Signal, Image and Video Processing (2024) 18:3063–3077
https://doi.org/10.1007/s11760-023-02971-8

ORIGINAL PAPER

CLSM-IEA: a novel cosine-logistic-sine map and its application in a new image encryption scheme

Xiaosong Gao[1] · **Xingbin Liu**[1]

Received: 22 November 2023 / Revised: 12 December 2023 / Accepted: 14 December 2023 / Published online: 5 February 2024

Abstract
Chaotic systems have initial value sensitivity, unpredictability, and random-like properties, which are widely employed in image encryption schemes. However, many existing encryption schemes are deficient in security due to the shortcomings of the adopted chaotic maps and designed encryption algorithms, such as the discontinuous chaotic ranges, unevenly distributed trajectories, and the fixed orders to process the pixels. To solve these problems, we propose a new two-dimensional cosine-logistic-sine map (2D-CLSM), which is shown to have an extensive chaotic range and complex chaotic behaviors in terms of trajectory, bifurcation diagram, Lyapunov exponent, sample entropy, permutation entropy and TestU01. Furthermore, a new 2D-CSLM-based image encryption algorithm (CLSM-IEA) is designed, which includes the chaotic efficient permutation and random multi-directional diffusion operations. The chaotic efficient permutation is designed to quickly separate adjacent pixels into different positions randomly according to chaotic sequences generated from the 2D-CLSM. The random multi-directional diffusion secretly processes the pixels in diverse directions, the processes of which are determined by the chaotic matrix. The simulation analysis reveals that the proposed encryption algorithm has a higher security level than some state-of-the-art algorithms.

Keywords Chaotic system · Hyperchaotic map · Image encryption · Image security analysis

1 Introduction

In recent years, with the rapid popularization and development of information science and technology, a large amount of information transmission has become more and more common in the network. People are concerned about the transmission and preservation of some specific images, which may contain national security and personal privacy, once leaked, it will make the nation or personal interests suffer great losses. Existing techniques for image protection include image watermarking [1, 2], data hiding [3], and image encryption [4–8]. Among them, image encryption is the most straightforward and effective, which encrypts an image into another completely random and meaningless image.

The methods of image encryption include wavelet transform [9], DNA coding [10], quantum image encryption [11, 12], and encryption based on chaos theory [13–17]. In these techniques, the chaos theory plays an important role in image encryption due to its unpredictability, randomness, and sensitivity to initial values [18]. A chaotic map with favorable chaotic properties generally results in a secure encryption scheme and achieves excellent results. For example, based on a logistic tent modular map, Hua et al. [19] proposed an image encryption algorithm that employs cross-plane permutation and non-sequential diffusion to encrypt images, where non-sequential diffusion changes the pixel values according to a secret sequence. Simulation tests show that the encryption scheme has high security. Erkan et al. [20] proposed a new 2D chaotic map by utilizing the diversity of Euler and Pi numbers and used bit reversion operation to change the pixel values to achieve better results. In [21], the author developed a cosine-transform-based chaotic system and based on the proposed chaotic system designed a cryptographic scheme that includes high-efficiency scrambling to randomly distribute pixels and random order substitution to change pixel values in a secret order. Teng et al. [22] proposed a new two-dimensional cross-mode hyperchaotic map based on logistic and sine maps, which has good unpredictability and a wide chaotic range. The author further designed an encryption

✉ Xingbin Liu
xbliu6@163.com

[1] College of Electronic and Information Engineering, Southwest University, Chongqing 400715, China

scheme to encrypt the pixel positions and values simultaneously, which is effective against various attacks; Mansouri et al. [23] developed a one-dimensional sine-powered chaotic system that is highly sensitive and unpredictable. In addition, row-by-row and column-by-column confusion operations are used to change the pixel position, and the bit-level pixel operations are used to change the pixel value. Simulations show that the proposed encryption scheme has good performance. A 2D-LSM is proposed and a CIEA based on the 2D-LSM is designed in [24], which employs the point-to-point permutation and plane-cross-plane diffusion to encrypt the pixels, and it achieves better performance compared with some existing algorithms.

However, some chaotic maps proposed in recent years suffer from shortcomings. Some chaotic maps have discontinuous or limited parameter ranges, and when they are affected by external conditions, their chaotic behaviors would be degraded or even disappear [25, 26]. Some trajectories of the chaotic maps are not uniformly distributed throughout the entire phase space and exhibit specific patterns, which suggests that it is easy for an attacker to predict [27, 28]. When some chaotic maps are applied to platforms with limited accuracy, their chaotic properties may be weakened [29]. In addition, many encryption schemes have deficiencies in security. Some of them process pixels in a specified order, which may lead to a decrease in the security of the algorithms [30, 31]. To overcome the above deficiencies of chaotic maps and improve the security of encryption schemes, we propose the 2D-CLSM. Compared with the existing chaotic maps, the 2D-CLSM has an ultra-wide chaotic range and superior chaotic behaviors in the trajectory, bifurcation diagram, Lyapunov exponent, sample entropy, permutation entropy **and TestU01** tests. Meanwhile, a 2D-CLSM-based image encryption algorithm (CLSM-IEA) is proposed, which consists of chaotic efficient permutation and random multi-directional diffusion. The chaotic efficient permutation is different from confusing the pixel positions row by row or column by column, and it changes the positions of pixels according to a secret order, which could greatly increase the randomness of the confusion process and reduce the correlations of the adjacent pixels. The random multi-directional diffusion chooses the diffusion direction based on the chaotic matrix to change the pixel values in multiple directions, which improves the security of the diffusion process. Under the condition of generating only two chaotic sequences, a plain image can be encrypted into another unrecognizable cipher image. The proposed CLSM-IEA shows high security in terms of key sensitivity, information entropy, adjacent pixel correlation, and the ability to resist differential attacks, noise attacks, and cropping attacks.

The innovations and contributions of this paper are summarized as follows:

(1) A new two-dimensional chaotic map 2D-CLSM is proposed. Compared with the chaotic maps proposed in recent years, the 2D-CLSM has better ergodicity and unpredictability, and it behaves more complex chaotic behaviors across a large range of control parameters.
(2) An image encryption scheme including the chaotic efficient permutation and random multi-directional diffusion is proposed. The chaotic efficient permutation can quickly separate adjacent pixels from horizontal and vertical directions at the same time through the random order. The random multi-directional diffusion chooses the diffusion direction determined by the chaotic matrix to spread changes in multiple directions.
(3) Through various simulation experiments and security analysis, the CLSM-IEA provides strong security against diverse security attacks and surpasses some state-of-the-art image encryption algorithms in terms of security.

2 The 2D-CLSM hyperchaotic map

In this paper, the proposed 2D-CLSM firstly combines logistic and improved sine maps, exploiting the diversity of floating-point number π at the same time. Then, the combination result is used to perform the cosine transform. In this way, it can make its output sequence more unpredictable and acquires more complex chaotic behaviors over a wide range of control parameters. The mathematical definition of 2D-CLSM is as follows:

$$\begin{aligned} x_{i+1} &= cos\left(4ux_i(1-x_i)\sin(\pi(y_i(1-y_i)))\pi^{10}+\pi^2\right) \\ y_{i+1} &= cos\left(4uy_i(1-y_i)\sin(\pi(x_i+y_i))\pi^{10}+\pi^2\right) \end{aligned} \tag{1}$$

where u is the control parameter and π takes 20 decimal places 3.14159265358979323846. The proposed chaotic map is used to generate sequences with high randomness and initial value sensitivity.

3 Performance evaluation of 2D-CLSM

The chaos properties of chaotic maps occupy a key position in the security evaluation of image encryption algorithms. Chaotic maps with superior chaotic properties often imply secure and reliable encryption schemes. Therefore, we evaluate the 2D-CLSM in various aspects, such as the trajectory, bifurcation diagram, Lyapunov exponent, sample entropy, permutation entropy **and TestU01**. Compared with the chaotic maps proposed in recent years, such as the 2D sine logistic modulation map(2D-SLMM) [32] and 2D infinite

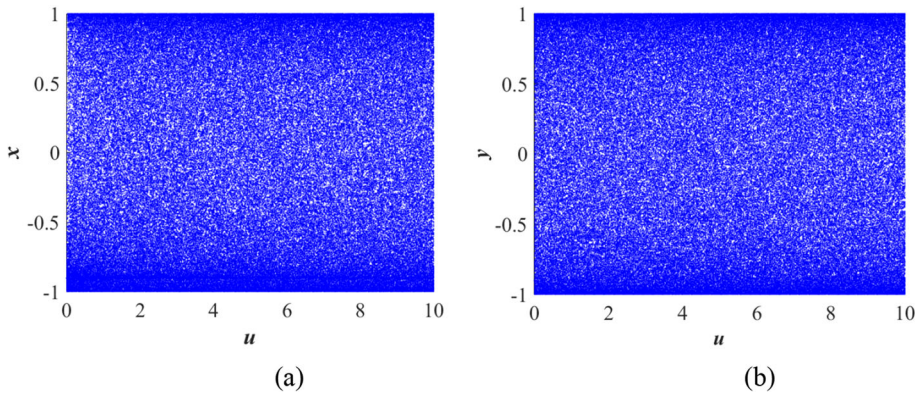

Fig. 1 Bifurcation diagrams of the 2D-CLSM (**a**) for variable x. (**b**) for variable y

