag{2}$$

The Lyapunov exponent analysis of the 2D-SSCDB is shown in Fig. 1, and compare the Lyapunov exponent with Logistic Map and cascade modulation couple with two 1D-chaotic map (2D-SCMCI) [39].

At $\eta = 2$, the 2D-SSCDB exhibits weak dynamic behavior when $\mu \leq 6.921$, the 2D-SSCDB exhibits strong dynamic behavior when $\mu > 6.921$. At $\eta = 5$, the 2D-SSCDB presents a chaotic state, and the behavior of hyperchaotic states alternately appears. With η increasing gradually, the period window gradually disappears. At $\eta = 7.2$, the period window disappears completely, when $\mu < 2.151$, the 2D-SSCDB presents a chaotic state, and when $\mu \geq 2.151$, the 2D-SSCDB presents a hyperchaotic state. Thereafter, the 2D-SSCDB exhibits stable kinetic behavior with η increasing gradually. Compared with Logistic Map, the 2D-SSCDB has more complex dynamic behavior. Compared with the 2D-SCMCI, the parameter space of the 2D-SSCDB in hyperchaotic state is continuous. Therefore, the 2D-SSCDB has better expressiveness.

In order to generate chaotic sequences with excellent performance, the range of parameters we choose in the cryptosystem is $\eta \geq 7.2$, and $\mu \geq 3$. At this time, the state of 2D-SSCDB is hyperchaotic, which means that the sequence generated by it has excellent randomness.

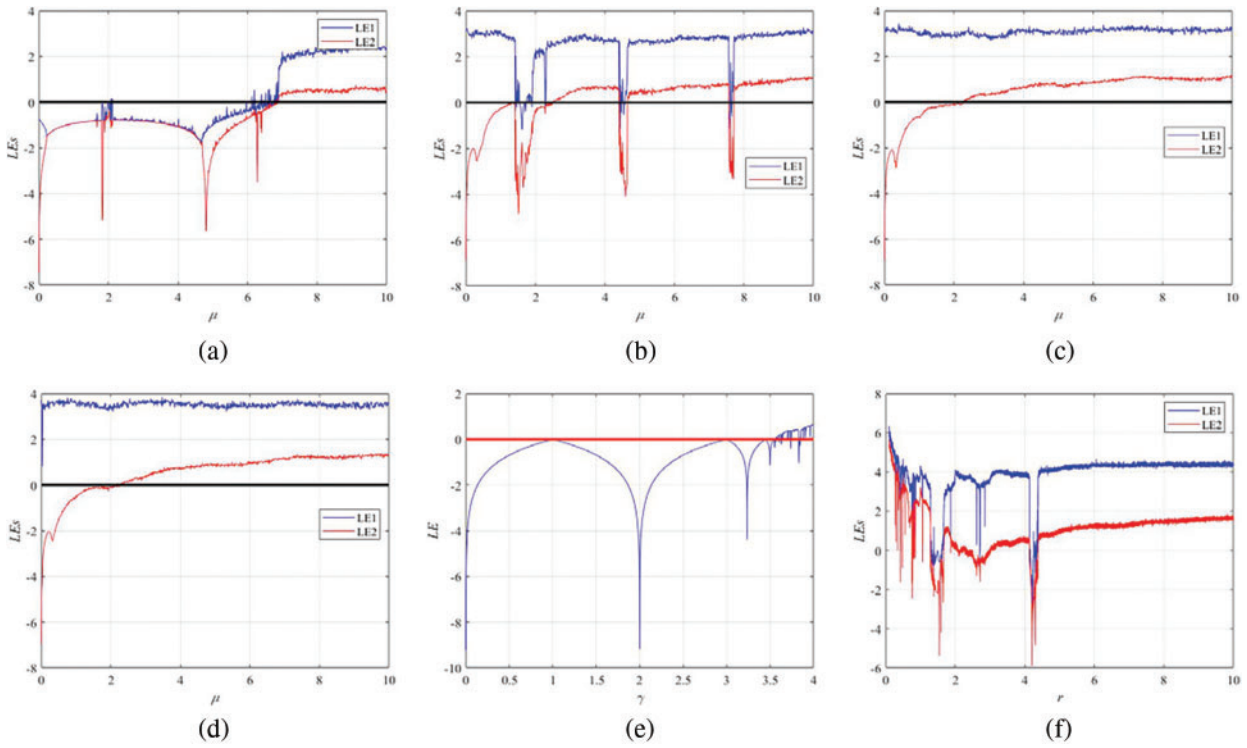

Figure 1: Lyapunov exponents (a) LEs of 2D-SSCDB with $\eta = 2$. (b) LEs of 2D-SSCDB with $\eta = 5$. (c) LEs of 2D-SSCDB with $\eta = 7.2$. (d) LEs of 2D-SSCDB with $\eta = 15$. (e) LEs of Logistic. (f) LEs of 2D-SCMCI

2.2 Phase Diagram Analysis

Phase diagram analysis describes the trajectory of a nonlinear dynamical system. The larger the area occupied by the phase diagram, the better the chaotic performance of the nonlinear dynamical system. The phase diagram analysis of the 2D-SSCDB is shown in Fig. 2. The initial value are $x_0 = 0.465651321$, and $y_0 = 0.32131654$. Phase diagram analysis shows that the 2D-SSCDB occupies a larger space compared to 2D-SCMCI [39] and 2D-SLMM [40]. Therefore, the 2D-SSCDB has better ergodicity and can take all the values of the phase space.

2.3 NIST Statistical Test Suite

The NIST statistical test suite was used to test the randomness of the sequences generated by the 2D-SSCDB.

NIST contains 15 tests, and when the *P*-value is greater than 0.01, the random sequence passes the test. The NIST test of the 2D-SSCDB is shown in Table 1, where $x_0 = 0.465651321$ and $y_0 = 0.32131654$. The parameters for the 2D-SSCDB are $\eta = 7.2, \mu = 7.2$ and $\eta = 15, \mu = 8.9$. NIST tests show that the sequences generated by the 2D-SSCDB have good randomness.

