Information Sciences 546 (2021) 1063–1083

Contents lists available at ScienceDirect

Information Sciences

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

Cross-plane colour image encryption using a two-dimensional logistic tent modular map

Zhongyun Hua [a,*], Zhihua Zhu [a], Shuang Yi [b], Zheng Zhang [c], Hejiao Huang [a]

[a] School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, Shenzhen 518055, China
[b] Engineering Research Center of Forensic Science, Chongqing Education Committee, College of Criminal Investigation, Southwest University of Political Science and Law, Chongqing 401120, China
[c] Shenzhen Key Laboratory of Visual Object Detection and Recognition, Harbin Institute of Technology, Shenzhen 518055, China

ARTICLE INFO

Article history:
Received 29 November 2019
Received in revised form 31 July 2020
Accepted 17 September 2020
Available online 30 September 2020

Keywords:
Chaotic system
Colour-image security
Hyperchaotic system
Image encryption
Image security
Non-linear system

ABSTRACT

Chaotic systems are suitable for image encryption owing to their numerous intrinsic characteristics. However, chaotic maps and algorithmic structures employed in many existing chaos-based image encryption algorithms exhibit various shortcomings. To overcome these, in this study, we first construct a two-dimensional logistic tent modular map (2D-LTMM) and then develop a new colour image encryption algorithm (CIEA) using the 2D-LTMM, which is referred to as the LTMM-CIEA. Compared with the existing chaotic maps used for image encryption, the 2D-LTMM has a fairly wide and continuous chaotic range and more uniformly distributed trajectories. The LTMM-CIEA employs cross-plane permutation and non-sequential diffusion to obtain the diffusion and confusion properties. The cross-plane permutation concurrently shuffles the row and column positions of pixels within the three colour planes, and the non-sequential diffusion method processes the pixels in a secret and random order. The main contributions of this study are the construction of the 2D-LTMM to overcome the shortcomings of existing chaotic maps and the development of the LTMM-CIEA to concurrently encrypt the three colour planes of images. Simulation experiments and security evaluations show that the 2D-LTMM outperforms recently developed chaotic maps, and the LTMM-CIEA outperforms several state-of-the-art image encryption algorithms in terms of security.

1. Introduction

As a result of the rapid development of information technology, considerable amount of digital information is generated and spreads over all types of networks. Digital images have a straightforward visual effect and are consequently one of the most widely used digital data formats. Furthermore, a digital image has significant potential and additional information [39]. For example, a personal photograph can convey not only the physical appearance of someone but also other details such as their health and age. Therefore, protection of classified digital images from unauthorised access in systems such as cloud computing is of the utmost importance [34,37]. In some cases, the entire contents should be protected. However, in certain artificial intelligence scenarios, only some of the image features comprise useful information that requires protection [38,40,45]. Encryption is a popular and efficient technique for ensuring the privacy of digital images [10,21].

* Corresponding author.
E-mail address: huazyum@gmail.com (Z. Hua).

https://doi.org/10.1016/j.ins.2020.09.032
0020-0255/

An effective image encryption strategy is the treatment of a digital image as a bit stream and then encrypt this bit stream using traditional data encryption schemes, such as the triple data encryption standard, advanced encryption standard, and international data encryption algorithm. However, compared with a bit stream, a digital image has distinct intrinsic properties, including data redundancies and large pixel correlations. By treating a digital image as a bit stream to be encrypted via existing data encryption algorithms, we neglect to consider these properties. Therefore, these strategies suffer from numerous shortcomings, such as low encryption efficiencies [31]. Thus, development of new image encryption algorithms that adequately consider the properties of digital images can significantly enhance the efficiency of image protection.

Several image encryption algorithms have been designed using various techniques from diverse fields [32], such as chaos theory [7,48,47,8], frequency domain transformation [41], compressive sensing [46], and DNA coding [42]. Among these techniques, chaos theory is the most widely used because chaotic systems have many important intrinsic properties, including aperiodicity, pseudo-random behaviour, and initial-state sensitivity; these properties are fairly similar to the concepts involved in image encryption [17,22]. A recent survey [5] has shown that more than 32% of existing image encryption algorithms were based on chaos theory. For example, Zhang proposed a new lifting transform-based image encryption algorithm using chaos [44]. This algorithm differs from traditional permutation-diffusion structures and achieves a high level of security. However, chaos-based image encryption algorithms have some disadvantages [5]. For instance, the chaotic systems employed may have many notable characteristics such as discrete and narrow chaotic ranges and incomplete output distributions [10,22]. In addition, the structures of many encryption algorithms suffer from performance and efficiency shortcomings. For example, most image encryption algorithms process image pixels in fixed orders, which may facilitate cryptanalysis [24,21]; as a result, these algorithms offer an inefficient encryption process and weak security levels for the encrypted results [47,26].

Many chaos-based image encryption algorithms have disadvantages in terms of the chaotic systems employed and their encryption structures. To address these limitations, we first develop a two-dimensional logistic tent modular map (2D-LTMM). Performance evaluations show that the 2D-LTMM has a wide and continuous chaotic range and exhibits robust chaotic behaviour. In addition, the trajectories of the 2D-LTMM can be uniformly distributed over the entire phase plane, thereby indicating the sizeable randomness of its outputs. Using the 2D-LTMM, we develop a colour image encryption algorithm (CIEA), which we refer to as LTMM-CIEA. The LTMM-CIEA adequately considers the properties of colour images and employs n rounds of cross-plane permutation and non-sequential diffusion. The cross-plane permutation concurrently shuffles the row and column positions of pixels within the red, green, and blue colour planes via a single operation, and the non-sequential diffusion method processes the pixels in all three colour planes in a secret and random order. Simulation experiments and security evaluations demonstrate the high efficiency and security of the LTMM-CIEA. Comparative analysis indicates that the LTMM-CIEA can outperform several state-of-the-art encryption algorithms. The main contributions of this study are as follows.

(1) Existing chaotic maps have discontinuous chaotic ranges, periodic windows, and non-uniformly distributed trajectories, thereby limiting the performance of chaos-based applications. To overcome these shortcomings of existing chaotic maps, we propose a new 2D chaotic map called the 2D-LTMM.
(2) Compared with existing chaotic maps, the 2D-LTMM exhibits a continuous and considerably wider chaotic range, as well as robust chaotic behaviours and uniformly distributed trajectories, thereby making it suitable for image encryption.
(3) Many existing CIEAs have weaknesses in their encryption structures. Thus, using the 2D-LTMM, we propose LTMM-CIEA, a new CIEA to overcome the shortcomings of existing image encryption algorithms.
(4) Compared with the existing CIEAs, the LTMM-CIEA employs cross-plane permutation and non-sequential diffusion. The cross-plane permutation concurrently shuffles the row and column positions of pixels within the three colour planes, and the non-sequential diffusion method processes pixels in these planes in a secret and random order.
(5) Simulation experiments and security evaluations demonstrate that the LTMM-CIEA offers a high security level and outperforms the state-of-the-art image encryption algorithms.

The remainder of this paper is organised as follows. Section 2 presents a review of the relevant research on chaotic systems and image encryption algorithms. Section 3 details the proposed 2D-LTMM and an analysis of its chaotic complexity. Section 4 introduces our CIEA, referred to as the LTMM-CIEA. Section 5 details the LTMM-CIEA simulations and comparisons of its efficiency with those of several other algorithms. Section 6 presents security evaluations of the LTMM-CIEA and comparisons with several other image encryption algorithms. Section 7 provides the conclusions.

2. Related work

This section presents a review of existing chaotic systems and image encryption algorithms and further discusses their properties.

2.1. Chaotic maps

A one-dimensional (1D) chaotic map typically has a simple structure and a small number of variables, thereby making its behaviour readily predictable under certain conditions [14,20]. Furthermore, chaos degradation can easily occur in 1D chao-

tic maps simulated on platforms with finite precision [15]. When chaos degradation occurs, a chaotic map will lose its chaotic properties and the encryption algorithm it forms a component of will be rendered ineffective [28]. Examples of 1D chaotic maps include the logistic, sine, and tent maps [10]. By contrast, multi-dimensional (MD) chaotic maps typically have complex structures and chaotic behaviours, making it difficult to predict their behaviours or induce chaos degradation. MD chaotic maps with complex structures incur high implementation costs, making them inefficient for use in applications. Examples of MD chaotic maps include the three-dimensional piecewise-logistic map [30] and four-dimensional logistic map [33]. Therefore, considering the performance and implementation costs of chaos systems, 2D chaotic maps represent good choices for image encryption.

Many 2D chaotic maps have recently been developed for image encryption, including the 2D sine logistic modulation map (2D-SLMM) [10], 2D logistic-adjusted-sine map (2D-LASM) [9], 2D logistic-sine-coupling map (2D-LSCM) [7], and 2D logistic-modulated-sine-coupling-logistic (2D-LSMCL) map [48]. The bifurcation diagrams and trajectories of these 2D chaotic maps are plotted in Fig. 1. Note: the bifurcation diagrams are plotted for the variable x_i under the change of one parameter, whereas the trajectories (x_i, y_i) are plotted by setting the parameters at fixed values. By selecting fixed parameters, we allow the corresponding chaotic maps to exhibit complex chaotic behaviours. As illustrated in the bifurcation diagrams and trajectories, the 2D chaotic maps have discontinuous chaotic ranges with many periodic windows. In addition, small perturbations to their parameters may make the systems lose their chaotic behaviours. Moreover, the bifurcation diagrams and trajectories exhibit certain patterns, in which their outputs are non-uniformly distributed on the entire phase plane; this indicates that their outputs lack high randomness. Thus, these 2D chaotic maps may have some performance limitations when used for image encryption.

2.2. Image encryption algorithms

Many image encryption algorithms have been designed using different techniques. We list some representative examples. Liu and Kadir [18] developed an asymmetric colour image scheme based on chaos theory. First, their algorithm circularly shifts the pixels in the red, green, and blue colour planes through the rows and columns, using pseudo-random arrays; then, it performs *XOR* operations to diffuse all the pixels. Chen et al. [3] presented a colour image encryption scheme that used the fractional Fourier transform. Their algorithm employed a single-plane optical asymmetric strategy to encrypt colour images. Many similar image encryption algorithms have been designed; however, these algorithms have several disadvantages. In particular, the security efficiency levels of the chaos-based image encryption algorithms strongly depend on the chaotic maps employed; however, most of these chaotic maps do not realise stable and complex chaotic behaviours. In addition, the structures of the optical technique-based image encryption algorithms are highly complex, and thus incur high implementation costs. Owing to these disadvantages, the existing algorithms exhibit performance limitations in many scenarios, such as cloud computing [35,29] and Internet-of-Things systems [36,23]. Table 1 lists some representative image encryption algorithms and their properties.

Colour images contain more redundant information and more straightforward visual effects than greyscale ones; as such, many specialised encryption algorithms have been developed for colour images [27,13]. According to Shannon's theory, an encryption algorithm should have the properties of confusion and diffusion. Most CIEAs first separate the red, green, and blue colour planes before individually encrypting them, finally recombining the three encrypted results as a colour image [21,24]. A schematic illustration of this encryption strategy is presented in Fig. 2, indicating that this strategy has some notable disadvantages. For example, a change in one colour plane cannot spread rapidly to all the pixels, thereby resulting in low security levels. By contrast, other CIEAs first combine the three colour planes into a greyscale image (which is three times the size of the original colour image) and then encrypt this greyscale image to produce the encrypted information [16,26]. This encryption strategy can result in low-efficiency encryption. Thus, to encrypt a colour image, most existing encryption strategies treat the image as greyscale; they do not consider and utilise the specific characteristics of colour images. Thus, it is crucial to develop CIEAs that utilise these characteristics. Fig. 3 schematically illustrates an example of a colour image encryption strategy that considers the characteristics of colour images; here, a pixel can be randomly permuted to any position of the three colour planes, and pixel changes can be spread over the entire image.

3. 2D-LTMM

In this section, we propose the 2D-LTMM, evaluate its chaotic performance, and compare this performance with those of some recently developed 2D chaotic maps.