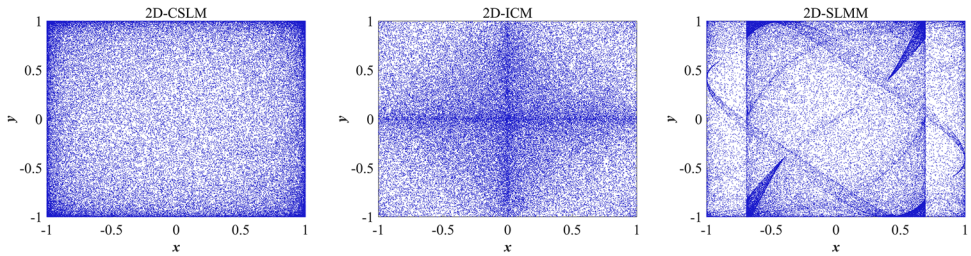

Fig. 2 Trajectories of the different chaotic maps: (**a**) 2D-CLSM. (**b**) 2D-ICM. (**c**)2D-SLMM

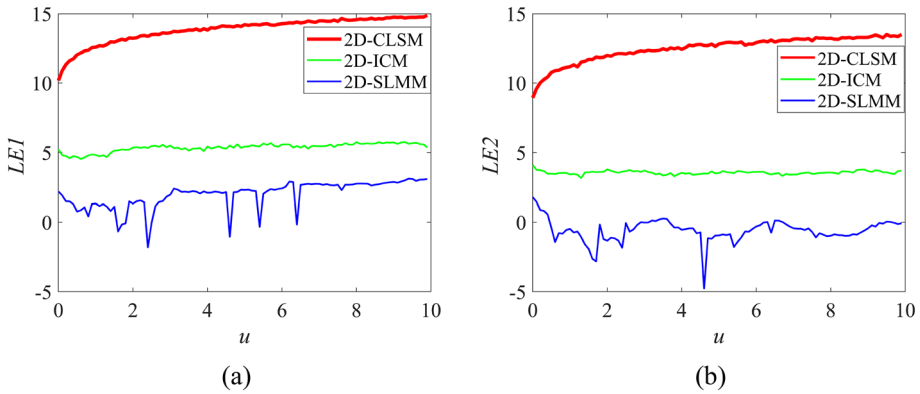

Fig. 3 The comparative LE spectrums for (**a**) LE1. (**b**) LE2

Table 1 TestU01 results of different chaotic maps

Gain		10^{14}	10^{15}	10^{16}
2D-SLMM (x, y)	Small Crush	(1, 1)	(1, 1)	(1, 1)
	Crush	(27, 25)	(27, 26)	(27, 25)
2D-ICM (x, y)	Small Crush	(0, 0)	(0, 0)	(0, 0)
	Crush	(0, 0)	(0, 0)	(0, 0)
	Big Crush	(2, 3)	(2, 2)	(2, 2)
2D-CLSM (x, y)	Small Crush	(0, 0)	(0, 0)	(0, 0)
	Crush	(0, 0)	(0, 0)	(0, 0)
	Big Crush	(1, 0)	(0, 0)	(1, 0)

collapse map (2D-ICM) [33], the 2D-CLSM has superior hyperchaotic properties, a larger and continuous parameter range.

3.1 Trajectory and bifurcation diagram

The phase trajectory is a method to evaluate the performance of the chaotic map. The outputs of chaotic maps with superior performance can uniformly distributed on the whole plane. The bifurcation diagrams are plotted for the variable x_i and y_i using the varying control parameters. For the 2D-CLSM, the initial states were set as $(x_0,\ y_0) = (0.312,\ 0.723)$ and control parameter u was set as 0.53. For the 2D-ICM, the initial states were set as $(x_0,\ y_0) = (0.712,\ 0.323)$ and control parameters $(a,\ b)$ were set as $(10,\ 21)$.For the 2D-SLMM, the initial states were set as $(x_0,\ y_0) = (0.532,\ 0.623)$ and control parameters $(\alpha,\ \beta)$ were set as $(2,\ 1)$. As shown in Fig. 1, x_i and y_i of the 2D-CLSM can be spread to all data ranges in the whole control parameter range, which demonstrates that the 2D-CLSM has a broad and continuous parameter range, and can effectively resist the influence of external factors. As shown in Fig. 2, compared to the 2D-CIM and the 2D-SLMM, 2D-CLSM has no periodic structure or specific pattern clustering. Meanwhile, the outputs of 2D-CLSM are uniformly distributed over the whole phase plane, which suggests that the 2D-CLSM owns robust chaotic behaviors for a large range of the control parameter and it is particularly sensitive to the initial values and control parameter (Fig. 3).

3.2 Lyapunov exponent (LE)

LE can be used to evaluate the dynamic properties of chaotic maps, which indicates the average rate of convergence or divergence of two trajectories with similar initial states [34]. For a nonlinear dynamic system $x_{i+1} = f(x_i)$, LE is calculated as follows.

$$LE = \lim_{n\to\infty} \sum_{i=1}^{n-1} \ln\left|f'(x_i)\right| \tag{2}$$

A chaotic map with a positive LE indicates its chaotic behavior. A multi-dimensional chaotic map has multiple LE values. Moreover, if the system has multiple positive LEs, it owns the hyperchaotic behaviors, which means that the system is more sensitive to the initial values and control parameters and its trajectory is more difficult to predict.

The 2D-CLSM has two positive LEs in the $u \in [0,\ 10]$, showing its hyperchaotic properties. In addition, the 2D-CLSM yields bigger LEs compared with the 2D-ICM and 2D-SLMM, demonstrating its preferable chaotic properties.

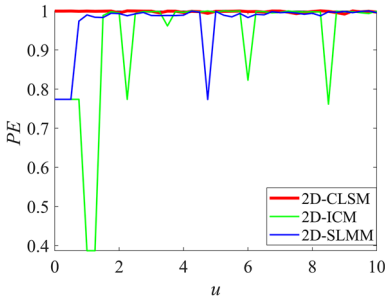

Fig. 4 Comparison with different chaotic maps in the aspect of PE

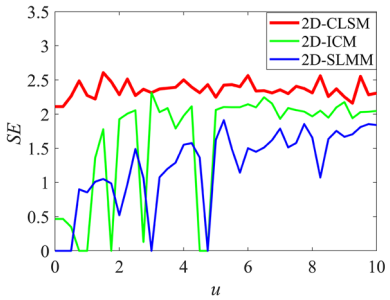

Fig. 5 Comparison with different chaotic maps in the aspect of SE

3.3 Permutation entropy

Permutation entropy (PE) is a quantitative indicator to measure the randomness of the outputs [35]. For a dynamic system, the closer the PE result is to 1, the better the randomness of the system's output sequences. 2D-ICM and 2D-SLMM are selected as a comparison, and it can be seen from Fig. 4 that the proposed 2D-CLSM has the highest PE score, which demonstrates the better randomness and unpredictability of the 2D-CLSM.

3.4 Sample entropy

Sample entropy (SE) is a criterion used to measure the complexity of a time series. For a chaotic system, a larger SE means that the output sequence is more complex and the chaotic system has a better chaotic behavior [36]. The SE of time series $\left(t_1, t_2, \cdots t_k\right)$ is mathematically defined by

$$SE(n,\ h,\ K) = -\log \frac{N_1}{N_2}, \tag{3}$$

where N_1 and N_2 stand for the numbers of vectors satisfying $d|T_{n+1}(i),\ T_{n+1}(j)| < h$ and $d|T_n(i),\ T_n(j)| < h$, respectively. The symbol n is a given dimension and h is a given distance. $d|T_n(i),\ T_n(j)|$ is the Chebyshev distance between $T_n(i)$ and $T_n(j)$.

As shown in Fig. 5, compared to 2D-ICM and 2D-SLMM,

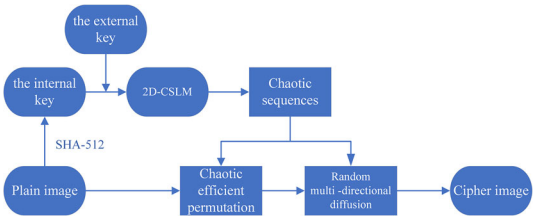

Fig. 6 The flowchart of the proposed CLSM-IEA

the 2D-CLSM owns the largest SE score, indicating that 2D-CLSM owns more complex chaotic behaviors.