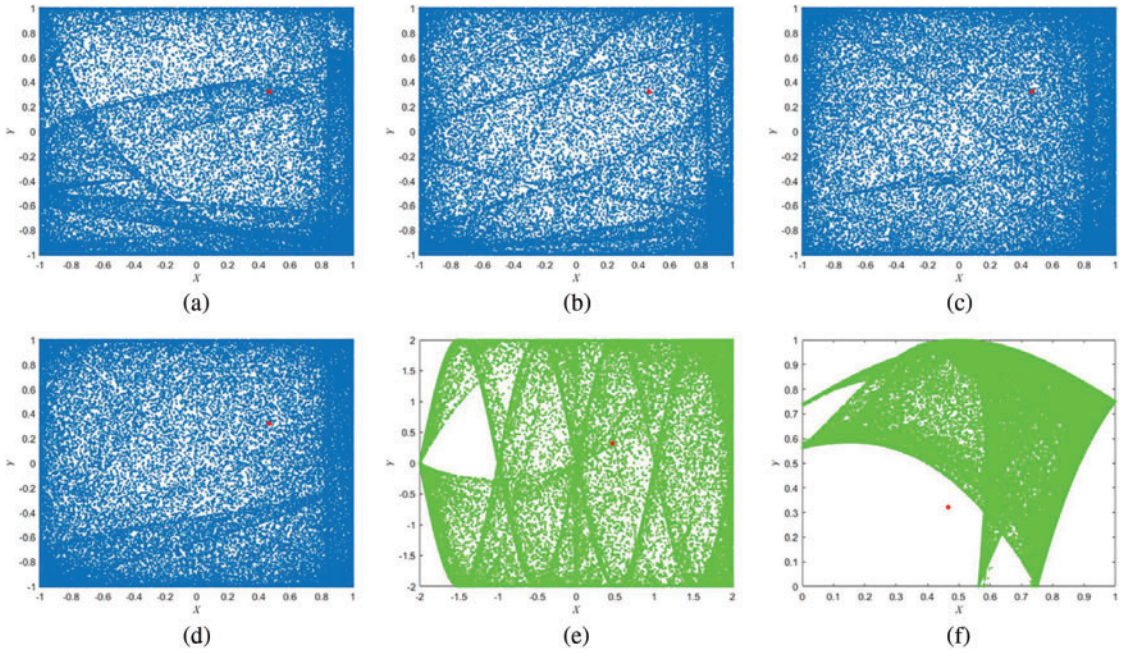

Figure 2: Phase diagram analysis. (a) $\eta = 2.8, \mu = 5$ of 2D-SSCDB. (b) $\eta = 5, \mu = 5.5$ of 2D-SSCDB. (c) $\eta = 7.2, \mu = 7.2$ of 2D-SSCDB. (d) $\eta = 15, \mu = 8.9$ of 2D-SSCDB. (e) 2D-SCMCI. (f) 2D-SLMM [40]

Table 1: NISTtest of 2D-SSCDB

Number	Statistical test	$\eta = 15, \mu = 8.9$				$\eta = 7.2, \mu = 7.2$			
		X		Y		X		Y	
		P-value	Result	P-value	Result	P-value	Result	P-value	Result
1	Longest run of ones	0.455937	Success	0.699313	Success	0.574903	Success	0.419021	Success
2	Overlapping template matching	0.171867	Success	0.911413	Success	0.213309	Success	0.983453	Success
3	Random excursions variant	0.253551	Success	0.148094	Success	0.122325	Success	0.949602	Success
4	Rank	0.991468	Success	0.616305	Success	0.616305	Success	0.383827	Success
5	Frequency	0.419021	Success	0.023545	Success	0.015598	Success	0.085587	Success
6	Universal	0.911413	Success	0.983453	Success	0.045675	Success	0.657933	Success
7	Random excursions	0.739918	Success	0.804337	Success	0.911413	Success	0.804337	Success
8	Block frequency	0.779188	Success	0.616305	Success	0.494392	Success	0.066882	Success
9	Cumulative sums	0.657933	Success	0.534146	Success	0.122325	Success	0.191687	Success
10	Runs	0.851383	Success	0.350485	Success	0.383827	Success	0.051942	Success
11	Serial	0.816537	Success	0.779188	Success	0.534146	Success	0.383827	Success
12	Spectral	0.191687	Success	0.911413	Success	0.816537	Success	0.383827	Success
13	Approximate entropy	0.699313	Success	0.494392	Success	0.534146	Success	0.739918	Success
14	Non-overlapping template matching	0.534146	Success	0.883171	Success	0.779188	Success	0.108791	Success
15	Linear complexity	0.108791	Success	0.153763	Success	0.350485	Success	0.616305	Success

3 Color Image Encryption Algorithm by 2D-SSCDB

In order to explore the application of the 2D-SSCDB to image encryption, we propose a color image encryption algorithm based on 2D-SSCDB, which we call simple structure-color image encryption (SS-CIE). The SS-CIE is a symmetric encryption algorithm, and the decryption process is the reverse process of encryption. The SS-CIE is an encryption algorithm that performs scrambling and diffusion at the same time. This design structure increases the security of the algorithm.

3.1 Encryption

The plaintext image is $P \in \mathcal{M}_{m\times n\times 3}$, the red channel of the plaintext is $PR \in \mathcal{M}_{m\times n}$, the green channel of the plaintext is $PG \in \mathcal{M}_{m\times n}$, and the blue channel of the plaintext is $PE \in \mathcal{M}_{m\times n}$. The algorithm of the SS-CIE is described as follows,

Input: P (PR, PG, PG)

Output: C ($C \in \mathcal{M}_{m\times n\times 3}$)

Step 1: Connect the three channels of the plaintext in turn to obtain a new plaintext $P \in \mathcal{M}_{m\times 3n}$, $P = [PR, PG, PB]$.

Step 2: Get an initial fine-tuning key k by P, where $k = \sum_{i=1}^{m}\sum_{j=1}^{3n} P(i,j)/10^{10} \times \pi$. If $k = 0$, then we set $k = 100$.