3.1. Definition of 2D-LTMM

We develop the 2D-LTMM using two classical 1D chaotic maps: logistic and tent maps. The mathematical definitions of logistic and tent maps are

$$x_{i+1} = 4rx_i(1 - x_i), \tag{1}$$

and

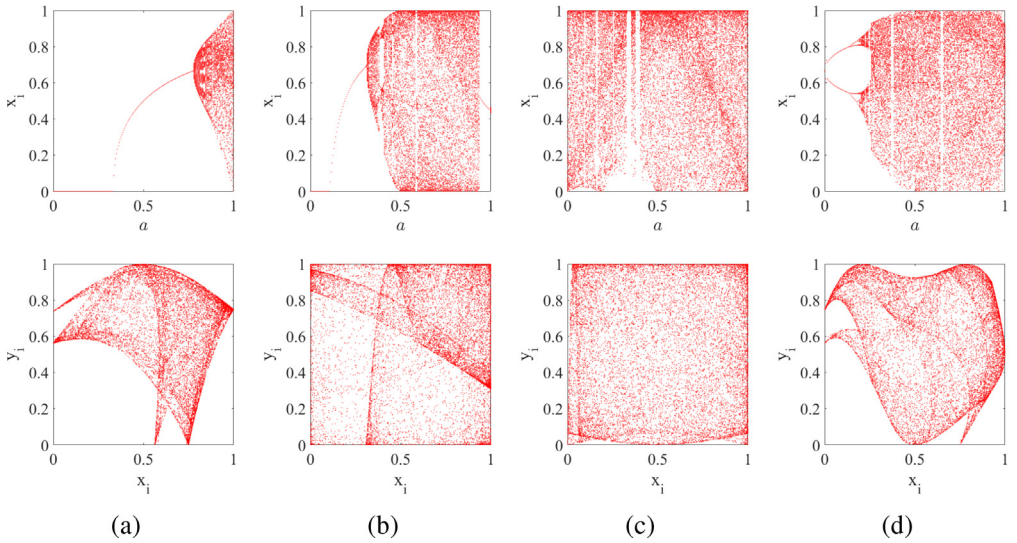

Fig. 1. Bifurcation diagrams and trajectories of several 2D chaotic systems: (a) 2D-SLMM under $b = 3$ and $a \in (0, 1)$, and its trajectory under $(a, b) = (1, 3)$; (b) 2D-LASM under $a \in (0, 1)$, and its trajectory under $a = 0.9$; (c) 2D-LSCM under $a \in (0, 1)$, and its trajectory under $a = 0.98$; (d) 2D-LSMCL under $b = 3$ and $a \in (0, 1)$, and its trajectory under $(a, b) = (0.75, 3)$.

Table 1
Representative image encryption algorithms and their properties.

Encryption algorithm	Encryption strategy	Limitations
Ref. [26]	Chaos theory	High complexity, simple behaviour
Ref. [11]	Chaos theory	Small key space, low efficiency
Ref. [49]	Chaos theory	Small key space
Ref. [6]	Optical	High complexity
Ref. [19]	DNA coding	High complexity, low efficiency
Ref. [46]	Compressive sensing, Mellin transform	High complexity
Ref. [25]	Chaos theory, cellular automata	Small number of reversal rules
Ref. [41]	Frequency domain transform	Low quality or data loss
Ref. [1]	Hash function	Potential redundancy or data loss
Ref. [4]	Bit plane	Potential redundancy or data loss

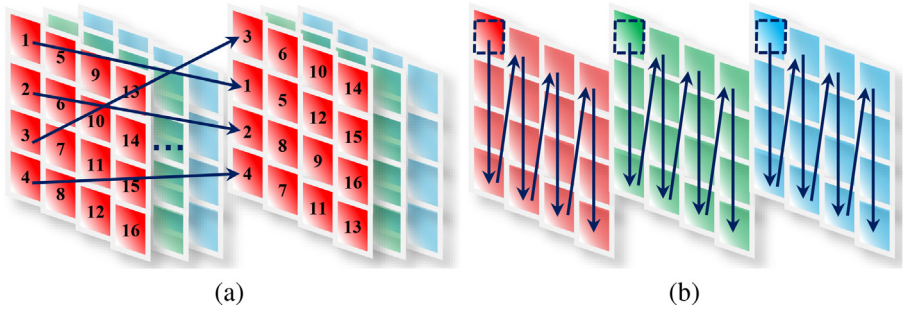

Fig. 2. Schematic illustration of most existing CIEAs: (a) confusion process and (b) diffusion process.

$$x_{i+1} = \begin{cases} 2rx_i & \text{for } x_i < 0.5; \\ 2r(1 - x_i) & \text{for } x_i \geqslant 0.5, \end{cases} \tag{2}$$

respectively; here, r is a control parameter for the two chaotic maps, and $r \in [0, 1]$.

The 2D-LTMM is derived from the logistic and tent maps. First, we combine the outputs of the logistic and tent maps; then, we fold the results obtained from the two chaotic maps into a fixed range using a modular operation, before finally extending the dimensions of the new chaotic map from 1D to 2D to obtain the 2D-LTMM. The mathematical expression of the 2D-LTMM is as follows:

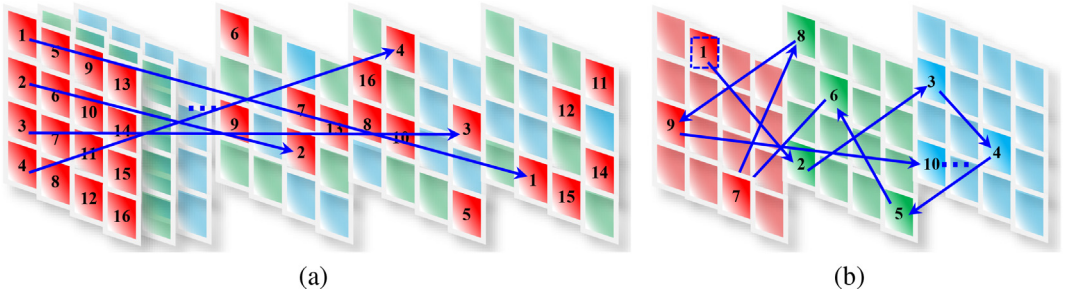

Fig. 3. Schematic illustration of an example encryption strategy that considers the properties of colour images: (a) confusion process and (b) diffusion process.

$$\begin{cases} x_{i+1} = \begin{cases} (4ax_i(1-x_i)+2by_i) \bmod 1 & \text{for } y_i < 0.5; \\ (4ax_i(1-x_i)+2b(1-y_i)) \bmod 1 & \text{for } y_i \geqslant 0.5; \end{cases} \\ y_{i+1} = \begin{cases} (4ay_i(1-y_i)+2bx_i) \bmod 1 & \text{for } x_i < 0.5; \\ (4ay_i(1-y_i)+2b(1-x_i)) \bmod 1 & \text{for } x_i \geqslant 0.5. \end{cases} \end{cases} \tag{3}$$

The parameters a and b in the 2D-LTMM are inherited from the logistic and tent maps, respectively. The modular operation in the 2D-LTMM is a globally bounded operation; it can always fold the value into a fixed range; thus, users can set a and b as any large values. In this study, we investigated the performance of the 2D-LTMM in terms of its parameters $a, b \in [1, 100]$.

3.2. Performance Evaluation

The proposed 2D-LTMM can exhibit complex chaotic behaviours. Here, we evaluate its chaotic performance in terms of its bifurcation diagram and trajectory, Lyapunov exponent (LE), and sample entropy (SE).

3.2.1. Bifurcation diagram and trajectory

The bifurcation diagram shows the visited or asymptotically approached values for a dynamical system with different control parameters, and it illustrates how a non-linear system exhibits chaotic dynamics. The trajectory of a 2D chaotic map illustrates the outputs of this chaotic map in its 2D phase plane. Fig. 4 shows the bifurcation diagrams and trajectory obtained for the 2D-LTMM. The initial states were set as $(x_0, y_0) = (0.2, 0.8)$, and the two control parameters used for plotting the trajectory were set as $(a, b) = (50, 50)$. The two bifurcation diagrams demonstrate that the variables x and y can visit or asymptotically approach the entire data range, and that the trajectories are uniformly distributed over the whole phase plane, indicating that the chaotic behaviours of the 2D-LTMM are robust over the entire parameter ranges. As shown in Fig. 1, 2D-SLMM, 2D-LASM, 2D-LSCM, and 2D-LSMCL have discontinuous chaotic ranges, and their trajectories cannot occupy the entire phase plane at random. Thus, compared with other 2D chaotic maps, the 2D-LTMM can achieve higher chaotic complexity.

3.2.2. LE

The LE is a numerical indicator developed to evaluate the complexity of a dynamical system. For two trajectories of a non-linear system starting from similar initial states, the LE tests their average exponential divergence rate. The LE of a differentiable non-linear system $x_{i+1} = f(x_i)$ can be calculated as

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f\prime(x_i)|. \tag{4}$$

A positive LE indicates that similar trajectories of a non-linear system diverge exponentially at each iteration and evolve into two entirely different trajectories over time. Thus, a positive LE is an indicator of chaotic behaviour if the phase plane of the system is also compacted; here, a larger LE denotes better chaotic performance. For an n-dimensional chaotic map, its trajectories diverge into n dimensions; thus, it has n LEs, of which the largest LE (LLE) is an indicator of chaos. When the trajectory of an n-dimensional chaotic map exponentially diverges in several directions, it can exhibit more than one positive LE; in such cases, the system is hyperchaotic, which is a considerably more complicated type of behaviour than chaotic behaviour.

A 2D chaotic map has two LEs. Fig. 5 shows the two LEs for our proposed 2D-LTMM and compares them with those of four different 2D chaotic maps. As shown in Figs. 5(a) and (b), the 2D-LTMM can obtain two positive LEs for the entire range of control parameters $a, b \in [1, 100]$, thereby indicating that it exhibits hyperchaotic behaviour in these parameter ranges. The 2D-SLMM, 2D-LTMM, and 2D-LSMCL have two control parameters, whereas the 2D-LASM and 2D-LSCM have only one. To

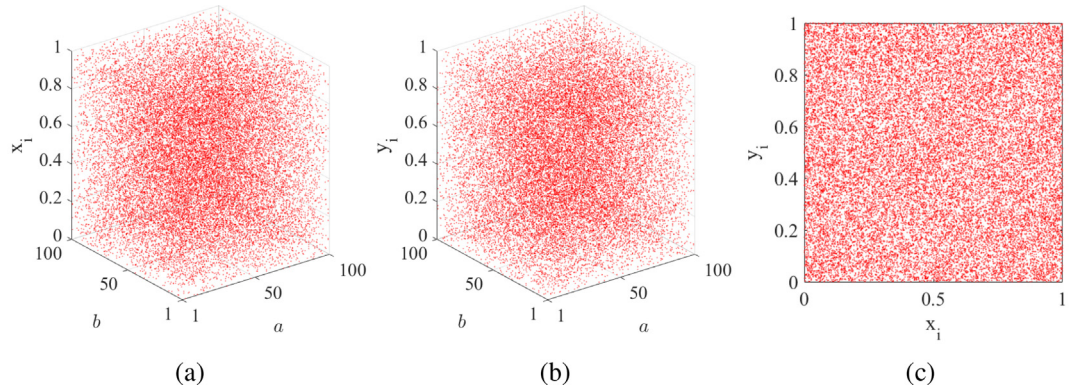

Fig. 4. Bifurcation diagrams obtained for 2D-LTMM in terms of (a) variable x and (b) variable y, and (c) its trajectory with parameters $(a, b) = (50, 50)$.