3.5 Randomness evaluation

TestU01 is one of the most stringent randomness evaluation methods [37]. We use the three batteries of TestU01 to evaluate the degree of randomness of the sequences by setting different precision gains. As shown in Table 1, compared to the 2D-ICM and 2D-SLMM, the 2D-CLSM passed most of the statistical tests, demonstrating better randomness for 2D-CLSM.

4 The proposed image encryption algorithm CSLM-IEA

The proposed 2D-CSLM has an extremely wide chaotic range, better unpredictability, and complex chaotic behaviors, which lays the foundation for creating a secure encryption algorithm. In this paper, based on the 2D-CSLM, we propose a new image encryption algorithm named CSLM-IEA. The flowchart of the CSLM-IEA is shown in Fig. 6, which employs the typical confusion and diffusion structure [38].

The proposed scheme consists of three phases, (1) key generation related to the plain image, (2) generation of two chaotic sequences with the given initial values and control parameters, and (3) chaotic efficient permutation and random multi-directional diffusion according to the chaotic matrixes. The CSLM-IEA achieves a high security level and high efficiency. It only needs one round of permutation and diffusion with two chaotic sequences to encrypt the plain image into a cipher image in a relatively short time.

4.1 Key generation

Security key is used to determine the initial values and control parameters of the 2D-CSLM. To improve the security of the key, it consists of the internal key (*Key*) and the external one-time key (u_s, x_s, y_s) obtained of sampled natural noise [39]**.** Firstly, we combine SHA-512 function with plain image P according to $K{=}SHA_{512}(P)$, then the obtained 128-bit hexadecimal K is processed by Eq. (4).

$$Key(i) = hex2dec(K((i-1)\times 16+1 : i\times 16))/2^{49}, \quad i \in [1, 8] \tag{4}$$

Based on the performance evaluation of the 2D-CLSM, the 2D-CLSM has a hyperchaotic behavior across $u = [0, 10]$, so the initial values and control parameter of the 2D-CLSM can be obtained through Eq. (5).

$$\begin{cases} u{=}u_s{+}mod((Key(1){+}Key(2)),\ 10) \\ x_0{=}x_s{+}mod((Key(3){+}Key(4) + Key(5)),\ 2) \\ y_0{=}\ y_s{+}mod((Key(6){+}Key(7) + Key(8)),\ 2) \end{cases} \tag{5}$$

Owning to the key is correlated with the plain image, thus, the key generation algorithm has excellent security. Even if only one bit of the plain image is changed, the key is completely different, which can effectively enhance the ability of the CSLM-IEA to resist differential attacks and selected plaintext/ciphertext attacks. At the same time, the sampled value of the noise adds more unpredictability to the key generation, expanding the key space and further improving the security of the key. (u_s, x_s, y_s) is the external one-time key obtained from sampled noise and it was set as $(u_s, x_s, y_s) = (0.751833256729493, 0.391475239716349, 0.153976931726841)$ in our experiments.

4.2 Chaotic efficient permutation

Some existing permutation algorithms of image encryption schemes tend to disrupt the pixels in a fixed row-by-row or column-by-column manner, which provides helpful information for attackers and may lead to a decrease in the security. To improve the security level and randomness of the encryption algorithm, a new chaotic efficient permutation (CEP) is proposed, which confuses the pixel positions in a random and secret order. Besides, it can change the positions of the pixels in horizontal and vertical directions at the same time. After the permutation operation, the pixels can be distributed to different positions in the image, which could greatly reduce the correlation of the pixels. The chaotic efficient permutation is described as follows:

Algorithm 1 Chaotic efficient permutation.

Input: The plain image P with size $M \times N$ and the initial state (x_0, y_0, u).

1: Generate $M \times N$ length chaotic serials x_i and y_i using 2D-CLSM with initial state;

2: A=reshape$\left(x_i, [M, N]\right)$; B=reshape$\left(y_i, [M, N]\right)$;

$X = \mathrm{mod}\left(\mathrm{floor}\left(x_i \times 10^{25}\right), 256\right)$; S=reshape$\left(X, [M, N]\right)$;

3: $S1$ is obtained by sorting each row of A with an ascending order;

4: $S2$ is obtained by sorting each column of B with an ascending order;

5: Combine $S1$ with first column of $S2$ to get $S1'$;

6: Combine $S2$ with first row of $S1$ to get $S2'$;

7: **for** i=1 to M **do**

8: **for** j=1 to N **do**

9: $T\left(S1'(i, j)\right) = P\left(S2'(i, j)\right)$;

10: **end for**

11: **end for**

Output: The shuffled image T.

Figure 7 shows the generation of row index matrix $S1$, column index matrix $S2$, and position index matrix $S1'$ and $S2'$. The elements of $S1$ matrix combine with the corresponding elements of $C1$ to get the position index matrix $S1'$. For instance, the first row of $S1$ combines with the first element of $C1$ to get the first row of $S1'$(4, 2),(2, 2),(3, 2),(1, 2). The elements of $S2$ matrix combine with the corresponding elements of $R1$ to get the position index matrix $S2'$. For instance, the first column of $S2$ combines with the first element in $R1$ to get the first column of $S2'$(2, 4),(4, 4),(1, 4),(3, 4).

Figure 8 provides an example of plain image confused by CEP, the positions in the plain image P are 1 to 16 in order. The plain image of size 4 × 4 is confused by $S1'$ and $S2'$ matrix, then the disordered matrix T is obtained. As shown in Fig. 8, just after employing CEP one time, the pixel positions in the plain image are completely changed. The result of permutation is only related to the chaos matrix. Without knowing the chaos matrix, it is difficult for the attacker to crack the scheme, which improves the security of the encryption scheme; besides, only two different chaos matrices are required for CEP, which could improve the efficiency of the algorithm.

The detailed process of the CEP is described in the following steps.

Step 1 Select the pixels in the P according to the first row of $S2'$, then move these pixels to different locations given to the first row of $S1'$:T(4, 2) = P(2, 4),T(2, 2) = P(1, 2),T(3, 2) = P(4, 3),T(1, 2) = P(1, 1), which are shown by the orange elements in the Fig. 9a.

Step 2 Select the pixels in the P according to the second row of $S2'$, then move these pixels to different locations given to the row column of $S1'$: T(1, 4) = P(4, 4),T(2, 4) = P(4, 2),T(3, 4) = P(1, 3),T(4, 4) = P(3, 1), which are shown by the blue elements in the Fig. 9b.

Step 3 Select the pixels in the P according to the third row of $S2'$,then move these pixels to different locations given to the third row of $S1'$: T(4, 1) = P(1, 4),T(2, 1) = P(3, 2),T(3, 1) = P(2, 3),T(1, 1) = P(2, 1), which are shown in purple elements in the Fig. 9c.

Step 4 Select the pixels in the P according to the fourth row of $S2'$, then move these pixels to different locations given to the fourth row of $S1'$: T(2, 3) = P(3, 4),T(1, 3) = P(2, 2),T(3, 3) = P(3, 3),T(4, 3) = P(4, 1), which are shown as red elements in the Fig. 9d.

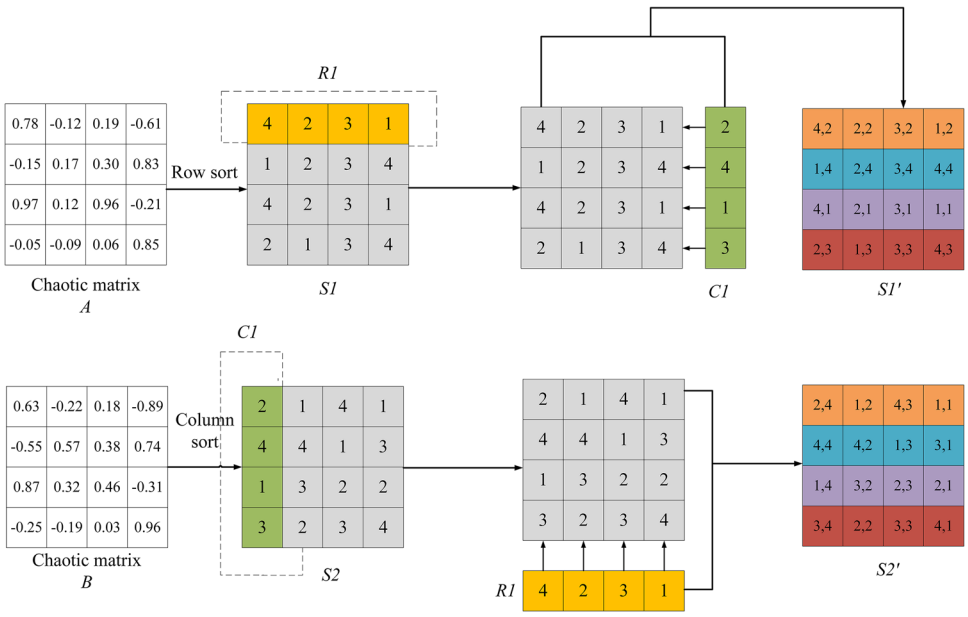

Fig. 7 The generation of the position index matrices

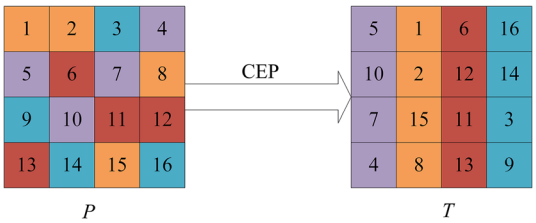

Fig. 8 An example of the plain image P shuffled by CEP

4.3 Random multi-directional diffusion

A reliable encryption algorithm should own the diffusion property, which means that a small change in the plain image should be spread to all the positions in the cipher image. However, most existing diffusion algorithms follow some fixed orders to change the pixels, which may reduce the security of the encryption schemes. Moreover, some diffusion algorithms only process image pixels in a single direction, as shown in Fig. 10.