Step 3: Bring k into the Logistic iteration for 50 times to get the final fine-tuning key $k_1(k_1 = z_{50})$ by Eq. (3),

$$z_{n+1} = 3.99999 \times z_n \times (1 - z_n), n = 1, 2, 3, \ldots, 50, z_0 = k. \tag{3}$$

Step 4: Randomly give the initial key of the cryptosystem, x_0 ($x_0 \in (0,1)$), y_0 ($y_0 \in (0,1)$), μ ($\mu \in [3, +\infty)$) and η ($\eta \in [7.2, +\infty)$). Set the new keys which are $xn_0 = x_0 + k_1$, $yn_0 = y_0 + k_1$, $\mu n = \mu + k_1$, and $\eta n = \eta + k_1$.

Step 5: Let xn_0, yn_0, μn and ηn be the initial values and parameters of the 2D-SSCDB, iteratively generate chaotic sequences are X and Y, where $X \in \mathcal{M}_{1\times 3mn}$ and $Y \in \mathcal{M}_{1\times 3mn}$. It should be noted that the generated sequence needs to discard the initial sequence, so that the generated sequence is sufficiently chaotic, and the number of discarded sequences set in this paper is 300.

Step 6: Generate the encryption matrix of the cryptosystem D ($D \in \mathcal{M}_{m\times 3n}$), $D = \text{floor}(X \times 10^{10})\text{mod}256$.

Step 7: Set a sorting function $A = f(a, L)$, which can truncate the first L sequences from a one-dimensional vector a. Sort the intercepted sequence, and find the position of the sorted sequence in the original sequence, and return as A.

According to the sorting function, generate two sorting matrices S_1 and S_2, where $S_1 = f(Y, m)$ and $S_2 = f(Y(m + 3n : end), 3n)$.

Step 8: The encryption process is described as,

(1) $C(S_1(1), S_2(1)) = (P(1,1) + D(S_1(1), S_2(1)))\text{mod}256$.
(2) $C(S_1(i), S_2(1)) = (P(i,1) + D(S_1(i), S_2(1)) + C(S_1(i-1), S_2(1)))\text{mod}256, i = 1, 2, 3, \ldots, m$.
(3) $C(S_1(1), S_2(i)) = (P(1,i) + D(S_1(1), S_2(i)) + C(S_1(1), S_2(i-1)))\text{mod}256, i = 1, 2, 3, \ldots, 3n$.
(4) $C(S_1(i), S_2(j)) = (P(i,j) + D(S_1(i), S_2(j)) + C(S_1(i-1), S_2(j-1)))\text{mod}256, i = 1, 2, 3, \ldots, m$, $j = 1, 2, 3, , \ldots, 3n$.

3.2 Decryption

The decryption algorithm is the inverse process of the encryption algorithm. The decryption algorithm is described as follows.

Input: C ($C \in \mathcal{M}_{m\times n\times 3}$), x_0, y_0, μ, η, and k_1

Output: P ($P \in \mathcal{M}_{m\times n\times 3}$)

Step 1: Convert ciphertext C to new ciphertext $C \in \mathcal{M}_{m\times n\times 3} \rightarrow C \in \mathcal{M}_{m\times 3n}$.

Step 2: According to the secret keys x_0, y_0, μ, η, and k_1, the encryption matrix D of the cryptosystem can be generated, and two sorting matrices S_1 and S_2 are generated.

Step 3:The decryption process is described as follows,

(1) $P(1,1) = (C(S_1(1), S_2(1)) - D(S_1(1), S_2(1)))\text{mod}256$
(2) $P(i,1) = (C(S_1(i), S_2(1)) - D(S_1(i), S_2(1)) - C(S_1(i-1), S_2(1)))\text{mod}256, i = 1, 2, 3, \ldots, m$
(3) $P(1,i) = (C(S_1(1), S_2(i)) - D(S_1(1), S_2(i)) - C(S_1(1), S_2(i-1)))\text{mod}256, i = 1, 2, 3, \ldots, 3n$
(4) $P(i,j) = (C(S_1(i), S_2(j)) - D(S_1(i), S_2(j)) - C(S_1(i-1), S_2(j-1)))\text{mod}256, i = 1, 2, 3, \ldots, m,$
$j = 1, 2, 3, , \ldots, 3n$

4 Performance Analysis

4.1 Visualization

The encryption simulation experiment is carried out using the image encryption algorithm based on chaos theory proposed in this paper.

Taking Lena as an example, the image encryption and decryption results are shown in Fig. 3. Taking Black as an example, the image encryption and decryption results are shown in Fig. 4. The initial keys for SS-CIE are set to $x_0 = 0.465651321$, $y_0 = 0.32131654$, $\mu = 7.2$, and $\eta = 7.2$. Visual analysis shows that the SS-CIE is visually secure, and the ciphertext is transformed into an unrecognizable noise image.

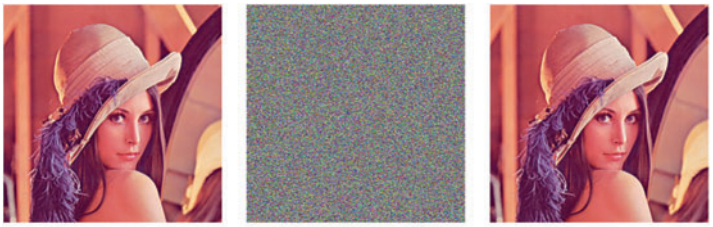

Figure 3: Visualization of SS-CIE for Lena (512×512). (a) Plaintext of lena. (b) Ciphertext of lena. (c) Decrypted lena

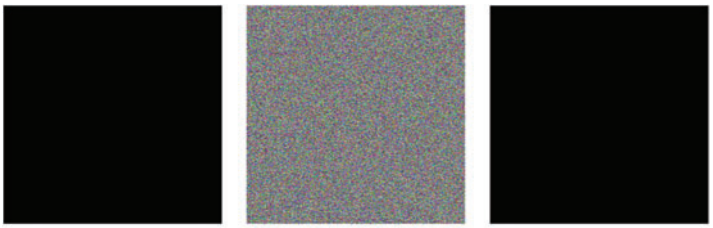

Figure 4: Visualization of SS-CIE for black (512 × 512). (a) Plaintext of black. (b) Ciphertext of black. (c) Decrypted black

4.2 Key Analysis

Key analysis is divided into key sensitivity analysis and key space analysis. The secret key of SS-CIE are x_0 ($x_0 \in (0, 1)$), y_0 ($y_0 \in (0, 1)$), μ ($\mu \in [3, +\infty)$), η ($\eta \in [7.2, +\infty)$), and k_1, if the calculation accuracy of the computer is 10^{-15}, the secret key space of x_0, y_0, μ, η, and k_1 are 10^{15}, 10^{15}, $10^{15} \times 10^{15}$, $10^{15} \times 10^{15}$, and 10^{15}. The secret key space of SS-CIE is

$$\text{keyspace} = 10^{15} \times 10^{15} \times (10^{15} \times 10^{15}) \times (10^{15} \times 10^{15}) \times 10^{15} = 10^{105} \approx 2^{348}.$$

When the key space of the algorithm exceeds 2^{100}, the algorithm is considered to be resistant to brute force attacks. So the SS-CIE can resist brute force attacks.