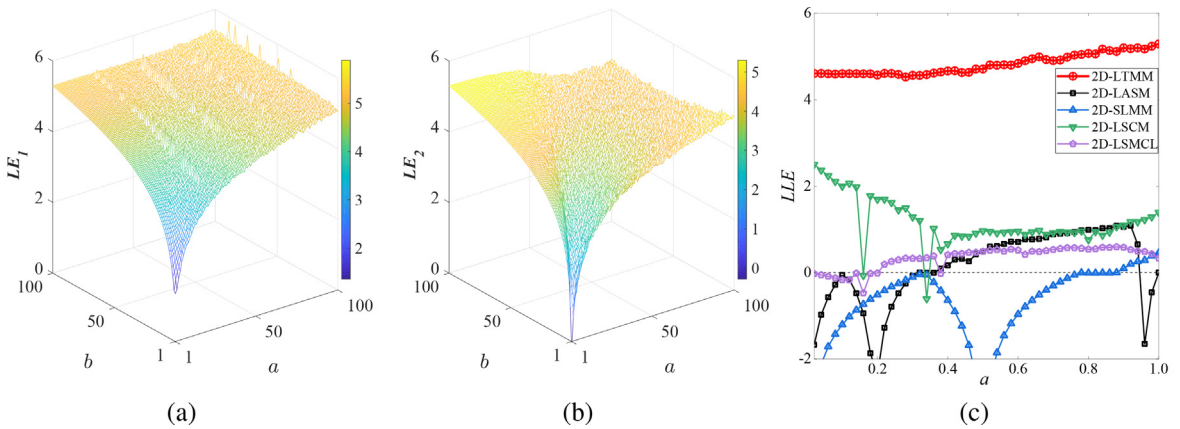

Fig. 5. LEs for different 2D chaotic maps: (a)–(b) the two LEs for 2D-LTMM; (c) a comparison of the LLEs for 2D-LTMM ($a/100$), 2D-LASM, 2D-SLMM, 2D-LSCM, and 2D-LSMCL.

provide a more visual comparison, we set one parameter in the 2D-SLMM, 2D-LTMM, and 2D-LSMCL as a fixed value and compared the LLEs for all the 2D chaotic maps along one parameter; that is, we set parameter b in the 2D-SLMM, 2D-LTMM, and 2D-LSMCL as 3, 50, and 3, respectively. As shown in the comparison of the results in Fig. 5(c), only the proposed 2D-LTMM obtains positive LLEs throughout the parameter range; the other four 2D chaotic maps exhibit many periodic windows within the chaotic ranges, thereby indicating that their chaotic ranges are discontinuous. In addition, compared with the other four maps, the 2D-LTMM yields much larger LLEs; this implies that the similar trajectories of the 2D-LTMM diverge rapidly and exhibit more complicated chaotic behaviours.

3.2.3. SE

As a type of approximate entropy, the SE is used to measure the complexity of a time series. The SE for time series $\{y_1, y_2, \cdots, y_n, \cdots\}$ is defined as

$$\mathrm{SE}(m, r, N) = -\log\frac{A}{B}, \tag{5}$$

where m is a given dimension of the time series, r represents a given distance, and A and B represent the numbers of vectors that satisfy $d[Y_{m+1}(i), Y_{m+1}(j)] < r$ and $d[Y_m(i), Y_m(j)] < r$, respectively. The vector $Y_m(i) = \{y_i, y_{i+1}, \ldots, y_{i+m-1}\}$ and distance $d[Y_m(i), Y_m(j)]$ represent the Chebyshev distance between $Y_m(i)$ and $Y_m(j)$. A larger SE indicates the lower regularity of the time series. When the SE is used to measure the regularity of a time series produced by a chaotic map, a larger SE indicates more complex behaviours.

Fig. 6 shows the SEs of the 2D-LTMM and the four competing 2D chaotic maps. To ensure consistency, the control parameters for all 2D chaotic maps in this experiment were set the same as those in the LE experiment. As shown in Fig. 6(a), the 2D-LTMM yields positive SEs within the entire parameter range. Fig. 6(b) shows that the 2D-LTMM yields considerably larger positive SEs than the four other 2D chaotic maps, indicating that the 2D-LTMM can generate a highly complex time series.

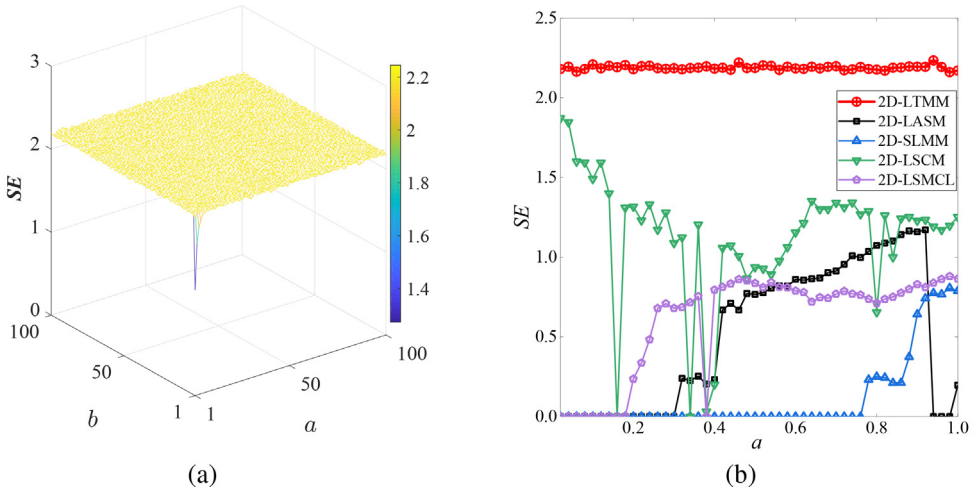

Fig. 6. (a) SEs for 2D-LTMM; (b) a comparison of SEs for 2D-LTMM ($a/100$), 2D-LASM, 2D-SLMM, 2D-LSCM, and 2D-LSMCL.

4. 2D-LTMM-Based CIEA

The 2D-LTMM has a large and continuous chaotic range and demonstrates complex chaotic performance; moreover, its outputs can randomly visit the entire phase plane. With these distinct properties, the 2D-LTMM exhibits a strong image-encryption performance. Using the 2D-LTMM, we construct a new CIEA, referred to as the LTMM-CIEA. The structure of the LTMM-CIEA is illustrated in Fig. 7. The LTMM-CIEA has three components: peripheral-pixel blurring, cross-plane permutation, and non-sequential diffusion. The peripheral-pixel blurring process adds random noise to the two least-significant bits of the peripheral pixels in the red colour plane. The cross-plane permutation method concurrently and randomly shuffles all the pixel positions in the red, green, and blue colour planes. Non-sequential diffusion processes all pixels in the three colour planes, following a random and secret order. The orders of permutation and diffusion are determined by the chaotic sequences, which are generated from the 2D-LTMM using a secret key. To enhance the encryption result, a total of n rounds of cross-plane permutation and non-sequential diffusion are performed for the image. To balance the trade-off between efficiency and security, we set n as two in this study. Users can also set n as a larger integer, to achieve a higher level of security.

4.1. Key schedule

An encryption algorithm must have a large key space to prevent brute-force attacks. The secret key used in our encryption structure has a length of 256 bits, which is sufficiently large to satisfy the security requirements under current computational abilities. The secret key comprises eight components: $K = \{x_1, y_1, a_1, b_1, x_2, y_2, a_2, b_2\}$. (x_i, y_i) $(i = 1, 2)$ denote the initial

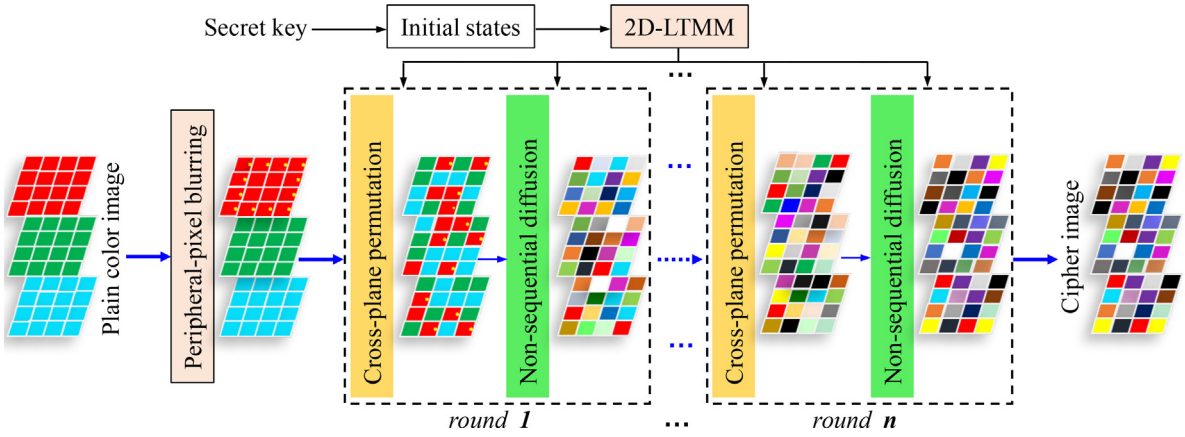

Fig. 7. Structure of LTMM-CIEA.

values of the 2D-LTMM in the two encryption rounds, whereas (a_i, b_i) $(i = 1, 2)$ denote the two control parameters. Each of the eight components has a length of 32 bits. x_i and y_i are float numbers from the range $[0, 1)$, converted from 32-bit streams. Both a_i and b_i contain two parts: the first 7 bits are integers in the range $[0, 128)$, whereas the remaining 25 bits are float numbers in the range $[0, 1)$. When used for the 2D-LTMM, a_i and b_i are added to 1, to ensure that the 2D-LTMM has a consistently strong chaotic performance.

4.2. Peripheral-pixel blurring

To strengthen its ability to defend against various types of security attacks, our encryption structure blurs the peripheral pixels, to insert noise into the plain-colour image before encryption. In particular, noise is added to the two least-significant bits of the peripheral pixels in the red colour plane. This operation only changes a small amount of information in the colour image; as such, it does not affect the visual effect because the peripheral pixels in a natural image typically contain less information than the central ones. In addition, the lower bits of a pixel contain less information than the higher bits.

Fig. 8 illustrates the visual effects of different bit planes for an 8-bit greyscale image. Clearly, the two lowest bit planes contain no visual information for the image and are noise-like, whereas the two highest bit planes contain much more information and can represent the patterns in the image. This is because a '1' in the 8-th bit represents $2^{8-1} = 128$ for an 8-bit greyscale image, whereas it represents $2^{1-1} = 1$ in the 1-st bit. Thus, the information percentage for the i-th bit plane of an 8-bit greyscale image can be calculated as

$$I(i) = \frac{2^{i-1}}{\sum_{i=1}^{8} 2^{i-1}}. \tag{6}$$

Table 2 lists the information percentages calculated for each bit plane in an 8-bit greyscale image. In our algorithm, the peripheral-pixel blurring operation only adds noise to the two least-significant bits of the peripheral pixels in the red colour plane. Thus, the colour image loses the most information when all these blurred bits are changed. If we assume that the 8-bit colour image to be encrypted measures $M \times N \times 3$, then the maximum percentage of information changed can be calculated as

$$I_{\max} = \frac{(I(1) + I(2)) \times (2M + 2N - 4)}{M \times N \times 3}. \tag{7}$$

For example, if a colour image measures $512 \times 512 \times 3$ pixels, then the maximum percentage of information changed is $I_{\max} = 0.00304\%$. Because the blurring operation adds randomly generated noise to the image, it can change approximately half of the original data. Thus, the percentage of information changed is far less than $I_{\max}$. Natural images have a high data redundancy, and blurring occurs in the peripheral pixels in one colour plane; thus, this operation does not affect the visual quality of the image.

The inserted noise is random and differs for each encryption; hence each encryption produces a unique cipher image. Even if the same secret key is used to encrypt the same image twice, the two encrypted results will differ completely, thereby ensuring robust and secure encryption for defending against various attacks (e.g., the chosen-plaintext attack).