In this paper, a new random multi-directional diffusion is proposed, it only relies on the chaos matrix to choose the diffusion direction. Without knowing the specifics of the chaos matrix, it is difficult to predict the order of processing pixels and the diffusion result. In this way, we could add more randomness to the encryption images and improve the safety of the encryption scheme. Besides, the proposed diffusion algorithm changes pixels in the diagonal, horizontal, or vertical directions at the same time, which strengthens the performance of diffusion. The detailed process of the random multi-directional diffusion is described as follows.

First, the diffusion selection matrix $S3$ is obtained from the S matrix according to Eq. (6), and the matrix V is obtained

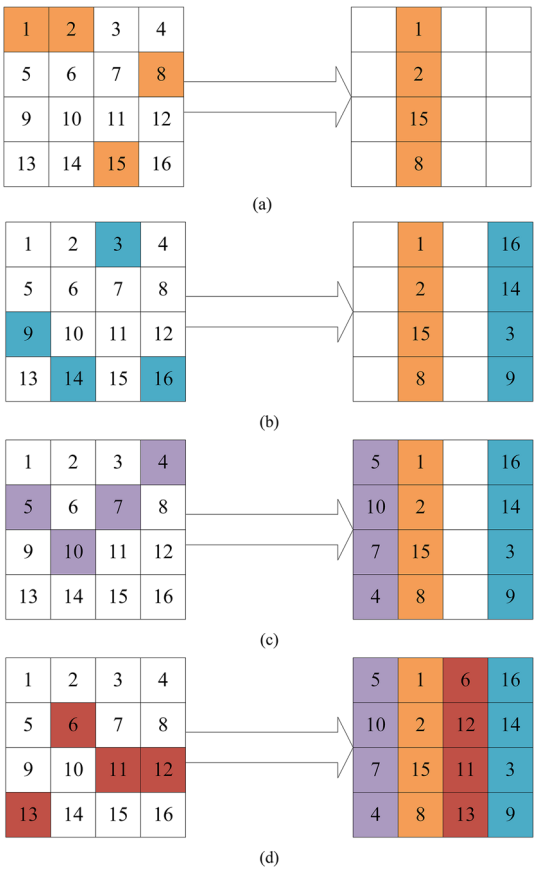

Fig. 9 The detailed process of CEP for the numerical example P. (**a**) the pixels in orange confused by the first row of $S1'$ and $S2'$; (**b**) the pixels in blue confused by the second row of $S1'$ and $S2'$; (**c**) the pixels in purple confused by the third row of $S1'$ and $S2'$; (**d**) the pixels in red confused by the fourth row of $S1'$ and $S2'$

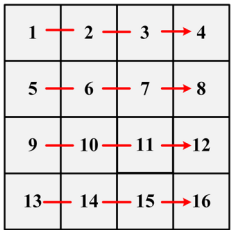

Fig. 10 Diagram illustration of the diffusion process for some existing IEAs

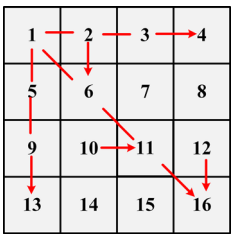

Fig. 11 The schematic illustration of the random multi-directional diffusion

from the X matrix according to Eq. (7).

$$S3 = \mathrm{mod}(S2) \tag{6}$$

$$V = reshape(X,\ [M,\ N]) \tag{7}$$

Then, the diffusion operation is described as the Eq. (8).

$$C_{i,j} = \begin{cases} 1 & \text{if } i = 1,\ j = 1 \\ T_{i,j} \oplus C_{i,j-1} \oplus V_{i,j} & \text{if } i = 1,\ j \neq 1 \\ T_{i,j} \oplus C_{i-1,j} \oplus V_{i,j} & \text{if } i \neq 1,\ j = 1 \\ T_{i,j} \oplus C_{i-1,j-1} \oplus C_{i-1,j} \oplus V_{i,j} & \text{if } i \neq 1,\ j \neq 1,\ S3_{i,j} = 0 \\ T_{i,j} \oplus C_{i-1,j-1} \oplus C_{i,j-1} \oplus V_{i,j} & \text{if } i \neq 1,\ j \neq 1\ ,\ S3_{i,j} = 1 \end{cases} \tag{8}$$

where symbol $\oplus$ denotes the bit-level XOR operation.

The random multi-directional diffusion schematic is shown in Fig. 11. Accordingly, the decryption process of random multi-directional diffusion can be described as the Eq. (9).

$$T_{i,j} = \begin{cases} 1 & \text{if } i = 1,\ j = 1 \\ C_{i,j} \oplus C_{i,j-1} \oplus V_{i,j} & \text{if } i = 1,\ j \neq 1 \\ C_{i,j} \oplus C_{i-1,j} \oplus V_{i,j} & \text{if } i \neq 1,\ j = 1 \\ C_{i,j} \oplus C_{i-1,j-1} \oplus C_{i-1,j} \oplus V_{i,j} & \text{if } i \neq 1,\ j \neq 1,\ S3_{i,j} = 0 \\ C_{i,j} \oplus C_{i-1,j-1} \oplus C_{i,j-1} \oplus V_{i,j} & \text{if } i \neq 1,\ j \neq 1,\ S3_{i,j} = 1 \end{cases} \tag{9}$$

5 Simulation results and performance analysis

The security of the encryption algorithm is a priority to be considered. In this part, various tests and analyses are adopted to evaluate the security of CSLM-IEA in terms of key space, key sensitivity, histogram, adjacent pixel correlation, information entropy analysis, and the ability to defend against differential attacks, noise attacks, and cropping attacks. A variety of images with different sizes and types are used for testing, which are derived from the USC-SIPI image database.[1]

5.1 Key space analysis

A secure encryption scheme requires a large key space, otherwise, an attacker could potentially crack the scheme through brute force attacks. In theory [40], an encryption scheme with a key space exceeding 2^{100} has the potential to effectively resist brute force cracking attacks. The CLSM-IEA employs SHA-512 in combination with a plaintext image and the external one-time key obtained from sampled natural noise to generate the key. Thus, the key space is $2^{512} \times 10^{45}$, which is significantly greater than 2^{100} and indicates that CLSM-IEA can effectively prevent brute-force attacks.

5.2 Key sensitivity analysis

A secure encryption scheme is supposed to own the highly sensitive key. Otherwise, the attackers may restore the original image through incorrect keys with tiny changes and the actual key space would be narrowed. An encryption algorithm with key sensitivity means that a small change in the key will result in totally different results and no valuable information about the plain image can be revealed. We test the key sensitivity of CLSM-IEA by making small changes in the encryption and decryption keys. Figure 12 shows that CLSM-IEA performs well in terms of key sensitivity, and the original image can only be retrieved by the correct key.

5.3 Histogram analysis

Histograms visually show the distribution of pixels at each intensity level and are a widely used technique for statistical analysis. Most of the pixels in a plain image are distributed at a few intensity pixel levels, as shown by the histograms. However, an efficient encryption algorithm can distribute the pixels uniformly at each intensity pixel level, which also means that an attacker cannot get any information about the plain image.