In order to test the key sensitivity of the image encryption algorithm in this paper, the key is changed 10^{-15}, and the simulation results are shown in Fig. 5. The initial keys for SS-CIE are set to $x_0 = 0.465651321$, $y_0 = 0.32131654$, $\mu = 7.2$, and $\eta = 7.2$. Key sensitivity analysis shows that the SS-CIE is sensitive to keys, and the decryption system also has good sensitivity.

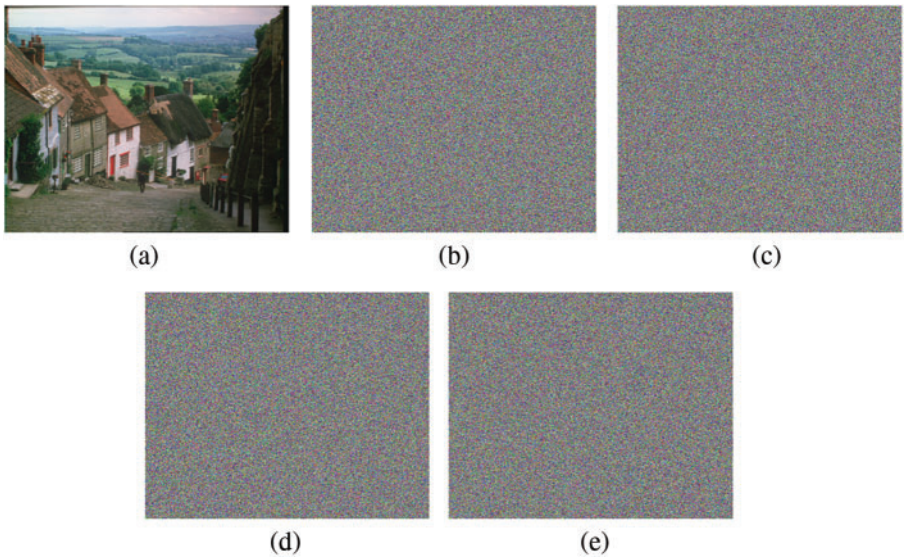

Figure 5: Key sensitivity analysis of SS-CIE for Goldhill (576 × 702). (a) Correct key to decrypt. (b) Wrong key to decrypt with $x_0 = x_0 + 10^{-15}$. (c) Wrong key to decrypt with $y_0 = y_0 + 10^{-15}$. (d) Wrong key to decrypt with $\eta = \eta + 10^{-15}$. (e) Wrong key to decrypt with $\mu = \mu + 10^{-15}$

4.3 Histogram Analysis

The histogram can be used to visually see the distribution characteristics of the pixel value of an image. Taking Goldhill as an example, the histogram analysis of SS-CIE is shown in Fig. 6.

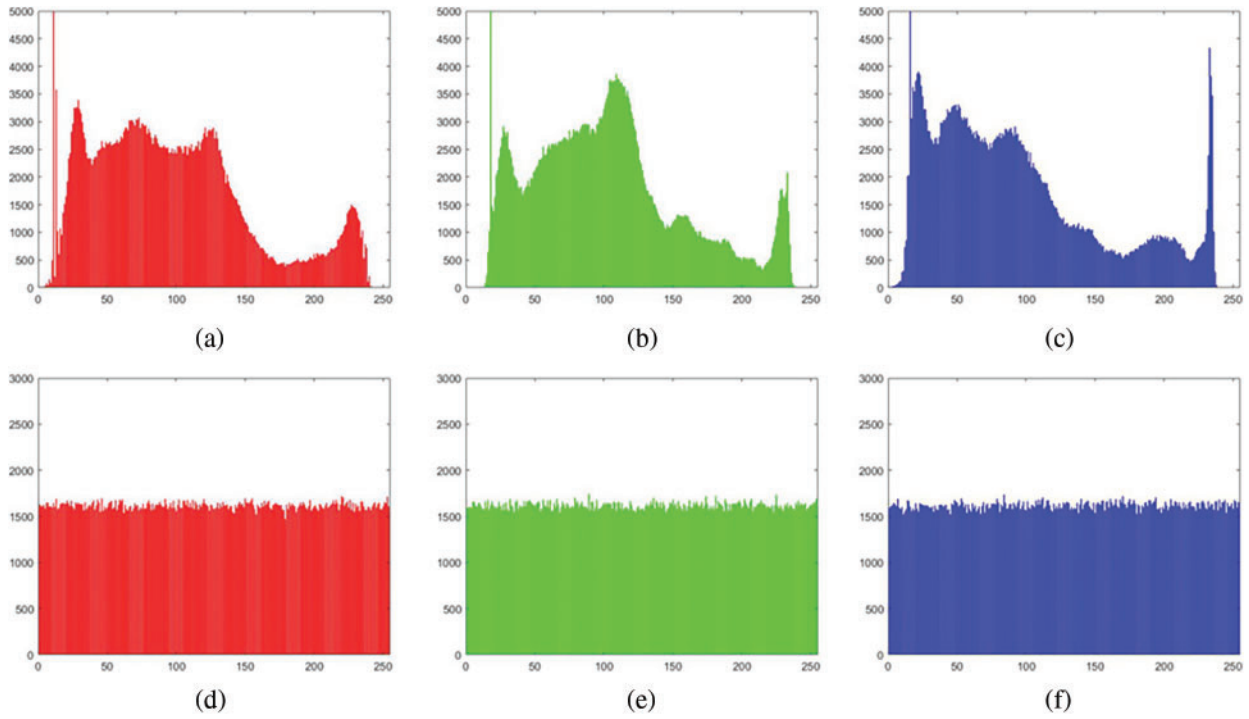

Figure 6: Histogram analysis of SS-CIE. (a) Histogram of R channel. (b) Histogram of G channel. (c) Histogram of B channel. (d) Histogram of encrypted R channel. (e) Histogram of encrypted G channel. (f) Histogram of encrypted B channel

Histogram analysis shows that the ciphertext histogram distribution of SS-CIE is uniform, which means that the ciphertext pixel value distribution is random, and the attacker cannot obtain any useful information from the ciphertext, so SS-CIE can Resist statistical attacks.