4.3. Cross-Plane Permutation

A colour image contains three colour planes: red, green, and blue. Most colour image shuffling algorithms shuffle the pixel positions only within one independent colour plane; they do not consider the relationships between the three colour planes. Some algorithms shuffle the pixel positions row by row or column by column in each colour plane, as shown in Fig. 2(a); this may lead to a low encryption performance and efficiency. To overcome these deficiencies, our encryption structure employs cross-plane permutation, to comprehensively shuffle the pixel positions in the three colour planes via a single operation, as shown in Fig. 3(a). A pixel can be randomly shuffled to any position in the three colour planes. Assuming that a colour image $\mathbf{P}$ measures $M \times N \times 3$ pixels and a chaotic sequence $\mathbf{L}$ of length $M \times N \times 3 + 3(M + N)$ is generated by the 2D-LTMM, the detailed procedure of the cross-plane permutation can be described as follows:

- *Step 1*: Rearrange the chaotic sequence $\mathbf{L}$ as one three-dimensional (3D) chaotic matrix $\mathbf{A}$ and two 2D chaotic matrices $\mathbf{B}$ and $\mathbf{C}$. $\mathbf{A}, \mathbf{B}$, and $\mathbf{C}$ measure $M \times N \times 3, 3 \times M$, and $3 \times N$, respectively.
- *Step 2*: Sort $\mathbf{A}$ by the third dimension and obtain a 3D index matrix $\mathbf{I}$.
- *Step 3*: Sort $\mathbf{B}$ and $\mathbf{C}$ by row and obtain two 2D index matrices $\mathbf{T}$ and $\mathbf{Q}$. Initialise a 3D index matrix $\mathbf{J}$ measuring $M \times N \times 3$, by shifting $\mathbf{Q}$ using each row of $\mathbf{T}$. In particular, $\mathbf{J}(:, :, k)$ is obtained by shifting $\mathbf{Q}(k)$ using the values in the k-th row of $\mathbf{T}$, where $k \in \{1, 2, 3\}$.
- *Step 4*: Use the index matrix $\mathbf{I}$ to shuffle the pixels in the three colour planes of the colour image $\mathbf{P}$, to obtain the result as $\mathbf{P}\prime$.
- *Step 5*: Use the index matrix $\mathbf{J}$ to shuffle all pixels in $\mathbf{P}\prime$, to obtain the permutation result as $\mathbf{S}$.

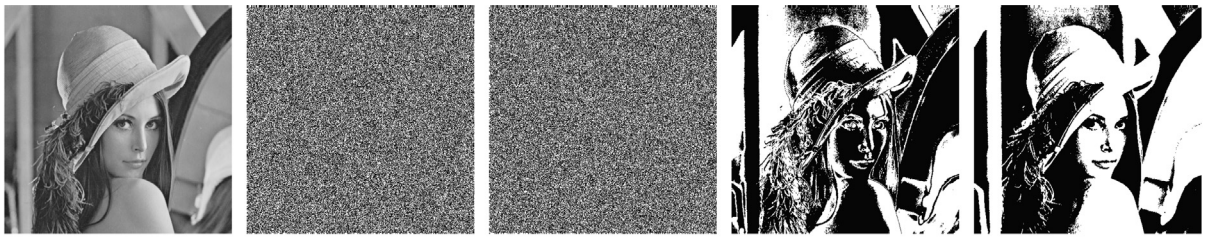

Fig. 8. Information contained in different bit planes of an 8-bit greyscale image: (a) original image; (b) first bit plane; (c) second bit plane; (d) seventh bit plane; (e) eighth bit plane.

Algorithm 1 shows the pseudo-code for the entire cross-plane permutation process. For simplicity, we provide a numeral example to explain its detailed operation for an image measuring $4 \times 4 \times 3$ pixels. Fig. 9 shows the procedure for generating the two index matrices, **I** and **J**. Chaotic matrices **A**, **B**, and **C** are generated using the 2D-LTMM. Index matrix **I** is obtained by sorting the third dimension of **A**, and index matrix **J** is generated by first sorting **B** and **C** by row (to obtain two 2D index matrices) and then shifting one 2D index matrix using the other.

Algorithm 1: Cross-plane permutation procedure for LTMM-CIEA

Output: Colour image $\mathbf{P} \in \mathbb{N}^{M\times N\times 3}$, and chaotic sequence $\mathbf{L} \in \mathbb{R}^{M\times N\times 3+3(M+N)}$.
Divide **L** into one 3D chaotic matrix $\mathbf{A} \in \mathbb{R}^{M\times N\times 3}$ and two 2D chaotic matrices $\mathbf{B} \in \mathbb{R}^{3\times M}$ and $\mathbf{C} \in \mathbb{R}^{3\times N}$;
Sort **A** in the third dimension and obtain the index matrix **I**;
Sort **B** and **C** by row and obtain the index matrices **T** and **Q**, respectively;
for $k = 1$ to 3 **do**
  for $i = 1$ to M **do**
    for $j = 1$ to N **do**
      $\mathbf{P}\prime(i,j,k) = \mathbf{P}(i,j,\mathbf{I}(i,j,k))$;
      $m = ((j - \mathbf{T}(k)_i - 1) \bmod N) + 1$;
      $\mathbf{J}(i,m,k) = \mathbf{Q}(k)_j$;
    end for
  end for
end for
for $k = 1$ to 3 **do**
  for $j = 1$ to N **do**
    for $i = 1$ to M **do**
      $r = i,\ c = \mathbf{J}(i,j,k)$;
      $m = ((r - \mathbf{J}(1,j,k) - 1) \bmod M) + 1,\ n = \mathbf{J}(m,j,k)$;
      $\mathbf{S}(m,n,k) = \mathbf{P}\prime(r,c,k)$;
    end for
  end for
end for
Output: The permutation result **S**.

The cross-plane permutation is performed using two index matrices **I** and **J**; Fig. 10 shows the permutation process. The complete permutation process comprises two steps: the first step shuffles the pixels within the three colour planes, using **I** to obtain $\mathbf{P}\prime$; then, the second step permutes the pixels in each colour plane, using **J**. The detailed processes of these two steps are shown in Figs. 10(a) and (b), respectively. As shown in Fig. 10(a), for the three colour planes $k = \{1,2,3\}$, the pixels in the $\mathbf{I}(:,:,k)$-th colour plane are permuted to the k-th colour plane; that is, $\mathbf{P}\prime(:,:,k) = \mathbf{P}(:,:,\mathbf{I}(:,:,k))$. The peripheral pixels in the red plane of **P** are underlined because their two least-significant bits have been blurred. As shown in Fig. 10(b), 2D index matrix $\mathbf{J}(:,:,1)$ is used to shuffle the pixels of the first colour plane. The shuffling procedure can be described as follows:

- For the 1-st column of $\mathbf{J}(:,:,1)$ (i.e., $\{1,2,4,3\}^T$), select the pixels in the first colour plane with positions $(1,1),(2,2),(3,4)$, and $(4,3)$ (i.e., pixels $B1, R6, B12$, and $G15$ marked as stars, respectively); shift them upwards by $\mathbf{J}(1,1,1) = 1$ cell. Thus, we find that $\mathbf{S}(1,1,1) = R6, \mathbf{S}(2,2,1) = B12, \mathbf{S}(3,4,1) = G15$, and $\mathbf{S}(4,3,1) = B1$.
- For the 2-nd column of $\mathbf{J}(:,:,1)$ (i.e., $\{3,1,2,4\}^T$), select the pixels in the first colour plane with positions $(1,3),(2,1),(3,2)$, and $(4,4)$ (i.e., pixels $G3, B5, B10$, and $B16$ marked as triangles, respectively); shift them upwards by $\mathbf{J}(1,2,1) = 3$ cells. Thus, $\mathbf{S}(1,3,1) = B16, \mathbf{S}(2,1,1) = G3, \mathbf{S}(3,2,1) = B5$, and $\mathbf{S}(4,4,1) = B10$.

Table 2
Information percentage in different bit planes of an 8-bit greyscale image.

Bit plane	Information percentage (%)
1	0.39
2	0.78
3	1.57
4	3.14
5	6.27
6	12.55
7	25.10
8	50.20

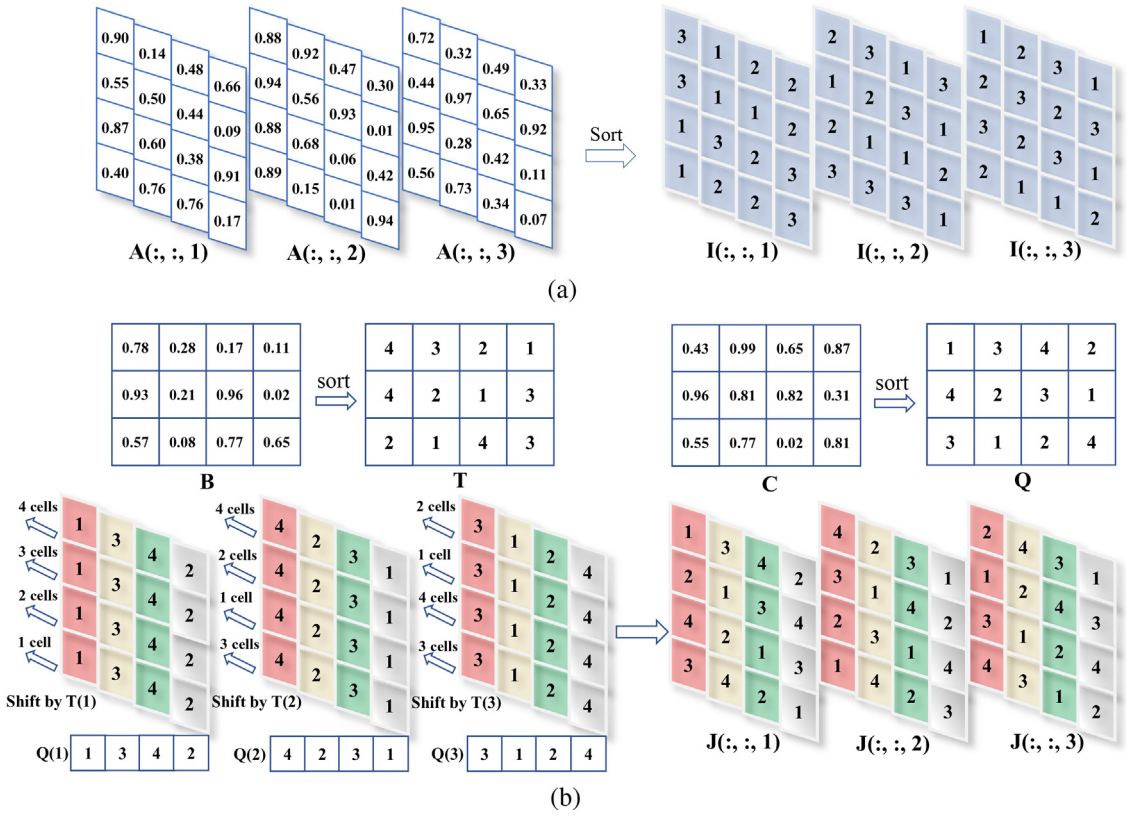

Fig. 9. Numerical example of the process used to generate index matrices: (a) **I** and (b) **J**.

- For the 3-rd column of $\mathbf{J}(:,:,1)$ (i.e., $\{4,3,1,2\}^T$), select the pixels in the first colour plane with positions $(1,4),(2,3),(3,1)$, and $(4,2)$ (i.e., pixels $G4, R7, R9$, and $G14$ marked as circles, respectively); shift them upwards by $\mathbf{J}(1,3,1)=4$ cells. Thus, $\mathbf{S}(1,4,1)=G4, \mathbf{S}(2,3,1)=R7, \mathbf{S}(3,1,1)=R9$, and $\mathbf{S}(4,2,1)=G14$.
- For the 4-th column of $\mathbf{J}(:,:,1)$ (i.e., $\{2,4,3,1\}^T$), select the pixels in the first colour plane with positions $(1,2),(2,4),(3,3)$, and $(4,1)$ (i.e., pixels $R2, G8, G11$, and $R13$ marked as squares, respectively); shift them upwards by $\mathbf{J}(1,4,1)=2$ cells. Thus, $\mathbf{S}(1,2,1)=G11, \mathbf{S}(2,4,1)=R13, \mathbf{S}(3,3,1)=R2$, and $\mathbf{S}(4,1,1)=G8$.

Similarly, shuffle the second and third colour planes of $\mathbf{P}\prime$ using the index matrices $\mathbf{J}(:,:,2)$ and $\mathbf{J}(:,:,3)$, respectively. After the pixels of all colour planes have been shuffled, we obtain the cross-plane permutation result as **S**.

Many existing permutation algorithms change only the pixel positions within one colour plane. Let the size of the colour image to be encrypted be $M \times N \times 3$ pixels. In existing algorithms, the probability of a permuted position for each pixel is $M \times N$. However, for the proposed permutation algorithm, this probability is $M \times N \times 3$, three times that of the existing algorithms. Thus, the cross-plane permutation process achieves high efficiency and performance. The decryption of cross-plane permutation is the reverse process of the forward operation.