In Fig. 13, the first column shows the histograms of the plain images, while the second column shows the histograms

[1] https://sipi.usc.edu/database/

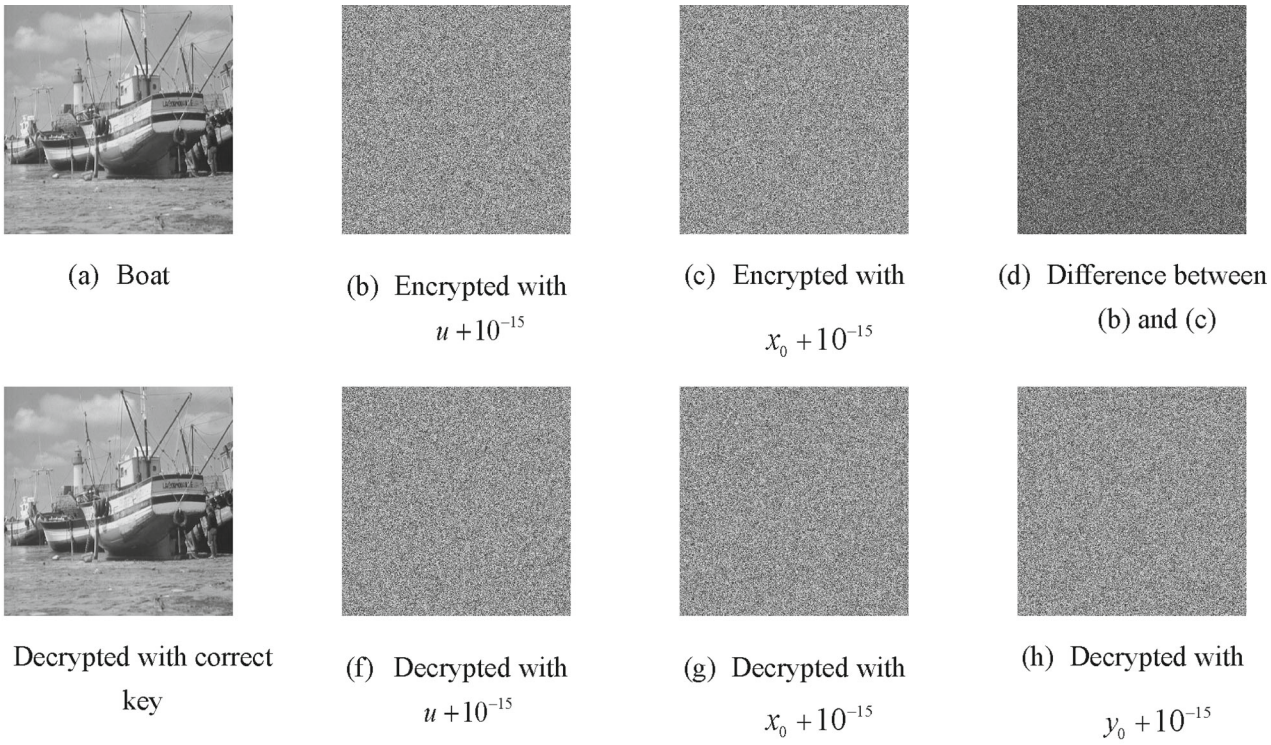

Fig. 12 The key sensitivity analysis

of the cipher images. As Fig. 13 shows, after the encryption process, the pixels are uniformly distributed across all the intensity levels, demonstrating the excellent encryption performance of CLSM-IEA.

5.4 Adjacent pixel correlation

Plain images tend to have strong pixel correlations in different directions. The attacker usually obtains information of a plaintext image through analyzing the correlations of adjacent pixels. Therefore, a secure encryption algorithm should reduce the correlations of neighboring pixels in an image as much as possible [40]. The pixel correlation coefficient is calculated as follows:

$$\begin{cases} r_{xy} = \dfrac{\mathrm{cov}(x,\, y)}{\sqrt{D(x)}\sqrt{D(y)}} \\ E(x) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} x_i \\ D(x) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} (x_i - E(x))^2 \\ \mathrm{cov}(x,\, y) = \dfrac{1}{N}\displaystyle\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \end{cases} \tag{10}$$

where x_i and y_i are gray values of the adjacent pixels. We select five color images of different sizes as the test images. Figure 14 shows the pixel correlations of R, G, and B channels for plain images and cipher images in horizontal, vertical, and diagonal directions.

Table 2 shows the correlation test scores on the R, G, and B channels in the horizontal, vertical, and diagonal directions. The images butterfly and house are $256 \times 256 \times 3$ size while the rest are $512 \times 512 \times 3$ size. As Fig. 14 and Table 2 show, the plain images usually own the high correlations of adjacent pixels, while after the encryption operation, pixels of the plain image are uniformly spread to all directions randomly, and the adjacent pixel correlations of the cipher images are very close to 0, which means that the attacker cannot get any information about the plain image from the pixel correlation.

5.5 Information entropy analysis

Information entropy is an important indicator to measure the amount of information and the degree of randomness for an information source. A secure encryption algorithm should make the image pixels uniformly distributed with high randomness to effectively resist entropy attacks. The formula of information entropy is as follows:

$$H(g) = \sum_{i=0}^{2^N-1} p(g_i) \log \frac{1}{p(g_i)} \tag{11}$$

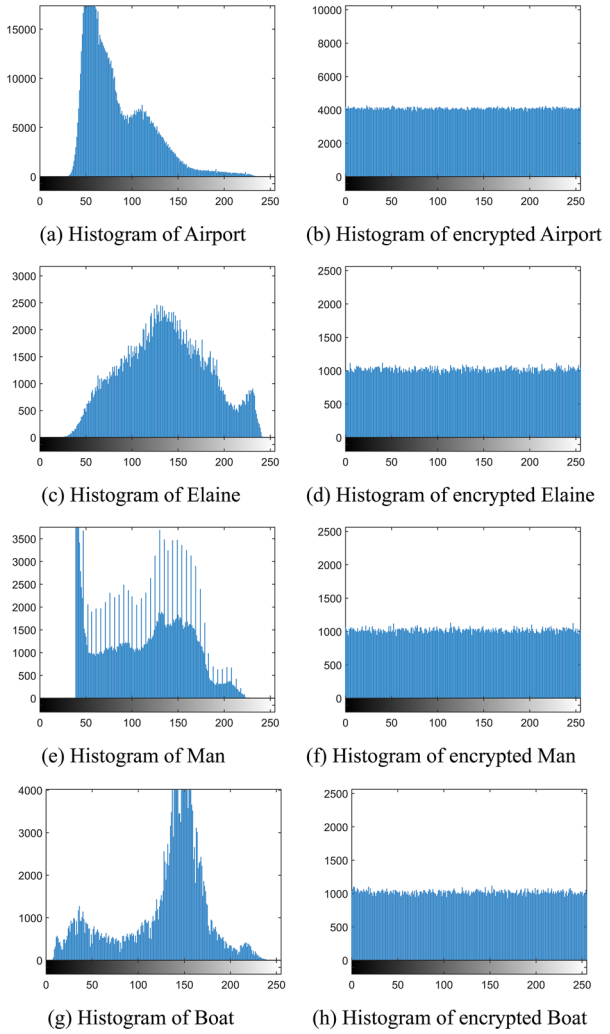

Fig. 13 Histogram analysis of different plain images and encrypted images

where $p(g_i)$ represents the probability of the information source g_i, and N represents the number of bits of g_i.

The theoretical value of information entropy of a completely random 8-bit pixel image is 8. The closer the information entropy of the cipher image is to 8, the better the randomness of the encryption algorithm and its ability to resist entropy attack. We select the same images in the adjacent pixel correlation test and calculate the information entropy of the encrypted images in each channel. It can be seen from Table 1 that after the encryption process, the information entropy is very close to 8, demonstrating the CLSM-IEA could distribute the image pixels uniformly with high randomness.

5.6 Analysis of defense against differential attacks

The differential attack is a useful attack in which the attacker studies the relationship between the plain image and the encrypted image to crack the encryption scheme. An encryption scheme with good diffusion properties can effectively resist differential attacks, which means that a small change in the plain image will result in a completely different encrypted image.

Figure 15 demonstrates the ability of CLSM-IEA to defend against differential attacks. As can be seen from Fig. 15, a one-pixel change in the plaintext image could produce a completely different encryption result, demonstrating the good diffusion property of CLSM-IEA.