4.4 Correlation Analysis

Generally, the correlation between adjacent pixels of the raw unprocessed image is high. We hope that the correlation performance between adjacent pixels of the image will be reduced after encryption, so that the ciphertext image cannot be cracked through the correlation analysis of adjacent pixels. Taking Goldhill as an example, the correlation analysis of the SS-CIE is shown in Figs. 7 and 8.

When the adjacent correlation is small, the correlation image shows a divergent state. When the adjacent correlation is large, the image presents an aggregated state. Therefore, visually, the ciphertext of SS-CIE has less correlation. To further verify the accuracy of the correlation, the calculation formula of the correlation is

$$r_\rho = \frac{\operatorname{cov}(x, y)}{\sqrt{D(x) \cdot D(y)}}. \tag{4}$$

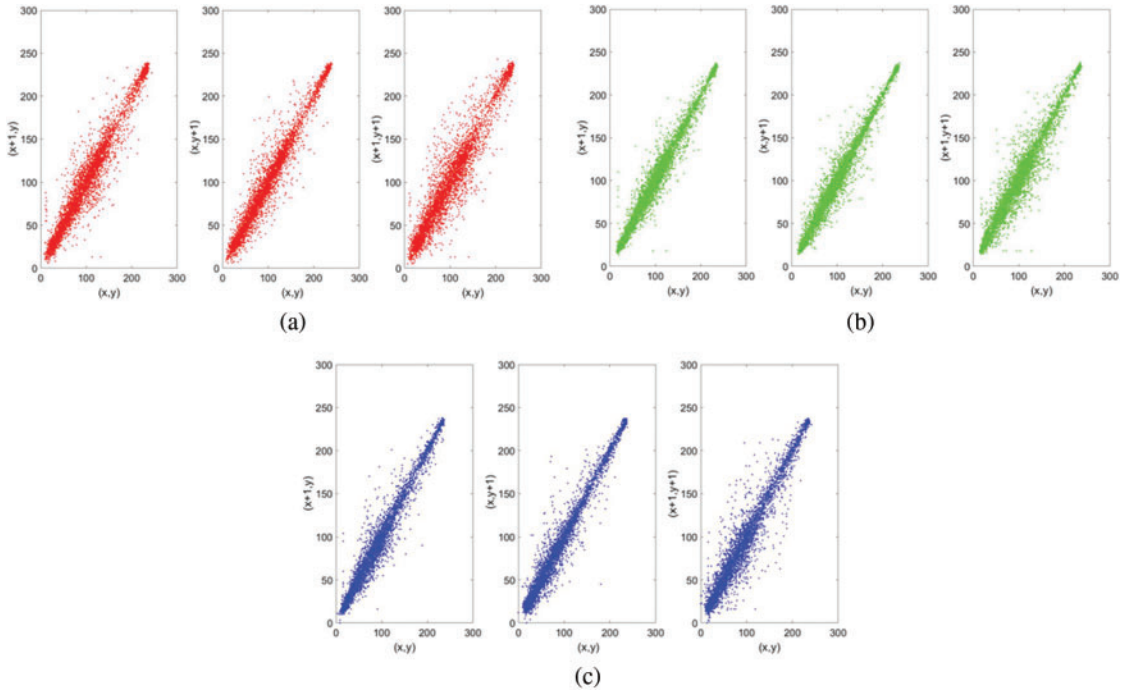

Figure 7: Correlation analysis of plaintext for SS-CIE. (a) Correlation of R channel. (b) Correlation of G channel. (c) Correlation of B channel

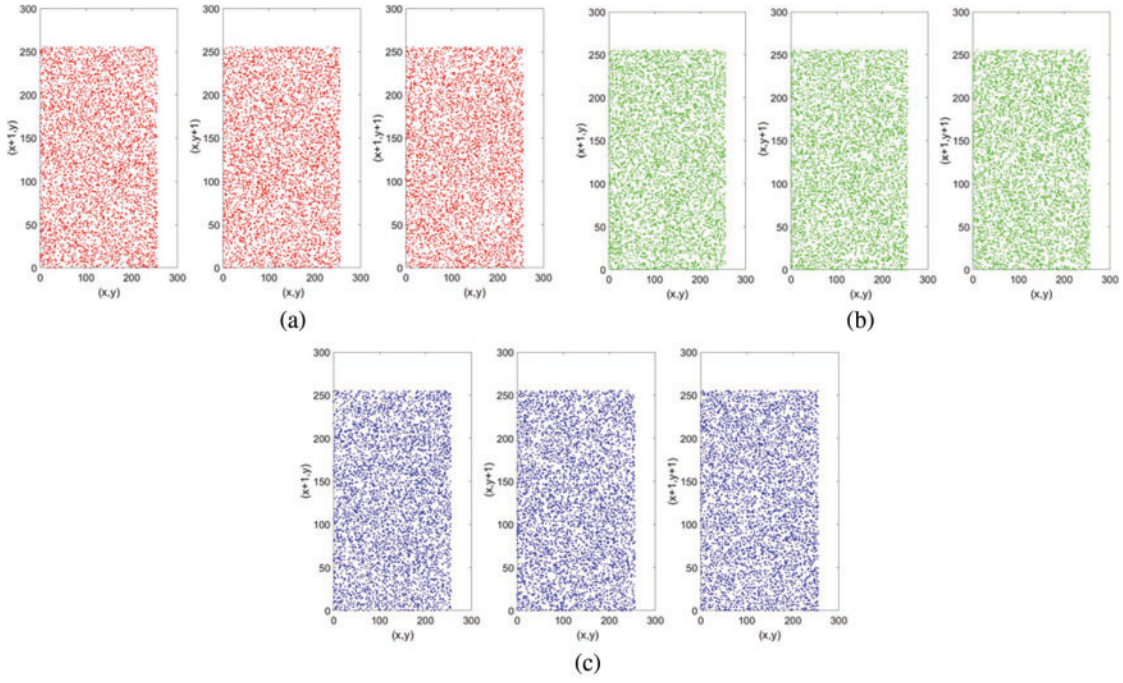

Figure 8: Correlation analysis of ciphertext for SS-CIE. (a) Correlation of encrypted R channel. (b) Correlation of encrypted G channel. (c) Correlation of encrypted B channel

Table 2 is the correlation analysis results of SS-CIE. And compared with some classic algorithms (Refs. [43–45]), the comparison results are shown in Table 3.