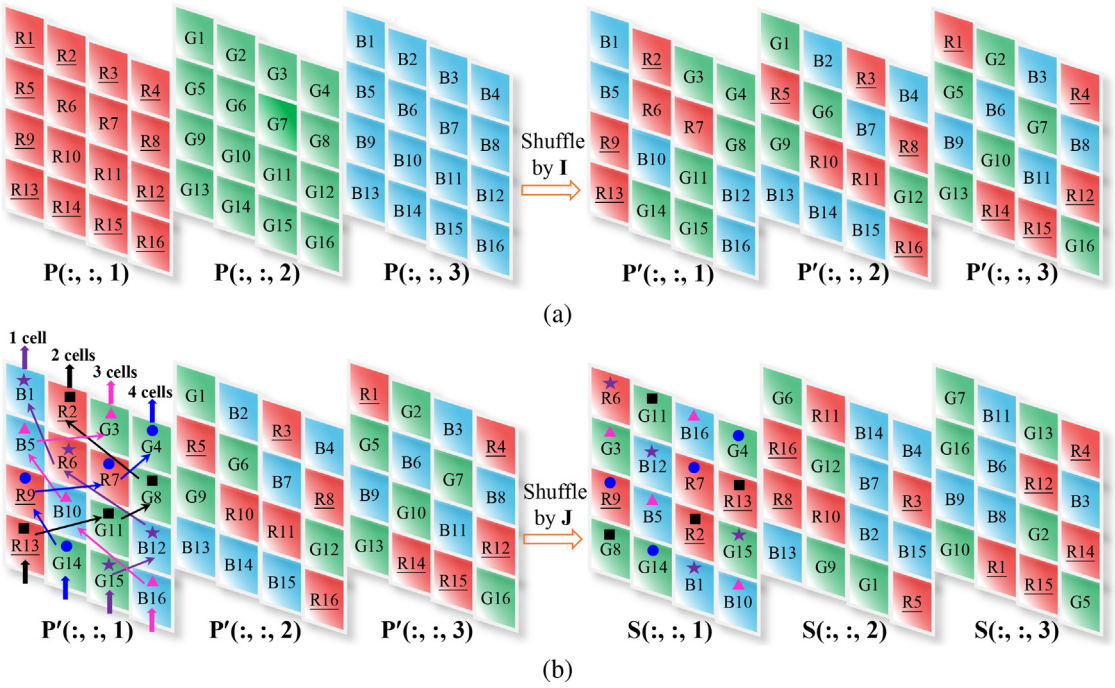

Fig. 10. Numerical example of cross-plane permutation for colour image **P** using index matrices **I** and **J**: (a) colour plane shuffling using **I** and (b) pixel position shuffling using **J**.

4.4. Non-sequential diffusion

An encryption algorithm must have a diffusion property. Most image encryption algorithms achieve diffusion by changing the current pixel using the previous pixel(s) according to some fixed order, as shown in Fig. 2(b). However, processing image pixels in a fixed order can result in a low encryption performance and provide attackers with large amounts of useful information with which to conduct cryptanalysis. To overcome this problem, our encryption structure employs non-sequential diffusion, using a random and secret visit mechanism to process pixels. Fig. 11 schematically illustrates this non-sequential diffusion process. The processing order is not fixed because it is determined by a chaotic sequence generated using the 2D-LTMM. Thus, a pixel may be affected by any pixel from the three colour planes. First, the chaotic matrix **A** is generated using the same approach employed in the cross-plane permutation process. The non-sequential diffusion process operates as

$$\mathbf{C}_{i,j,k} = \begin{cases} (\mathbf{S}_{i,j,k} + \mathbf{S}_{M,N,3} + \mathbf{A}_{i,j,k}) \bmod F & \text{if } i = 1, j = 1, k = 1, \\ (\mathbf{S}_{i,j,k} + \mathbf{C}_{M,N,k-1} + \mathbf{A}_{i,j,k}) \bmod F & \text{if } i = 1, j = 1, k \neq 1, \\ (\mathbf{S}_{i,j,k} + \mathbf{C}_{M,j-1,k} + \mathbf{A}_{i,j,k}) \bmod F & \text{if } i = 1, j \neq 1, \\ (\mathbf{S}_{i,j,k} + \mathbf{C}_{i-1,j,k} + \mathbf{A}_{i,j,k}) \bmod F & \text{if } i \neq 1, \end{cases} \tag{8}$$

where *mod* denotes the arithmetic modular operation, and F represents the number of pixel values in each colour image **P** (e.g., $F = 256$, where a pixel in **P** is represented by 8 bits).

Decryption is the reverse process of encryption; thus, the inverse operation for non-sequential diffusion is described as

$$\mathbf{S}_{i,j,k} = \begin{cases} (\mathbf{C}_{i,j,k} - \mathbf{S}_{M,N,3} - \mathbf{A}_{i,j,k}) \bmod F & \text{if } i = 1, j = 1, k = 1, \\ (\mathbf{C}_{i,j,k} - \mathbf{C}_{M,N,k-1} - \mathbf{A}_{i,j,k}) \bmod F & \text{if } i = 1, j = 1, k \neq 1, \\ (\mathbf{C}_{i,j,k} - \mathbf{C}_{M,j-1,k} - \mathbf{A}_{i,j,k}) \bmod F & \text{if } i = 1, j \neq 1, \\ (\mathbf{C}_{i,j,k} - \mathbf{C}_{i-1,j,k} - \mathbf{A}_{i,j,k}) \bmod F & \text{if } i \neq 1. \end{cases} \tag{9}$$

The non-sequential diffusion can spread changes from one pixel to all the pixels after it. For a colour image measuring $M \times N \times 3$ pixels, if the L-th ($L \leqslant M \times N \times 3$) pixel is changed, the number of changed pixel after one round of non-sequential diffusion is

$$R = \frac{M \times N \times 3 - L}{M \times N \times 3}. \tag{10}$$

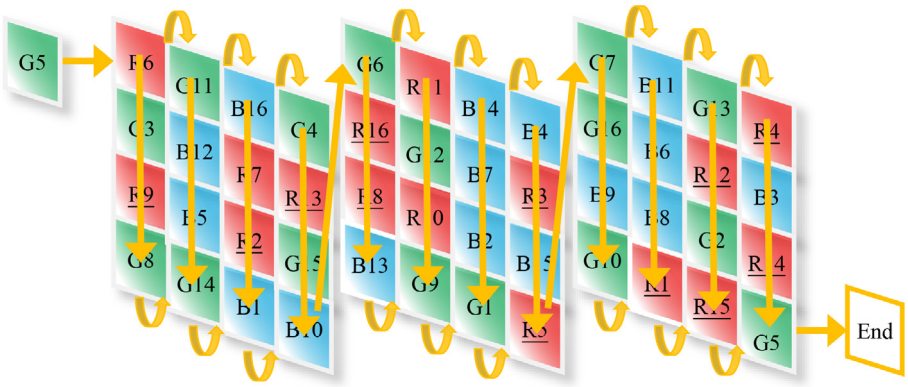

Fig. 11. Schematic illustration of the non-sequential diffusion process.

Thus, at least two rounds of diffusion are required to achieve good diffusion. Therefore, we set the number of encryption rounds n in Fig. 7 as two. Because the peripheral-pixel blurring adds different amounts of noise to the plain image during each encryption, the proposed LTMM-CIEA achieves good diffusion by combining the operation of peripheral-pixel blurring with non-sequential diffusion.

4.5. Discussion

As described, noise is inserted into the peripheral pixels, and the cross-plane permutation and non-sequential diffusion concurrently process pixels in the three colour planes of the colour image; thus, the proposed LTMM-CIEA exhibits an extremely good chaotic performance and offers the following advantages:

(1) The LTMM-CIEA can realise good confusion and diffusion properties; this is because the encryption structure strictly follows the principles of confusion and diffusion, and the cross-plane permutation and non-sequential diffusion processes can concurrently confuse and diffuse the three colour planes, respectively.
(2) The LTMM-CIEA is highly capable of resisting many popular and efficient security attacks, including chosen-plaintext, statistic, and differential attacks. This is because the encryption algorithm adds different amounts of noise to the plain images during each encryption operation, and this noise can be spread throughout the cipher image. Thus, even if we use the same secure key to encrypt an image multiple times, the cipher images differ completely from each other, thereby rendering numerous security attacks ineffective.
(3) The encryption/decryption speed of the LTMM-CIEA is rapid because the chaotic maps and encryption structures it employs have simple implementations and low computational costs.
(4) The LTMM-CIEA has a high capacity to mitigate data losses and noise. If the cipher image is blurred with noise, or some data is lost, the original image can still be reconstructed with high visual quality.

These advantages are verified by the simulation results and security analyses presented in Sections 5 and 6.

5. Simulation results and efficiency analysis

In this section, we evaluate the encryption efficiency of the LTMM-CIEA via simulation experiments. The experiments were performed using MATLAB software; most of the images employed were obtained from the USC-SIPI[1] and CVG-UGR[2] image databases.

5.1. Simulation Results

To adapt to various application scenarios, an image encryption algorithm must be able to encrypt different types of images into unrecognisable cipher images, such that the original image can be completely recovered only by using the correct secret key. It must be impossible to obtain any useful information regarding the original image without the correct secret key. Fig. 12 simulates the encryption and decryption processes in the LTMM-CIEA, using different colour images as test images. These test images were all natural images containing numerous patterns, as shown by their pixel histograms. Significant amount of information can be deduced about the images by analysing their histograms. However, the LTMM-

[1] http://sipi.usc.edu/database/
[2] http://decsai.ugr.es/cvg/dbimagenes/

CIEA can encrypt them into unrecognisable images with uniform-distribution pixel histograms such that no information can be retrieved. The LTMM-CIEA can reconstruct the complete original images with the same visual effects by using the correct key. Fig. 13 presents three-dimensional histograms for the original and corresponding encrypted images. This simplistically demonstrates that all pixels in the red, green, and blue colour planes are distributed uniformly in the encrypted images, thereby indicating that the LTMM-CIEA can encrypt a natural image as a cipher image with high performance.

5.2. Efficiency analysis

An image encryption algorithm must be highly efficient to satisfy the rapid increase in image data capacities. Our proposed LTMM-CIEA exhibits rapid encryption speeds for the following three reasons: (1) the 2D-LTMM has high chaotic performance and low implementation costs; (2) cross-plane permutation can completely shuffle all pixels in the three colour planes via a single operation, and non-sequential diffusion can process all pixels using a random and secret visit mechanism; and (3) two rounds of permutation and diffusion achieve high security.

To demonstrate the efficiency of our proposed LTMM-CIEA, we compare its performance with several state-of-the-art encryption algorithms. All the experiments were simulated on a computer operating the following environment: Intel(R)

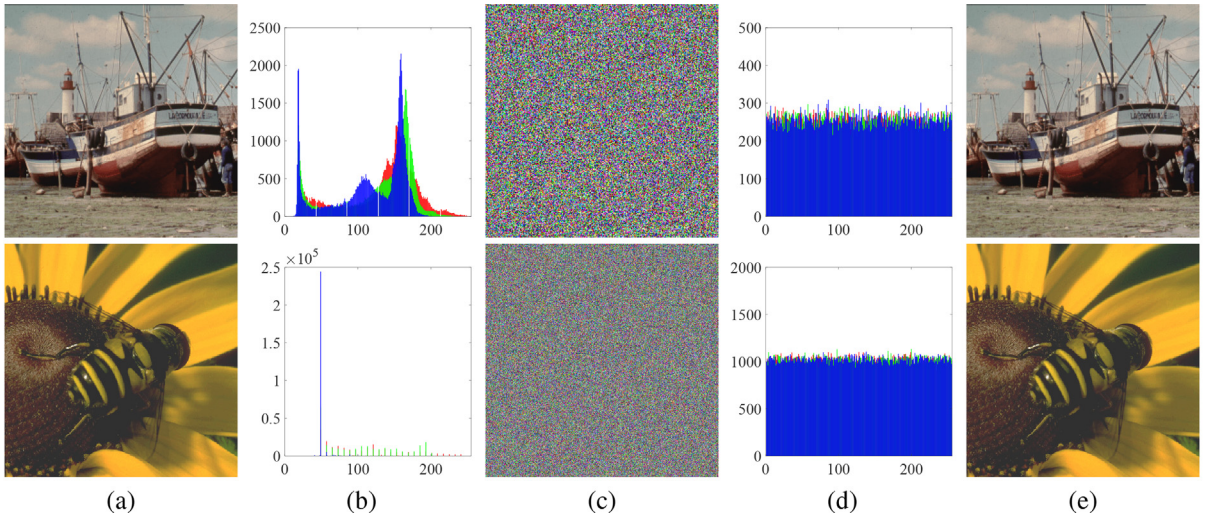

Fig. 12. Simulation results obtained using the LTMM-CIEA for colour images: (a) plain images; (b) histograms for (a); (c) encrypted results for (a); (d) histograms for (c); (e) decrypted results for (c).