The number of pixels change rate ($NPCR$) and the unified averaged changed intensity ($UACI$) are used to quantitatively test the characteristics of the CLSM-IEA against differential attacks. Theoretically, if the UACI and the NPCR are all close to the ideal values of 33.4635070% and 99.6094070%, the encryption scheme is considered to perform well against differential attacks [41]. Supposing that

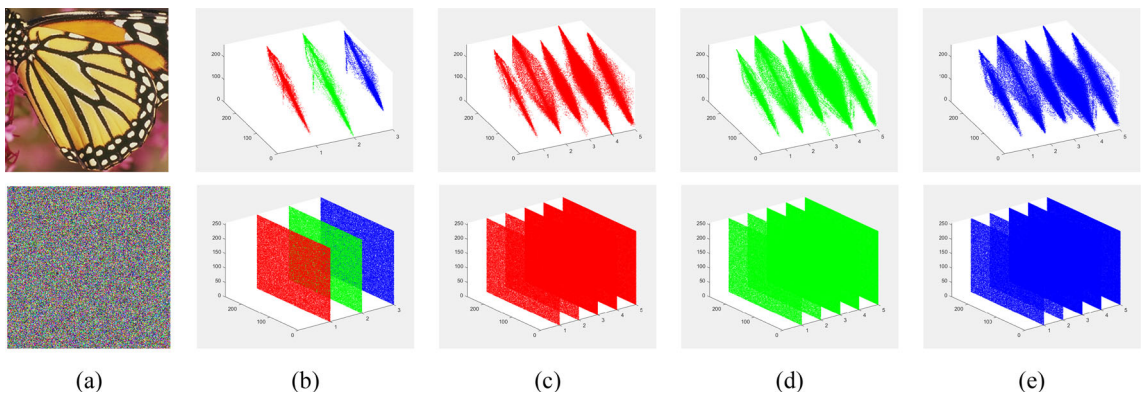

Fig. 14 Analysis of adjacent pixel correlation: (**a**) the color image named Butterfly and corresponding encrypted image; (**b**) correlation on the R, G and B channels of Butterfly from different directions; (**c**) correlation of adjacent pixels in the horizontal direction for five color images; (**d**) correlation of adjacent pixels in the vertical direction for five color images; (**e**) correlation of adjacent pixels in the diagonal direction for five color images

Table 2 The correlation coefficient and information entropy test scores on the R, G, B channels

File name		Plain- image			Cipher-image			Entropy
		H	V	D	H	V	D	
Butterfly	R	0.9233	0.9389	0.8948	0.0036	−0.0030	0.0010	7.9893
	G	0.9116	0.9367	0.8860	0.0020	−0.0053	−0.0075	7.9893
	B	0.8618	0.8859	0.8808	−0.0141	−0.1119	−0.0033	7.9893
House	R	0.9051	0.9304	0.8630	0.0031	−0.0126	0.0012	7.9888
	G	0.9190	0.9845	0.8963	−0.0053	0.0055	−0.0087	7.9893
	B	0.9846	0.9729	0.9812	−0.0023	0.0010	−0.0036	7.9897
4.2.06	R	0.7790	0.7975	0.6984	−0.0114	−0.0192	−0.0054	7.9915
	G	0.8595	0.8755	0.8102	0.0015	−0.0119	0.0110	7.9914
	B	0.8526	0.8399	0.7364	−0.0178	0.0017	−0.0060	7.9916
Baboon	R	0.4695	0.6576	0.5058	−0.0111	−0.0026	−0.0097	7.9914
	G	0.4621	0.6978	0.5327	−0.0065	0.0059	0.0031	7.9916
	B	0.4613	0.6879	0.4576	0.0056	−0.0017	0.0016	7.9916
Peppers	R	0.9715	0.9583	0.9304	0.0027	0.0005	0.0035	7.9916
	G	0.9766	0.9669	0.9450	0.0078	−0.0061	0.0079	7.9917
	B	0.9100	0.9499	0.8800	0.0058	−0.0080	−0.0003	7.9916

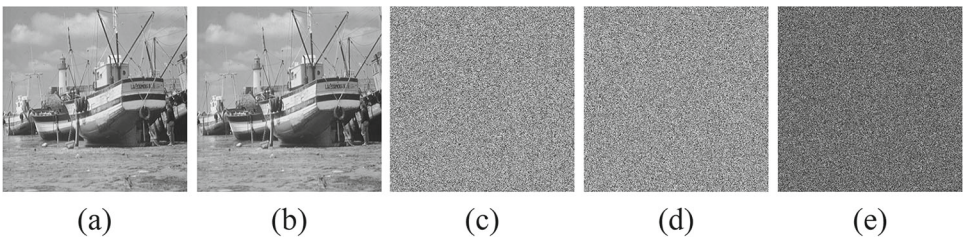

Fig. 15 Analysis of defense against differential attacks: (**a**) the plain image P; (**b**) P' is obtained by randomly changing one pixel of P; (**c**) C is obtained by encrypting P; (**d**) C' is obtained by encrypting P' with the same key; (**e**) the distinction between cipher images C and C'

C_1 and C_2 are encryption images of two plain images with one-bit difference, the mathematical definitions of the UACI and NPCR are as follows:

$$NPCR(C_1, C_2) = \sum_{i,j} \frac{D(i,j)}{R} \times 100\% \tag{12}$$

$$\boldsymbol{UACI}(C_1, C_2) = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{R \times S} \times 100\% \tag{13}$$

$$\boldsymbol{D}(i,j) = \begin{cases} 0 \ \boldsymbol{if}\ C_1(i,j) = C_2(i,j) \\ 1 \ \boldsymbol{if}\ C_1(i,j) \neq C_2(i,j) \end{cases} \tag{14}$$

where R represents the number of pixels and S is the largest pixel value.

In this paper, we adopt a proposed [42] strict standard test, which calculates the critical value of $NPCR$, and $UACI$ based on a given significance level to show the ability of the algorithm to resist differential attacks.

$$N_\alpha^* = \frac{R - \phi^{-1}(\alpha)\sqrt{R/S}}{R+1} \tag{15}$$

$$\begin{cases} u_\alpha^{*-} = \mu_u - \phi^{-1}(\alpha/2)\sigma_u \\ u_\alpha^{*+} = \mu_u + \phi^{-1}(\alpha/2)\sigma_u \end{cases} \tag{16}$$

$$\mu_u = \frac{R+2}{3R+3} \tag{17}$$

$$\sigma_u = \frac{(R+2)\left(R^2+2R+3\right)}{18(R+1)^2 R \times S} \tag{18}$$

Under the 0.05 criterion of α, for 256 × 256-sized images, $N_{0.05}^*$ is 99.5693% and $\left(u_{0.05}^{*-}, u_{0.05}^{*+}\right)$ is (33.2824%, 33.6447%).For 512 × 512-sized images,$N_{0.05}^*$ is 99.5893% and $\left(u_{0.05}^{*-}, u_{0.05}^{*+}\right)$ is (33.3730% , 33.5541%).For 1024 × 1024-sized images,$N_{0.05}^*$ is 99.5994% and $\left(u_{0.05}^{*-}, u_{0.05}^{*+}\right)$ is (33.4183% , 33.5088%). The ability of CLSM-IEA to resist differential attacks is shown in Tables 3, 4 and 5. The file name from 5.1.09 to 5.1.14 are 256 × 256 size, from 5.2.08 to Gray.512 are 512 × 512 size, from 5.3.01 to 7.2.01 are 1024 × 1024 size, the significance level is 0.05. In Tables (3, 4), numbers in bold are test results that successfully passed the test.

As Tables 3 and 4 display, compared to some advanced image encryption schemes, only the CLSM-IEA passed all

Table 3 Comparing with different encryption algorithms in term of the NPCR test

File name	WZ [43]	LX [44]	WL [45]	ZH [46]	Proposed
5.1.11	**99.5801**	99.5532	99.5587	**99.5868**	**99.6061**
5.1.12	**99.6102**	**99.6013**	**99.6212**	**99.6124**	**99.6068**
5.1.13	**99.6203**	**99.6325**	**99.6159**	**99.6456**	**99.6007**
7.1.01	**99.6104**	**99.6089**	**99.6056**	**99.6075**	**99.6089**
7.1.02	99.5832	**99.6123**	**99.6237**	**99.6035**	**99.6090**
7.1.04	**99.5966**	**99.6109**	**99.6105**	99.5855	**99.6086**
7.1.05	**99.5918**	**99.6307**	**99.5998**	**99.6012**	**99.6076**
7.1.06	**99.6010**	99.5769	99.5843	99.5738	**99.6076**
5.3.01	**99.6132**	**99.6035**	**99.6065**	**99.6065**	**99.6091**
7.2.01	**99.6010**	**99.6158**	**99.6065**	**99.6024**	**99.6096**
Pass rate	9/10	8/10	8/10	8/10	10/10

Table 4 Comparing with different encryption algorithms in term of the UACI test

File name	WZ [43]	LX [44]	WL [45]	ZH [46]	Proposed
5.1.11	**33.4316**	**33.4453**	**33.4398**	**33.4267**	**33.4339**
5.1.12	**33.4432**	33.0346	**33.4271**	**33.4526**	**33.4306**
5.1.13	33.2756	**33.5675**	**33.4376**	33.2761	**33.4339**
7.1.01	**33.4756**	**33.4376**	**33.5427**	**33.5073**	**33.4495**
7.1.02	**33.4642**	**33.4246**	33.3498	**33.5149**	**33.4480**
7.1.04	33.3679	**33.4259**	**33.4734**	**33.4673**	**33.4433**
7.1.05	**33.5204**	33.3563	**33.4476**	33.3628	**33.4399**
7.1.06	**33.4657**	**33.4643**	**33.4835**	**33.5149**	**33.4519**
5.3.01	**33.4854**	**33.4235**	**33.4586**	**33.4487**	**33.4473**
7.2.01	**33.4968**	**33.4496**	**33.4724**	**33.4839**	**33.4636**
Pass rate	8/10	8/10	9/10	8/10	10/10

the tests, demonstrating its superior capabilities to defend against differential attacks.