Table 2: Correlation coefficients of SS-CIE

Image		Plaintext			Ciphertext		
		H	V	D	H	V	D
Lena	R	0.9798	0.9893	0.9697	−0.0012	−0.0004	−0.0002
	G	0.9689	0.9824	0.9554	0.0012	−0.0014	0.0005
	B	0.9325	0.9574	0.9181	−0.0023	−0.0023	−0.0002
Goldhil	R	0.9783	0.9722	0.9583	0.0005	−0.0006	0.0016
	G	0.9815	0.9831	0.9699	−0.0006	0.0012	0.0013
	B	0.9837	0.9840	0.9723	−0.0014	−0.0010	0.0005
White	R	1	1	1	−0.0022	−0.0013	0.0020
	G	1	1	1	0.0012	−0.0001	0.0015
	B	1	1	1	−0.0029	0.0011	−0.0014
Black	R	1	1	1	0.0023	−0.0012	0.0002
	G	1	1	1	0.0006	0.00006	−0.0016
	B	1	1	1	−0.0003	0.0003	0.0046
Average		0.9854	0.9890	0.9786	−0.0004	−0.0004	0.0007

Table 3: Correlation coefficients comparison

Algorithms	SS-CIE	Algorithm in [43]	Algorithm in [44]	Algorithm in [45]
Horizontal	**−0.0004**	−0.0082	−0.0013	0.0057
Vertical	**−0.0004**	−0.0128	0.0004	0.0061
Diagonal	**0.0007**	−0.0012	0.0078	−0.0031

The correlation coefficient of the plaintext image is large, and the correlation is very strong. However, the correlation coefficient of adjacent pixels of the ciphertext image is very small, and the correlation is low. It shows that after the encryption of the algorithm in this paper, the ciphertext image can well resist the attack of statistical analysis. In addition, the correlation comparison with other algorithms shows that the SS-CIE is more resistant to statistical analysis.

4.5 Correlation Analysis of R, G, and B

Using the method of correlation analysis to analyze the correlation between the three channels, a safe algorithm can not only reduce the correlation between adjacent pixels, but also reduce the correlation between the three channels of the plaintext image. The correlation analysis of the three channels is shown in Table 4.

Table 4: Correlation between R, G, and B components of color image

Ours	Image	(R, G)	(R, B)	(G, B)
Plaintext	Lena	0.8785	0.6763	0.9105
	Goldhil	0.9390	0.9000	0.9736
	White	1	1	1
	Black	1	1	1
Ciphertext	Lena	−0.0020	0.0021	0.0017
	Goldhil	−0.0018	−0.0001	0.0026
	White	−0.0012	−0.0023	−0.00041
	Black	−0.0032	−0.0037	0.0004

The experimental results show that the SS-CIE effectively reduces the correlation between the three channels, and the attacker cannot infer the information of the remaining channels through the ciphertext value of one channel, indicating that the algorithm has good security.

4.6 Information Entropy Analysis

The amount of information contained in an image can be reflected by information entropy. The greater the information entropy, the better the encryption effect of the algorithm and the more hidden information. The calculation formula of information entropy is,

$$H = \sum_{i=0}^{255} p\left(g_i\right) \log_2 \frac{1}{p(g_i)}. \tag{5}$$

The information entropy analysis of SS-CIE is shown in Table 5, and the information entropy comparison results with other algorithms are shown in Table 6 (Refs. [43–45]).

Table 5: Information entropy of SS-CIE

Image		Plaintext	Ciphertext
Lena	R	7.2531	7.9993
	G	7.5952	7.9993
	B	6.9686	7.9993
Goldhil	R	7.6101	7.9996
	G	7.5544	7.9996
	B	7.5540	7.9996
White	R	0	7.9992
	G	0	7.9992
	B	0	7.9993

(Continued)

Table 5: Continued

Image		Plaintext	Ciphertext
Black	R	0	7.9992
	G	0	7.9992
	B	0	7.9992
Average		3.71128	7.9993

Table 6: Information entropy comparison

Algorithms	SS-CIE	Algorithm in [43]	Algorithm in [44]	Algorithm in [45]
Information entropy	**7.9993**	7.9895	7.9973	7.9979

The information entropy analysis shows that the plaintext image carries a lot of information, while the ciphertext image obtained by the SS-CIE has a small amount of information (the information entropy is close to 8). The ciphertext image presents a random noise image. The information entropy comparison results show that the ciphertexts of SS-CIE have better randomness and less information, so the SS-CIE is more resistant to statistical attacks, and the algorithm has better security.

4.7 Differential Attack Analysis

A secure algorithm is sensitive to the plaintext. Even if the plaintext changes slightly, two distinct ciphertexts will still be obtained. NPCR and UACI are two indicators to evaluate the ability of the algorithm to resist differential attack. Wu et al. proposed in the Ref. [46] that when the value of NPCR exceeds 99.5893%, the value of UACI is between 33.3730% and 33.5541%, indicating that the algorithm can resist differential attacks. The ability of SS-CIE to resist differential attacks is shown in Table 7. Differential attack analysis shows that SS-CIE has excellent resistance to differential attacks, and the attacker cannot crack the algorithm by analyzing the characteristics of the two ciphertexts.