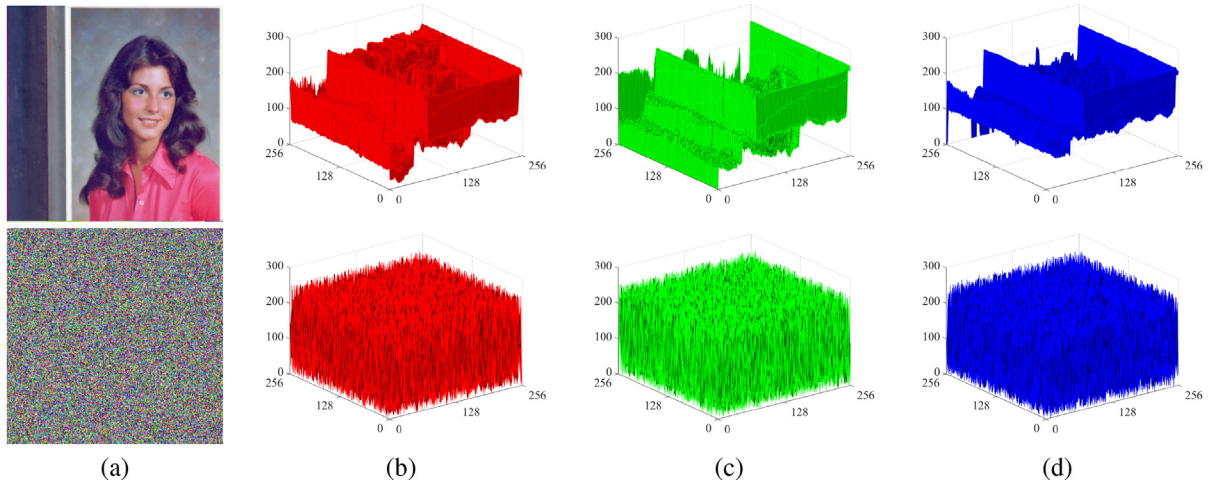

Fig. 13. Three-dimensional visualisation of the plain image and its cipher image obtained using LTMM-CIEA: (a) plain image and cipher image; (b) red colour plane; (c) green colour plane; (d) blue colour plane.

Table 3
Average encryption times, (*s*), for different image encryption algorithms on colour images of different sizes.

Colour image size	LTMM-CIEA	Ref. [10]	Ref. [7]	Ref. [2]	Ref. [47]
$128 \times 128 \times 3$	**0.0309**	0.0577	0.1034	0.5221	0.4919
$256 \times 256 \times 3$	**0.1253**	0.2483	0.4274	2.2636	2.2786
$512 \times 512 \times 3$	**0.5101**	1.1386	2.1782	8.4003	8.4127
$1024 \times 1024 \times 3$	**2.3802**	4.8970	10.3231	34.3617	34.5904

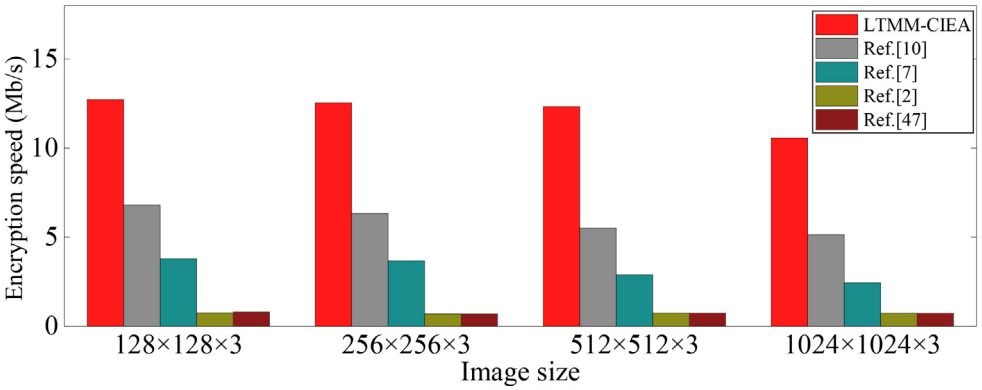

Fig. 14. Encryption speeds for different image encryption algorithms on colour images of different sizes.

Core(TM) i5-8265U central processing unit running at 1.60 GHz, 8 GB random-access memory, and a Windows 10 operating system. Table 3 lists the encryption times for various image encryption algorithms using colour images of different sizes. The results were obtained by calculating the average encryption time of 100 experiments. Our proposed LTMM-CIEA requires the shortest encryption time. Fig. 14 also shows the encryption speeds for the encryption algorithms using colour images of different sizes. The encryption speed of our proposed LTMM-CIEA is the fastest and can exceed 10 Mb/s for an image measuring $1024 \times 1024 \times 3$ pixels. These results indicate that the proposed LTMM-CIEA significantly outperforms the other encryption algorithms.

6. Security analysis

The security level of the encrypted images is the most important performance indicator for an encryption algorithm. Thus, we evaluate the security of the LTMM-CIEA in terms of the key sensitivity, capacity for defending against different security attacks, and information entropy.

6.1. Key sensitivity

An encryption algorithm must be extremely sensitive to its secret key; otherwise, the actual key space will be smaller than the theoretical one. A high key sensitivity indicates that a small change in the secret key during the encryption/decryption processes will yield two completely different encrypted/decrypted results. To measure the sensitivity of the secret keys, we randomly produce a secret key K_1 and then obtain two more secret keys K_2 and K_3, by changing one bit in K_1. K_1, K_2, and K_3 are expressed as

$$K_1 = 4D820EA9F9F780BC11A3CF6E04F01638AB60217F34C1398CD5F16123A0BA0DF1,$$
$$K_2 = 4D821EA9F9F780BC11A3CF6E04F01638AB60217F34C1398CD5F16123A0BA0DF1,$$
$$K_3 = 4D820EA9F9F780BC11A3CF6E04F01638AB60217F34C1399CD5F16123A0BA0DF1.$$

Fig. 15 illustrates the secret key sensitivity analysis results obtained during the encryption process of the LTMM-CIEA. The top row shows the plain colour image, two cipher images encrypted using K_1 and K_2, and the difference between these two cipher images; the bottom row shows the histograms for the images in the top row. Fig. 15(d) shows that the two cipher images are completely different. Fig. 16 presents the experimental results for the key sensitivity during the decryption process. Only the correct key can accurately recover the original image. Two secret keys that differ by only one bit obtain unrecognisable decryption results; thus, the two decrypted results differ completely, as shown in Fig. 16(e). Therefore, the secret key in LTMM-CIEA is highly sensitive.

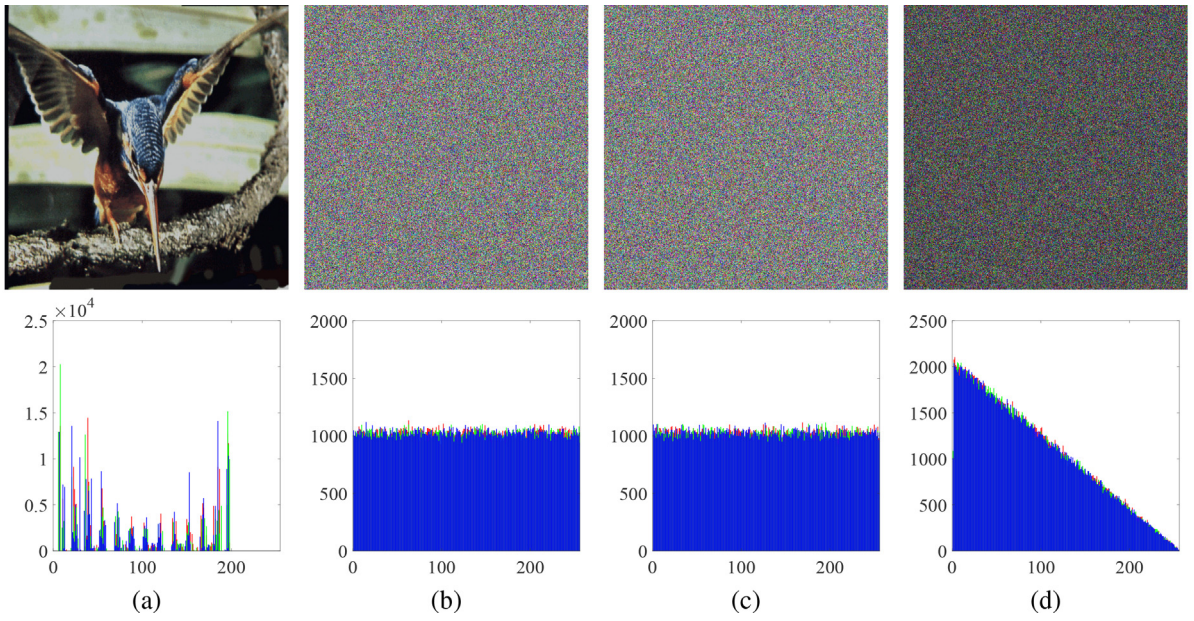

Fig. 15. Key sensitivity analysis in the encryption process: (a) plain colour image $\mathbf{P}$; (b) cipher image $\mathbf{C}_1 = Enc(\mathbf{P}, K_1)$; (c) cipher image $\mathbf{C}_2 = Enc(\mathbf{P}, K_2)$; (d) difference between $\mathbf{C}_1$ and $\mathbf{C}_2, |\mathbf{C}_1 - \mathbf{C}_2|$.

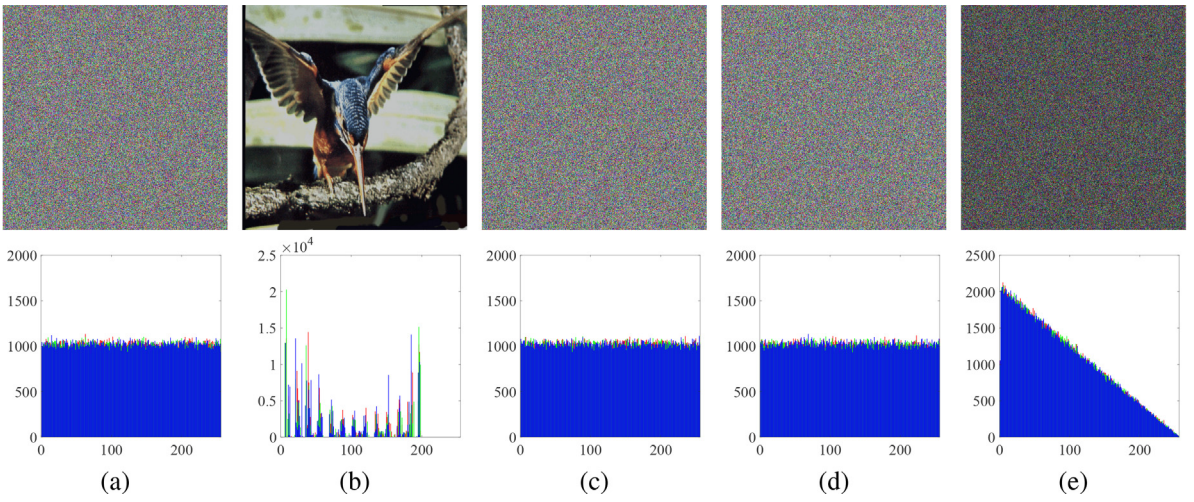

Fig. 16. Key sensitivity analysis during the decryption process: (a) cipher image $\mathbf{C}_1$; (b) decrypted result $\mathbf{D}_1 = Dec(\mathbf{C}_1, K_1)$; (c) decrypted result $\mathbf{D}_2 = Dec(\mathbf{C}_1, K_2)$; (d) decrypted result $\mathbf{D}_3 = Dec(\mathbf{C}_1, K_3)$; (e) difference between $\mathbf{D}_2$ and $\mathbf{D}_3, |\mathbf{D}_2 - \mathbf{D}_3|$.