Table 5 shows that all the color images of different sizes pass the stringent test. The NPCR and UACI values are very close to the ideal value, which indicates that CLSM-IEA has an excellent characteristic in resisting differential attacks.

5.7 Noise and cropping attack analysis

Images are inevitable to be affected by noise and lose some data when they are transmitted over network. A reliable encryption scheme should ensure that the decrypted image is visualized with high quality, which indicates that it can reconstruct most of the original information from the cipher image that has been affected by noise disturbance and data loss.

Figure 16 shows the quality of the decrypted image under different levels of salt & pepper noise interference in the cipher image. As shown in the Fig. 16, even though the decrypted images may not be able to retrieve all the content of the plaintext image, most of the information in the original image can still be obtained.

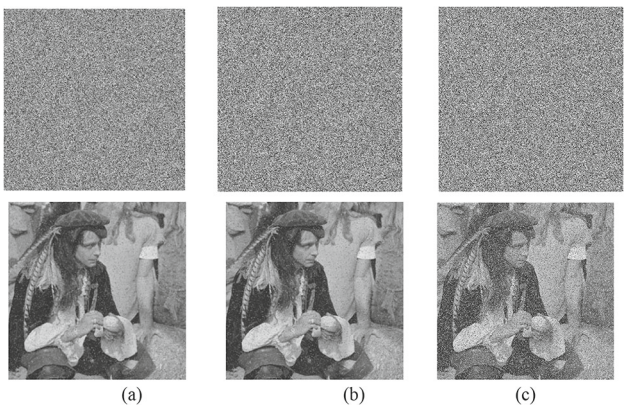

Fig. 16 Noise attack analysis. (**a**) decryption result with 1% 'salt & pepper' noise; (**b**) decryption result with 5% 'salt & pepper' noise; (**c**) decryption result with 10% 'salt & pepper' noise

Table 5 NPCR and UACI test scores using CLSM-IEA for color images of different sizes

Size	File Name	NPCR (%)			UACI (%)			Results
		R	G	B	R	G	B	
256 × 256 × 3	4.1.01	99.6100	99.6086	99.6077	33.4549	33.4629	33.4427	Pass
	4.1.02	99.6094	99.6078	99.6111	33.4438	33.4551	33.4626	Pass
	4.1.03	99.6074	99.6090	99.6089	33.4377	33.4288	33.4388	Pass
512 × 512 × 3	4.2.05	99.6093	99.6103	99.6033	33.4449	33.4449	33.4449	Pass
	4.2.06	99.6084	99.6095	99.6033	33.4397	33.4419	33.4471	Pass
	4.2.07	99.6088	99.6088	99.6033	33.4536	33.4450	33.4471	Pass
1024 × 1024 × 3	2.2.20	99.6095	99.6097	99.6095	33.4471	33.4462	33.4471	Pass
	2.2.21	99.6096	99.6095	99.6086	33.4466	33.4466	33.4472	Pass
	2.2.22	99.6093	99.6091	99.6033	33.4436	33.4417	33.4471	Pass

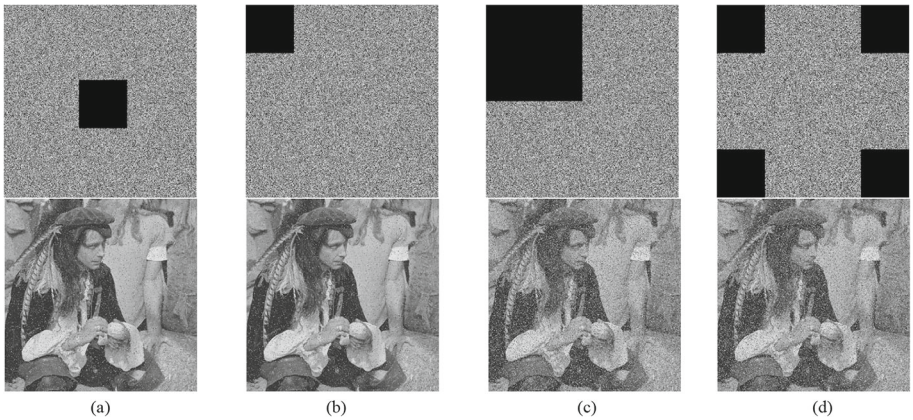

Fig. 17 Data loss attack analysis: (**a**)1/16 data loss of cipher image and its decryption result; (**b**) 1/16 center data loss of cipher image and its decryption result; (**c**) 1/4 data loss of cipher image and its decryption result; (**d**) 1/4 data loss of cipher image and its decryption result

Figure 17 shows the quality of the decrypted images under different levels of data loss for the cipher images. As seen in Fig. 17, even if a large portion of the information in the cipher image has been lost, decrypted images can still recover the main contents of the original image with high visual quality.

As shown in Figs. 16 and 17, the CLSM-IEA has talented resistance to noise and cropping attacks and could produce visually high-quality decrypted images without the local aggregation of missing pixels. This is because the alteration of pixels in the cipher image during decryption affects only a few pixels of decrypted image.

5.8 Speed performance

The image encryption schemes should be suitable for realistic applications owing to the rapid growth of image data capacities. The CLSM-IEA owns high efficiency because it only needs two chaotic sequences and one round of permutation and diffusion. To evaluate the efficiency of CLSM-IEA, we obtain the average time for different sizes of images by 100 experiments. Meanwhile, we compare the efficiency of CLSM-IEA with some state-of-the-art encryption algorithms. The speed performance results are shown in Table 6. The results show that the CLSM-IEA can encrypt different sizes of images in a few seconds, demonstrating its high efficiency (Table 6).

6 Conclusion

To overcome the shortcomings of some existing chaotic maps and improve the security of the encryption schemes, we propose the 2D-CSLM, which displays an extremely wide chaotic range and superior chaotic behaviors in terms of the trajectory, bifurcation diagram, LE, SE, PE and TestU01 tests. Furthermore, an image encryption scheme based on the 2D-CLSM is constructed. The 2D-CLSM-based image encryption algorithm (CLSM-IEA) consists of the chaotic efficient permutation and random multi-directional diffusion. The chaotic efficient permutation can quickly separate adjacent pixels from horizontal and vertical directions at the same time. The random multi-directional diffusion uses a secret order to change pixel values in multiple directions. The chaotic efficient permutation and random multi-directional diffusion dramatically strengthen the randomness of the encryption process and significantly improve the security

Table 6 Comparison with different algorithms in term of encryption time (s)

File name	Size	Proposed	Ref. [22]	Ref. [47]	Ref. [48]
barbara256	256 × 256	0.2888	0.4781	1.1469	0.3981
tank256	256 × 256	0.3008	0.4627	1.1637	0.3428
lake256	256 × 256	0.2985	0.4386	1.1537	0.3682
5.2.10	512 × 512	1.2065	1.7542	3.9756	1.3491
elaine.512	512 × 512	1.2234	1.7619	3.8173	1.3278

of the encryption scheme. Simulations show that CLSM-IEA achieves a high level of security, and can effectively resist various known security attacks. In future work, we will explore the application of the proposed algorithm to video encryption, medical image encryption, and simultaneous super-resolution encryption.

Author contributions X.L.: Resources, Supervision; X.G.: Data Curation, Writing—Original Draft;Software, Validation.

Funding The work was partly funded by the Chongqing Natural Science Foundation (Grant No. cstc2020jcyj-msxmX0767), partly funded by the National Key R&D Program of China (2020YFB1805400), partly funded by the Fundamental Research Funds for the Central Universities (Grant No. SWU-KQ22002), and partly funded by the National Natural Science Foundation of China (Grant No. 61802037).

Data avaliability Data will be made available on request.

Declarations

Conflict of interests The authors declare no competing interests.

Ethical approval This study did not involve human or animal subjects, and thus, no ethical approval was required. The study protocol adhered to the guidelines established by the journal.