Table 7: Differential attack analysis

Image		NPCR (%)	PASS/NO PAASS	UACI (%)	PASS/NO PAASS
Lena	R	99.6040	PASS	33.4707	PASS
	G	99.6101	PASS	33.4394	PASS
	B	99.6063	PASS	33.4214	PASS
Goldhil	R	99.6281	PASS	33.3890	PASS
	G	99.6250	PASS	33.4765	PASS
	B	99.6021	PASS	33.4699	PASS
White	R	99.6219	PASS	33.4023	PASS
	G	99.6109	PASS	33.4161	PASS
	B	99.6253	PASS	33.3908	PASS

(Continued)

Table 7: Continued

Image		NPCR (%)	PASS/NO PAASS	UACI (%)	PASS/NO PAASS
Black	R	99.6231	PASS	33.4272	PASS
	G	99.6067	PASS	33.3784	PASS
	B	99.6116	PASS	33.4496	PASS

4.8 Robustness Analysis

There will be noise attacks and clipping attacks in the transmission of ciphertext. The effect of SS-CIE against clipping attack is shown in Fig. 9. The effect of SS-CIE against noise attack is shown in Fig. 10. Noise attack and clipping attack show that SS-CIE has good robustness.

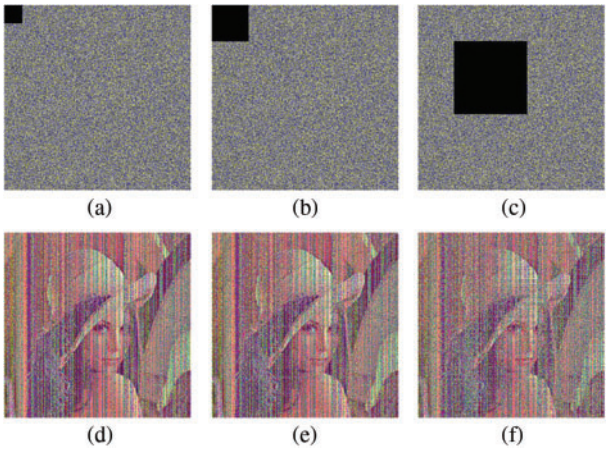

Figure 9: Clipping attacks analysis. (a) Correlation of encrypted R channel. (b) Data lost of $50 * 50$. (c) Data lost of $100 * 100$. (c) Data lost of $200 * 200$. (d) Decrypted image of (a). (e) Decrypted image of (b). (c) Decrypted image of (c)

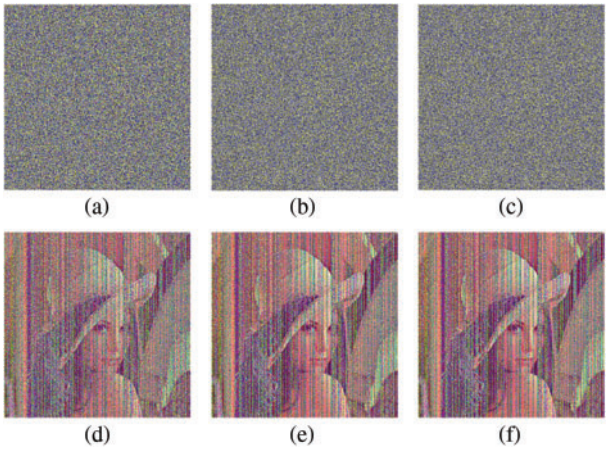

Figure 10: Noise attacks analysis. (a) 0.1 salt & pepper. (b) 0.01 salt & pepper. (c) 0.001 salt & pepper. (d) Decrypted image of (a). (e) Decrypted image of (b). (c) Decrypted image of (c)

4.9 Efficiency Analysis

The running environment of the SS-CIE is Windows 10, matlab 2020, i3-10105F. The efficiency analysis is shown in Table 8. Efficiency analysis shows that SS-CIE requires about 1.0930 s to encrypt color images with $512 * 512$. Compared with other algorithms, SS-CIE has higher efficiency. SS-CIE not only has high security, but also runs efficiently.

Table 8: Efficiency analysis

Algorithms	SS-CIE	Algorithm in [47]	Algorithm in [48]	Algorithm in [49]
Time/s	1.0930	19.1400	8.0130	4.2120

5 Conclusion

In this paper, a new 2D hyperchaotic system is proposed, called 2D-SSCDB. The 2D-SSCDB has a simple structure and can generate complex dynamic behavior. Through Lyapunov exponent, phase diagram analysis, NIST test, sensitivity analysis, and comparative analysis, it is verified that the 2D-SSCDB has good performance and can generate random numbers with better performance. In order to verify the practicability of the 2D-SSCDB, combined with the 2D-SSCDB system, we propose a color image encryption algorithm. Scrambling and diffusion are carried out at the same time in this algorithm. Through key analysis, information entropy analysis, statistical analysis, and other methods, it is verified that the cryptographic system has high security and can resist common attack methods. The 2D-SSCDB is a better candidate for keystream generation based on chaotic image encryption.

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

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

References

[1] X. Huang, Y. Dong, H. Zhu and G. Ye, "Visually asymmetric image encryption algorithm based on SHA-3 and compressive sensing by embedding encrypted image," *Alexandria Engineering Journal*, vol. 61, no. 10, pp. 7637–7647, 2022.

[2] F. Yang, J. Mou, C. Ma and Y. Cao, "Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application," *Optics and Lasers in Engineering*, vol. 129, pp. 106031, 2020.

[3] 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.

[4] X. Wang, S. Gao, X. Ye, S. Zhou and M. Wang, "A new image encryption algorithm with cantor diagonal scrambling based on the PUMCML system," *International Journal of Bifurcation and Chaos*, vol. 31, no. 1, pp. 2150003, 2021.

[5] R. Anitha and B. Vijayalakshmi, "Image encryption using multi-scroll attractor and chaotic logistic map," *Computers, Materials and Continua*, vol. 72, no. 2, pp. 3447–3463, 2022.

[6] X. Wang and S. Gao, "A chaotic image encryption algorithm based on a counting system and the semi-tensor product," *Multimedia Tools and Applications*, vol. 80, no. 7, pp. 10301–10322, 2021.

[7] X. Li, J. Mou, L. Xiong, Z. Wang and J. Xu, "Fractional-order double-ring erbium-doped fiber laser chaotic system and its application on image encryption," *Optics and Laser Technology*, vol. 140, pp. 107074, 2021.