6.2. Chosen-plaintext attack

The chosen-plaintext attack is an efficient and commonly used cryptanalysis technique. Our proposed LTMM-CIEA can defend against the chosen-plaintext attack owing to its following two properties. (1) The blurring of peripheral-pixel adds randomly generated noise to each encryption. This noise is different in every encryption operation and can affect all pixels in the encrypted results. (2) The diffusion property of the encryption algorithm allows it to disseminate any difference in the plain image to all pixels in the cipher image.

Fig. 17 illustrates the ability of the LTMM-CIEA to resist the chosen-plaintext attack. Two encrypted results are obtained by encrypting one image twice with the same secret key, and the difference between the two encrypted results is calculated. Fig. 17(d) shows that the two encrypted results differ completely; this is because randomly generated noise is added to the two least-significant bits of the peripheral pixels in the red colour plane, and this noise affects all the pixels in the encrypted results. This indicates that the encrypted result depends not only on the plain image and secret key but also the added noise.

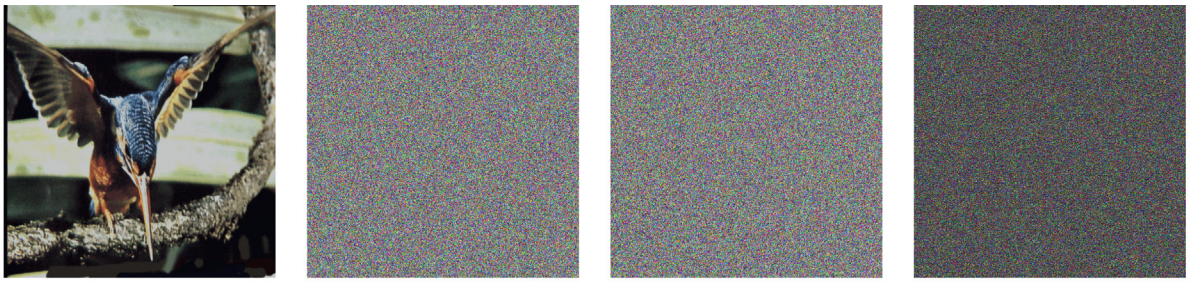

Fig. 17. Capacity of the LTMM-CIEA to resist the chosen-plaintext attack: (a) plain colour image $\mathbf{P}$; (b) first encrypted image $\mathbf{C}_{11} = Enc(\mathbf{P}, K_1)$; (c) second encrypted image $\mathbf{C}_{12} = Enc(\mathbf{P}, K_1)$; (d) difference between $\mathbf{C}_{11}$ and $\mathbf{C}_{12}$, $|\mathbf{C}_{11} - \mathbf{C}_{12}|$.

Thus, an attacker cannot determine the internal relationships between the plaintext and ciphertext by choosing some plaintext to encrypt. Therefore, the LTMM-CIEA is highly capable of resisting the chosen-plaintext attack.

6.3. Capacity to mitigate data losses and noise

When images are stored on physical devices or transmitted through any type of transmission channel, they can lose some data or be blurred by noise. Thus, a reliable image encryption algorithm should be able to recover most of the image information when the cipher images suffer such data losses or blurring. Therefore, we tested the capacity of our proposed LTMM-CIEA to mitigate data losses and noise. In particular, five processed cipher images were generated using the following five techniques: (1) data cutting with a size of 100×100 in the red colour plane; (2) data cutting with a size of 200×200 in the red colour plane; (3) data cutting with a size of 200×200 in all three colour planes; (4) adding 5% salt & pepper noise; and (5) adding 10% salt & pepper noise. Finally, we decrypted the five processed cipher images using the correct secret key.

Fig. 18 shows the simulation results. Either a considerable amount of data is lost from the cipher image or excessive noise is added to it; however, the LTMM-CIEA can still reconstruct the original image with a clear visual effect, because its encryption and decryption processes are asymmetrical. During encryption, a slight change will be spread over all pixels to produce completely dissimilar encrypted results, thereby ensuring that the cipher images are highly secure. However, during decryption, a slight change can only affect a few pixels, ensuring that the LTMM-CIEA can effectively mitigate data losses and noise.

6.4. Capacity to resist differential attacks

Differential attacks are another effective and commonly used cryptanalysis technique. However, our proposed LTMM-CIEA can effectively resist differential attacks owing to the following properties. (1) The peripheral-pixel blurring adds noise

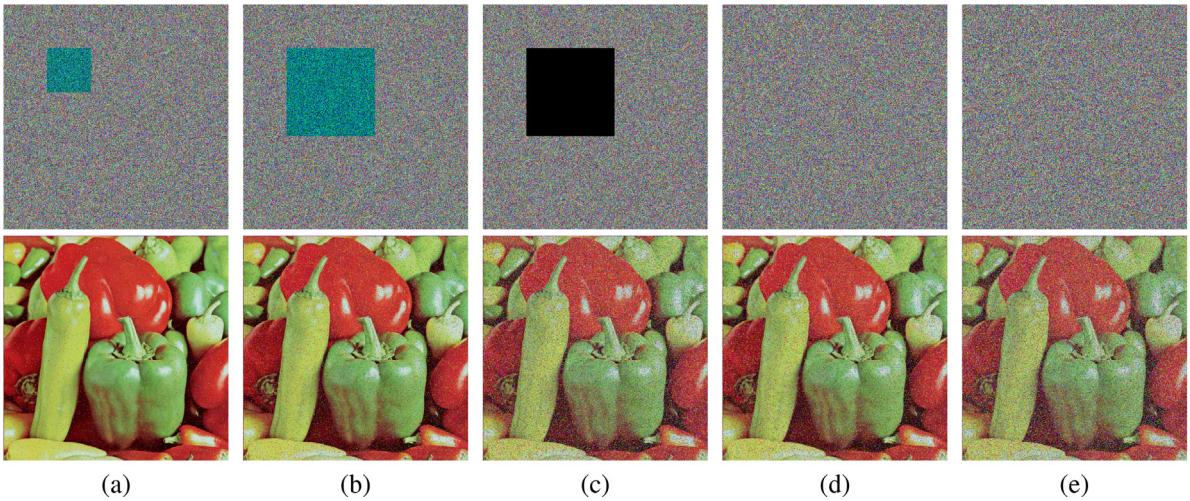

Fig. 18. Capacity of LTMM-CIEA to mitigate data losses and noise. The first row shows the cipher images with different types of data losses and noise; the second row presents the corresponding decrypted images: (a) 100×100 data losses in the red colour plane; (b) 200×200 data losses in the red colour plane; (c) 200×200 data losses in all three colour planes; (d) 5% salt & pepper noise; (e) 10% salt & pepper noise.

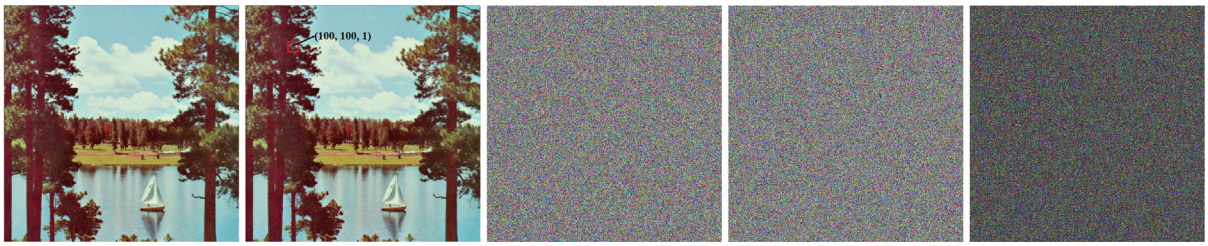

Fig. 19. Capacity of LTMM-CIEA to resist differential attacks: (a) plain colour image $\mathbf{P}_1$; (b) plain colour image $\mathbf{P}_2$ with a one-bit difference compared with $\mathbf{P}_1$ at position $(100, 100, 1)$; (c) encrypted image $\mathbf{C}_1 = Enc(\mathbf{P}_1, K_1)$; (d) encrypted image $\mathbf{C}_2 = Enc(\mathbf{P}_2, K_1)$; (e) difference between $\mathbf{C}_1$ and $\mathbf{C}_2$, $|\mathbf{C}_1 - \mathbf{C}_2|$.

to the peripheral pixels in the red colour plane, and this noise is spread over all pixels after two rounds of encryption. (2) The diffusion property allows a small difference in the plain image to be spread over all the pixels. Fig. 19 depicts the capacity of the LTMM-CIEA to resist differential attacks. First, a plain image $\mathbf{P}_2$ is generated from $\mathbf{P}_1$ by changing one bit at position $(100, 100, 1)$. Then, we encrypt $\mathbf{P}_1$ and $\mathbf{P}_2$ using the same secret key and calculate the difference between the two encrypted results. As shown in Fig. 19(d), these two results are completely different.

The capacity to resist differential attacks is quantitatively tested using the number of pixels change rate (NPCR) and the unified averaged changed intensity (UACI) [43]. Assuming that $\mathbf{C}_1$ and $\mathbf{C}_2$ are two cipher images encrypted from two plain images with a one-bit difference, their NPCR and UACI values are calculated as

$$NPCR(\mathbf{C}_1, \mathbf{C}_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\mathbf{W}(i,j)}{H} \times 100\%, \tag{11}$$

and

$$UACI(\mathbf{C}_1, \mathbf{C}_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|\mathbf{C}_1(i,j) - \mathbf{C}_2(i,j)|}{H \times Q} \times 100\%, \tag{12}$$

respectively; here, $[M, N]$ represents the size of one colour plane in the image, H is the total number of pixels in one colour plane, Q is the maximum pixel value, and $\mathbf{W}$ indicates the difference between $\mathbf{C}_1$ and $\mathbf{C}_2$. If $\mathbf{C}_1(i,j) = \mathbf{C}_2(i,j), \mathbf{W}(i,j) = 0$; otherwise, $\mathbf{W}(i,j) = 1$.

Wu et al. proposed strict criteria for the NPCR and UACI tests [43]. For an ideal encryption algorithm, the NPCR values should exceed a certain threshold and the UACI values should be within an appropriate interval. The threshold score $\mathcal{N}^*_\alpha$ for the NPCR test is obtained as

$$\mathcal{N}^*_\alpha = \frac{Q - \Phi^{-1}(\alpha)\sqrt{Q/H}}{Q+1}, \tag{13}$$

where α is the significance level. An encryption algorithm passes the NPCR test if its NPCR score exceeds $\mathcal{N}^*_\alpha$. The interval of $(\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha)$ for the UACI test can be calculated as

$$\begin{cases} \mathcal{U}^{*-}_\alpha = \mu_\mathcal{U} - \Phi^{-1}(\alpha/2)\sigma_\mathcal{U}; \\ \mathcal{U}^{*+}_\alpha = \mu_\mathcal{U} + \Phi^{-1}(\alpha/2)\sigma_\mathcal{U}, \end{cases} \tag{14}$$

$$\mu_\mathcal{U} = \frac{Q+2}{3Q+3}, \tag{15}$$

$$\sigma^2_\mathcal{U} = \frac{(Q+2)(Q^2+2Q+3)}{18(Q+1)^2QH}. \tag{16}$$

An encryption algorithm passes the UACI test if the UACI score obtained is within the range $(\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha)$.