References

1. Gong, L.H., Luo, H.X.: Dual color images watermarking scheme with geometric correction based on quaternion FrOOFMMs and LS-SVR. Opt. Laser Technol. **167**, 109665 (2023)
2. Wang, C., Wang, X., Xia, Z., Zhang, C.: Ternary radial harmonic Fourier moments based robust stereo image zero-watermarking algorithm. Inf. Sci. **470**, 109–120 (2019)
3. Sahu, A.K., Swain, G.: High fidelity based reversible data hiding using modified LSB matching and pixel difference. J. King Saud Univ.-Comput. Inf. Sci. **34**(4), 1395–1409 (2022)
4. Zhu, S., Deng, X., Zhang, W., Zhu, C.: Image encryption scheme based on newly designed chaotic map and parallel DNA coding. Mathematics. **11**(1), 231 (2023)
5. Zheng, P.X., Dai, Q., Li, Z.L., Ye, Z.Y., Xiong, J., Liu, H.C., Zheng, G.X., Zhang, S.: Metasurface-based key for computational imaging encryption. Sci. Adv. **7**(21), eabg0363 (2021)
6. Wang, B., Zhang, B.F., Liu, X.W.: An image encryption approach on the basis of a time delay chaotic system. Optik. **225**, 165737 (2021)
7. Li, Y., Yu, H., Song, B., Chen, J.: Image encryption based on a single-round dictionary and chaotic sequences in cloud computing. Concurr. Comput.-Pract. Exp. **33**(7), e5182 (2021)
8. Li, X., Mou, J., Cao, Y., Santo, B.: An optical image encryption algorithm based on a fractional-order laser hyperchaotic system. Int. J. Bifurcation Chaos. **32**(03), 2250035 (2022)
9. Huang, X., Dong, Y., Ye, G., Shi, Y.: Meaningful image encryption algorithm based on compressive sensing and integer wavelet transform. Front. Comput. Sci. **17**(3), 173804 (2023)
10. Gao, X., Sun, B., Cao, Y., Banerjee, S., Mou, J.: A color image encryption algorithm based on hyperchaotic map and DNA mutation. Chin. Phys. B **32**(3), 030501 (2023)
11. Wang, J., Geng, Y.C., Han, L., Liu, J.Q.: Quantum Image Encryption Algorithm Based on Quantum Key Image. Int. J. Theor. Phys. **58**(1), 308–322 (2019)
12. Abd El-Latif, A.A., Abd-El-Atty, B., Amin, M., Iliyasu, A.M.: Quantum-inspired cascaded discrete-time quantum walks with induced chaotic dynamics and cryptographic applications. Sci. Rep. **10**(1), 1930 (2020)
13. Zhou, N.R., Tong, L.J., Zou, W.P.: Multi-image encryption scheme with quaternion discrete fractional Tchebyshev moment transform and cross-coupling operation. Signal Process. **211**, 109107 (2023)
14. Wang, S., Wang, C., Xu, C.: An image encryption algorithm based on a hidden attractor chaos system and the Knuth-Durstenfeld algorithm. Opt. Lasers Eng. **128**, 105995 (2020)
15. Wang, X., Liu, P.: A new full chaos coupled mapping lattice and its application in privacy image encryption. IEEE Trans. Circuits Syst. I-Regul. Pap. **69**(3), 1291–1301 (2022)
16. Liu, X., Tong, X., Wang, Z., Zhang, M.: A new n-dimensional conservative chaos based on Generalized Hamiltonian System and its' applications in image encryption. Chaos Solitons Fractals. **154**, 111693 (2022)
17. Zhao, H., Wang, S., Wang, X.: Fast image encryption algorithm based on multi-parameter fractal matrix and MPMCML system. Chaos Solitons Fractals. **164**, 112742 (2022)
18. Habutsu, T., Nishio, Y., Sasase, I., Mori, S.: A secret key cryptosystem by iterating a chaotic map. N/A. **547**, 127–140 (1991)
19. 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. **546**, 1063–1083 (2021)
20. Erkan, U., Toktas, A., Toktas, F., Alenezi, F.: 2D eπ-map for image encryption. Inf. Sci. **589**, 770–789 (2022)
21. Hua, Z., Zhou, Y., Huang, H.: Cosine-transform-based chaotic system for image encryption. Inf. Sci. **480**, 403–419 (2019)
22. Teng, L., Wang, X., Xian, Y.: Image encryption algorithm based on a 2D-CLSS hyperchaotic map using simultaneous permutation and diffusion. Inf. Sci. **605**, 71–85 (2022)
23. Mansouri, A., Wang, X.: A novel one-dimensional sine powered chaotic map and its application in a new image encryption scheme. Inf. Sci. **520**, 46–62 (2020)
24. Hua, Z., Zhu, Z., Chen, Y., Li, Y.: Color image encryption using orthogonal Latin squares and a new 2D chaotic system. Nonlinear Dyn. **104**(4), 4505–4522 (2021)
25. Hua, Z., Zhou, Y., Pun, C.-M., Chen, C.L.P.: 2D Sine Logistic modulation map for image encryption. Inf. Sci. **297**, 80–94 (2015)

26. Gao, X., Mou, J., Xiong, L., Sha, Y., Yan, H., Cao, Y.: A fast and efficient multiple images encryption based on single-channel encryption and chaotic system. Nonlinear Dyn. **108**(1), 613–636 (2022)
27. Chen, Z.H., Yuan, X.H., Yuan, Y.B., Iu, H.H.C., Fernando, T.: Parameter identification of chaotic and hyper-chaotic systems using synchronization-based parameter observer. IEEE Trans. Circuits Syst. I-Regul. Pap. **63**(9), 1464–1475 (2016)
28. Liu, M.Q., Zhang, S.L., Fan, Z., Zheng, S.Y., Sheng, W.H.: Exponential H∞ synchronization and state estimation for chaotic systems via a unified model. IEEE Trans. Neural Netw. Learn. Syst. **24**(7), 1114–1126 (2013)
29. Farajallah, M., El Assad, S., Deforges, O.: Cryptanalyzing an image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. Multimed. Tools Appl. **77**(21), 28225–28248 (2018)
30. Mollaeefar, M., Sharif, A., Nazari, M.: A novel encryption scheme for colored image based on high level chaotic maps. Multimed. Tools Appl. **76**(1), 607–629 (2017)
31. Liu, P., Zhang, T., Li, X.: A new color image encryption algorithm based on DNA and spatial chaotic map. Multimed. Tools Appl. **78**(11), 14823–14835 (2019)
32. Teng, L., Wang, X., Yang, F., Xian, Y.: Color image encryption based on cross 2D hyperchaotic map using combined cycle shift scrambling and selecting diffusion. Nonlinear Dyn. **105**(2), 1859–1876 (2021)
33. Cao, W., Mao, Y., Zhou, Y.: Designing a 2D infinite collapse map for image encryption. Signal Process. **171**, 107457 (2020)
34. May, R.M.: Simple mathematical-models with very complicated dynamics. Nature **261**(5560), 459–467 (1976)
35. Bandt, C., Pompe, B.: Permutation entropy: A natural complexity measure for time series. Phys. Rev. Lett. **88**(17), 174102 (2002)
36. Richman, J.S., Moorman, J.R.: Physiological time-series analysis using approximate entropy and sample entropy. Am. J. Physiol.-Heart Circul. Physiol. **278**(6), H2039–H2049 (2000)
37. Chai, X., Bi, J., Gan, Z., Liu, X., Zhang, Y., Chen, Y.: Color image compression and encryption scheme based on compressive sensing and double random encryption strategy. Signal Process. **176**, 107684 (2020)
38. Liu, H., Kadir, A., Xu, C.: Cryptanalysis and constructing S-Box based on chaotic map and backtracking. Appl. Math. Comput. **376**, 125153 (2020)
39. Alvarez, G., Li, S.: Some basic cryptographic requirements for chaos-based cryptosystems. Int. J. Bifurcation Chaos. **16**(8), 2129–2151 (2006)
40. Liu, H., Kadir, A., Xu, C.: Color Image Encryption with Cipher Feedback and Coupling Chaotic Map. Int. J. Bifurcation Chaos. **30**(12), 2050173 (2020)
41. Toktas, A., Erkan, U., Ustun, D.: An image encryption scheme based on an optimal chaotic map derived by multi-objective optimization using ABC algorithm. Nonlinear Dyn. **105**(2), 1885–1909 (2021)
42. Liu, H., Liu, J., Ma, C.: Constructing dynamic strong S-Box using 3D chaotic map and application to image encryption. Multimed. Tools Appl. **82**(16), 23899–23914 (2023)
43. Wu, Y., Noonan, J.P., Agaian, S.S.: NPCR and UACI randomness tests for image encryption, cyber journals: multidisciplinary journals in science and technology. J. Sel. Areas Telecommun. (JSAT), 31–38 (2011).
44. Wang, X., Wang, Q., Zhang, Y.: A fast image algorithm based on rows and columns switch. Nonlinear Dyn. **79**(2), 1141–1149 (2015)
45. Xu, L., Li, Z., Li, J., Hua, W.: A novel bit-level image encryption algorithm based on chaotic maps. Opt. Lasers Eng. **78**, 17–25 (2016)
46. Liu, W., Sun, K., Zhu, C.: A fast image encryption algorithm based on chaotic map. Opt. Lasers Eng. **84**, 26–36 (2016)
47. Hua, Z., Zhou, Y.: Design of image cipher using block-based scrambling and image filtering. Inf. Sci. **396**, 97–113 (2017)
48. Ma, C., Mou, J., Xiong, L., Banerjee, S., Liu, T., Han, X.: Dynamical analysis of a new chaotic system: asymmetric multistability, offset boosting control and circuit realization. Nonlinear Dyn. **103**(3), 2867–2880 (2021)