[8] 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.
[9] X. Wang and P. Liu, "A new full chaos coupled mapping lattice and its application in privacy image encryption," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 69, no. 3, pp. 1291–1301, 2021.
[10] 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.
[11] 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.
[12] 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.
[13] 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.
[14] 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.
[15] S. Zhou, X. Wang, M. Wang, B. Ge, M. Wang *et al.,* "A novel image encryption cryptosystem based on true random numbers and chaotic systems," *Multimedia Systems*, vol. 28, no. 1, pp. 98–112, 2022.
[16] L. Gong, K. Qiu, C. Deng and N. Zhou, "An image compression and encryption algorithm based on chaotic system and compressive sensing," *Optics and Laser Technology*, vol. 115, pp. 257–267, 2019.
[17] F. H. Hsiao, "Applying 3DES to chaotic synchronization cryptosystems," *IEEE Access*, vol. 10, pp. 1036–1050, 2021.
[18] N. Zhou, S. Pan, S. Cheng and Z. Zhou, "Image compression encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Optics and Laser Technology*, vol. 82, pp. 121–133, 2016.
[19] L. Xu, Z. Li, J. Li and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Optics and Lasers in Engineering*, vol. 78, pp. 17–25, 2016.
[20] X. Chai, X. Fu, Z. Gan, Y. Lu and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Processing*, vol. 155, pp. 44–62, 2019.
[21] J. Wu, X. Liao and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Processing*, vol. 141, pp. 109–124, 2017.
[22] L. Wang, T. Dong and M. F. Ge, "Finite-time synchronization of memristor chaotic systems and its application in image encryption," *Applied Mathematics and Computation*, vol. 347, pp. 293–305, 2019.
[23] B. Liu, X. Ye and Q. Chen, "Generating infinitely many coexisting attractors via a new 3D cosine system and its application in image encryption," *IEEE Access*, vol. 9, pp. 136292–136301, 2021.
[24] W. Liu, K. Sun and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Optics and Lasers in Engineering*, vol. 84, pp. 26–36, 2016.
[25] C. Cao, K. Sun and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Processing*, vol. 143, pp. 122–133, 2018.
[26] 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.
[27] M. Alawida, A. Samsudin, J. S. Teh and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Processing*, vol. 160, pp. 45–58, 2019.
[28] X. Chai, Z. Gan, K. Yuan, Y. Chen and X. Liu, "A novel image encryption scheme based on DNA sequence operations and chaotic systems," *Neural Computing and Applications*, vol. 31, no. 1, pp. 219–237, 2019.
[29] Y. Zhou, L. Bao and C. Chen, "A new 1D chaotic system for image encryption," *Signal Processing*, vol. 97, pp. 172–182, 2014.
[30] C. Li, G. Luo, K. Qin and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[31] Y. Xiao, X. Tong, M. Zhang and Z. Wang, "Image lossless encoding and encryption method of SPECK based on 1D chaotic map," *Physica Scripta*, vol. 97, no. 5, pp. 05521, 2022.
[32] C. Zhu, G. Wang and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps," *Entropy*, vol. 20, no. 11, pp. 843, 2018.
[33] J. Chen, F. Han, W. Qian, Y. Yao and Z. Zhu, "Cryptanalysis and improvement in an image encryption scheme using combination of the 1D chaotic map," *Nonlinear Dynamics*, vol. 93, no. 4, pp. 2399–2413, 2018.
[34] S. Dhall, S. K. Pal and K. Sharma, "Cryptanalysis of image encryption scheme based on a new 1D chaotic system," *Signal Processing*, vol. 146, pp. 22–32, 2018.
[35] M. Khan and A. Rasheed, "A fast quantum image encryption algorithm based on affine transform and fractional-order Lorenz-like chaotic dynamical system," *Quantum Information Processing*, vol. 21, no. 4, pp. 134, 2022.
[36] H. Liu, J. Liu and C. Ma, "Constructing dynamic strong S-box using 3D chaotic map and application to image encryption," *Multimedia Tools and Applications*, 2022. https://doi.org/10.1007/s11042-022-12069-x.
[37] 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.
[38] X. Wang and J. Yang, "Spatiotemporal chaos in multiple coupled mapping lattices with multi-dynamic coupling coefficient and its application in color image encryption," *Chaos, Solitons and Fractals*, vol. 147, pp. 110970, 2021.
[39] J. Sun, "2D-SCMCI hyperchaotic map for image encryption algorithm," *IEEE Access*, vol. 9, pp. 59313–59327, 2021.
[40] Z. Hua, Y. Zhou, C. M. Pun and C. L. Chen, "2D sine logistic modulation map for image encryption," *Information Sciences*, vol. 297, pp. 80–94, 2015.
[41] J. Zheng and L. F. Liu, "Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map," *IET Image Processing*, vol. 14, no. 11, pp. 2310–2320, 2020.
[42] L. Teng, X. Wang and Y. Xian, "Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion," *Information Sciences*, vol. 605, pp. 71–85, 2022.
[43] X. Wu, K. Wang, X. Wang, H. Kan and J. Kurths, "Color image DNA encryption using NCA map-based CML and one-time keys," *Signal Processing*, vol. 148, pp. 272–287, 2018.
[44] X. Wang, H. Zhang and X. Bao, "Color image encryption scheme using CML and DNA sequence operations," *Biosystems*, vol. 144, pp. 18–26, 2016.
[45] X. J. Kang and Z. H. Guo, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 80, pp. 115670, 2020.
[46] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Journal of Selected Areas in Telecommunications*, vol. 1, no. 2, pp. 31–38, 2011.
[47] X. Wang, Y. Su, C. Luo, F. Z. Nian and L. Teng, "Color image encryption algorithm based on hyperchaotic system and improved quantum revolving gate," *Multimedia Tools and Applications*, vol. 81, no. 10, pp. 13845–13865, 2022.
[48] Y. Wang, C. Quan and C. J. Tay, "Optical color image encryption without information disclosure using phase-truncated Fresnel transform and a random amplitude mask," *Optics Communications*, vol. 344, pp. 147–155, 2015.
[49] Y. Luo, R. Zhou, J. Liu, S. H. Qiu and Y. Cao, "An efficient and self-adapting colour-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools and Applications*, vol. 77, no. 20, pp. 26191–26217, 2018.