Following the settings given in [43], the significance level α is set as 0.5 in our experiments; the criteria for different sizes of images are as follows: for an image size of $128 \times 128, \mathcal{N}^*_\alpha = 99.5292\%$ and $(\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha) = (33.1012\%, 33.8259\%)$; for an image size of $256 \times 256, \mathcal{N}^*_\alpha = 99.5693\%$ and $(\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha) = (33.2824\%, 33.6447\%)$; for an image size of $512 \times 512, \mathcal{N}^*_\alpha = 99.5893\%$ and $(\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha) = (33.3730\%, 33.5541\%)$; and for an image size of $1024 \times 1024, \mathcal{N}^*_\alpha = 99.5994\%$ and $(\mathcal{U}^{*-}_\alpha, \mathcal{U}^{*+}_\alpha) = (33.4183\%, 33.5088\%)$. Twelve colour images with different sizes were selected as the test images. The test results in Table 4 show that all test images pass the stringent tests, thereby indicating that our proposed LTMM-CIEA can effectively resist differential attacks.

Table 4
NPCR and UACI scores using LTMM-CIEA on colour images of different sizes. The significance level is $\alpha = 0.5$.

Image size	File name	NPCR (%)				UACI (%)				Test results
		Red	Green	Blue	Average	Red	Green	Blue	Average	
$128 \times 128 \times 3$	Carafe	99.6033	99.5789	99.6033	99.5952	33.3278	33.3176	33.5501	33.3985	pass
	Paper	99.5972	99.5850	99.6094	99.5972	33.4494	33.2025	33.4449	33.3656	pass
	Reno	99.6155	99.6033	99.6216	99.6135	33.6433	33.5536	33.3895	33.5288	pass
$256 \times 256 \times 3$	4.1.01	99.6078	99.6353	99.6017	99.6149	33.3850	33.5726	33.4345	33.4640	pass
	4.1.02	99.6140	99.6170	99.6063	99.6124	33.4441	33.5206	33.4097	33.4581	pass
	4.1.03	99.6124	99.6078	99.6078	99.6093	33.3506	33.4780	33.4458	33.4248	pass
$512 \times 512 \times 3$	4.2.05	99.6147	99.6120	99.6059	99.6109	33.4448	33.4412	33.4531	33.4464	pass
	4.2.06	99.6143	99.6029	99.6105	99.6092	33.4913	33.3867	33.3973	33.4251	pass
	4.2.07	99.6086	99.6044	99.6132	99.6087	33.4998	33.4788	33.4892	33.4893	pass
$1024 \times 1024 \times 3$	2.2.20	99.6066	99.6172	99.6181	99.6140	33.4378	33.4828	33.4358	33.4521	pass
	2.2.21	99.6076	99.6029	99.6190	99.6098	33.4733	33.4460	33.4798	33.4664	pass
	2.2.22	99.6011	99.6012	99.6143	99.6055	33.4282	33.4741	33.4982	33.4668	pass

Table 5
Comparison of different image encryption algorithms in terms of their NPCR and UACI scores. The test image used was *Lena*.

Encryption algorithm	NPCR (%)				UACI (%)			
	Red	Green	Blue	Average	Red	Green	Blue	Average
LTMM-CIEA	**99.6479**	**99.6597**	**99.6288**	**99.6455**	**33.4390**	**33.4799**	**33.4833**	**33.4674**
Ref. [28]	99.6296	99.6174	99.6473	99.6314	33.6027	33.4997	33.5516	33.5513
Ref. [13]	99.6188	99.6376	99.6003	99.6189	33.4285	33.4549	33.4275	33.4399
Ref. [12]	99.5643	99.6258	99.6285	99.6062	35.4560	33.2199	33.0184	33.8981
Ref. [16]	99.6323	99.6277	99.5712	99.6104	33.4913	33.3786	33.4692	33.4464
Ref. [42]	99.6052	99.6060	99.6113	99.6075	33.4280	33.4966	33.3779	33.4342
Ref. [7]	99.6151	99.6304	99.5903	99.6119	33.4371	33.5273	33.4781	33.4808
Ref. [10]	99.6040	99.6017	99.5972	99.6010	33.5465	33.5035	33.4625	33.5042
Ref. [47]	99.6929	99.7032	99.5049	99.6337	33.3596	33.5811	33.3844	33.4417

Table 5 presents a comparison of different image encryption algorithms in terms of their NPCR and UACI scores. The *Lena* image (measuring $512 \times 512 \times 3$ pixels) was used as the test image. For all encryption algorithms that pass the NPCR and UACI tests, a larger NPCR score and a UACI score closer to the centre of the UACI criterion interval (i.e., 33.4636%) indicate a stronger resistance to differential attacks [43]. The proposed LTMM-CIEA obtains the largest average NPCR score for the three colour planes. In addition, the average UACI obtained by the LTMM-CIEA is closest to the centre of the criterion interval (i.e., 33.4636%).

6.5. Information entropy

Information entropy is used to measure the distribution of a signal. In this study, we use the information entropy to test the randomness and distribution of the pixels in an image. For an image, **I**, the information entropy of its pixels is calculated as

$$H(\mathbf{I}) = -\sum_{i=1}^{F} Pr(x_i)\log_2 Pr(x_i), \tag{17}$$

where F indicates the number of pixel values, x_i denotes the i-th possible value, and $Pr(x_i)$ represents the probability of x_i. A higher information entropy value indicates that the image pixels are distributed more uniformly. When each possible pixel value has the same probability, the image achieves the theoretical maximum information entropy; expressed otherwise, the theoretical maximum information entropy is achieved when $Pr(x_i) = 1/F$ and $H(\mathbf{I})_{\max} = \log_2 F$. For an 8-bit image, this is $H(\mathbf{I})_{\max} = \log_2 2^8 = 8$.

In this experiment, we use the same 12 test images employed in the NPCR and UACI experiments. Table 6 lists the information entropies for the test images and these same images after encryption via the LTMM-CIEA. All the original images achieve relatively low entropies because they contain patterns and non-uniform pixel distributions. However, all the information entropies for the encrypted images are reasonably close to 8. Thus, the pixel values for these encrypted images are distributed highly uniformly, and no information can be obtained from their pixel distributions.

We also compare the information entropies for images encrypted using different image encryption algorithms; Table 7 presents the results obtained. The images encrypted by the proposed LTMM-CIEA have higher average information entropy values compared with those encrypted using other image encryption algorithms, thereby demonstrating the superior performance of the LTMM-CIEA.

Table 6
Information entropies for different-sized original images and those images after encryption using the LTMM-CIEA.

Image size	File name	Original images			Encrypted images		
		Red	Green	Blue	Red	Green	Blue
$128 \times 128 \times 3$	Carafe	3.8892	4.0716	4.2305	7.9894	7.9883	7.9887
	Paper	2.8532	2.9931	2.8678	7.9876	7.9887	7.9890
	Reno	4.3386	4.3803	4.4938	7.9869	7.9899	7.9883
$256 \times 256 \times 3$	4.1.01	6.4200	6.4457	6.3807	7.9974	7.9969	7.9983
	4.1.02	6.2499	5.9642	5.9309	7.9972	7.9976	7.9979
	4.1.03	5.7150	5.3738	5.7117	7.9968	7.9975	7.9973
$512 \times 512 \times 3$	4.2.05	6.7178	6.7990	6.2138	7.9993	7.9993	7.9993
	4.2.06	7.3124	7.6429	7.2136	7.9994	7.9993	7.9994
	4.2.07	7.3388	7.4963	7.0583	7.9993	7.9993	7.9994
$1024 \times 1024 \times 3$	2.2.20	6.8206	6.6007	5.6627	7.9998	7.9998	7.9998
	2.2.21	7.3256	6.6329	5.2769	7.9998	7.9998	7.9998
	2.2.22	7.1293	6.1215	4.6020	7.9998	7.9998	7.9998

Table 7
Information entropies for cipher images encrypted using different image encryption algorithms. The test image used was *Lena*.

Encryption algorithm	Encrypted image			Average of Encrypted images
	Red	Green	Blue	
LTMM-CIEA	**7.9994**	**7.9993**	**7.9994**	**7.99937**
Ref. [28]	7.9994	7.9993	7.9993	7.99933
Ref. [13]	7.9912	7.9914	7.9915	7.99137
Ref. [12]	7.9278	7.9744	7.9705	7.95757
Ref. [16]	7.9992	7.9993	7.9994	7.99930
Ref. [42]	7.9895	7.9894	7.9894	7.98943
Ref. [7]	7.9993	7.9993	7.9993	7.99930
Ref. [10]	7.9993	7.9992	7.9993	7.99927
Ref. [47]	7.9992	7.9994	7.9993	7.99930

7. Conclusions

Chaotic systems are widely used for image encryption. In this study, we reviewed the existing chaos-based image encryption algorithms and found that they have shortcomings in terms of the chaotic systems and encryption structures. To overcome these, we proposed a 2D chaotic map called the 2D-LTMM. The 2D-LTMM is based on the classical logistic and tent maps. Performance evaluations and discussions showed that the 2D-LTMM has a fairly wide and continuous chaotic range and uniformly distributed trajectories. Thus, the 2D-LTMM can achieve better image encryption than the existing chaotic maps. Using the introduced 2D-LTMM, we further designed a CIEA, referred to as the LTMM-CIEA. The LTMM-CIEA includes three processes: peripheral-pixel blurring, cross-plane permutation, and non-sequential diffusion. The peripheral-pixel blurring adds noise to the peripheral pixels in the red colour plane. The cross-plane permutation concurrently permutes all pixels in the three colour planes to different positions. Non-sequential diffusion processes these pixels according to a random and secret order, thereby significantly enhancing the security level of the encrypted results. Simulation experiments demonstrated that the LTMM-CIEA can encrypt different colour images into unrecognisable ones, and its encryption speed was faster than those of several state-of-the-art image encryption algorithms. Security evaluations demonstrated that the LTMM-CIEA can effectively resist various security attacks, and it outperformed several other image encryption algorithms. In future research, because our proposed LTMM-CIEA exhibits high efficiency with a strong security level, we will investigate its application to other media data, including super-resolution images and video.

CRediT authorship contribution statement

Zhongyun Hua: Conceptualization, Supervision, Project administration, Writing - original draft, Funding acquisition. **Zhihua Zhu:** Methodology, Software, Data curation, Validation, Investigation, Writing - original draft. **Shuang Yi:** Visualization, Funding acquisition. **Zheng Zhang:** Formal analysis, Funding acquisition. **Hejiao Huang:** Resources, Writing - review & editing.

Declaration of Competing Interest

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

Acknowledgements

This work was supported in part by the National Key R&D Program of China under Grant 2018YFB1003805, Natural Scientific Research Innovation Foundation in Harbin Institute of Technology under Grant HIT.NSRIF.2020077, National Natural Science Foundation of China under Grants 61701137, 62071142, 62002301 and 62002085, Natural Science Foundation of Chongqing under Grant cstc2019jcyj-msxmX0393, and Education Committee Foundation of Chongqing under Grant KJQN201900305, and Guangdong Basic and Applied Basic Research Foundation No. 2019A1515110475.

References

[1] A. Akhavan, A. Samsudin, A. Akhshani, Hash function based on piecewise nonlinear chaotic map, Chaos, Solitons Fractals 42 (2009) 1046–1053.
[2] X. Chai, Y. Chen, L. Broyde, A novel chaos-based image encryption algorithm using dna sequence operations, Opt. Lasers Eng. 88 (2017) 197–213.
[3] H. Chen, Z. Liu, L. Zhu, C. Tanougast, W. Blondel, Asymmetric color cryptosystem using chaotic Ushiki map and equal modulus decomposition in fractional Fourier transform domains, Opt. Lasers Eng. 112 (2019) 7–15.
[4] C. Fu, B.B. Lin, Y.S. Miao, X. Liu, J.J. Chen, A novel chaos-based bit-level permutation scheme for digital image encryption, Opt. Commun. 284 (2011) 5415–5423.
[5] H.M. Ghadirli, A. Nodehi, R. Enayatifar, An overview of encryption algorithms in color images, Signal Processing 164 (2019) 163–185.
[6] C. Han, Y. Shen, W. Ma, Iteration and superposition encryption scheme for image sequences based on multi-dimensional keys, Opt. Commun. 405 (2017) 101–106.
[7] Z. Hua, F. Jin, B. Xu, H. Huang, 2D Logistic-Sine-coupling map for image encryption, Signal Processing 149 (2018) 148–161.
[8] Z. Hua, B. Xu, F. Jin, H. Huang, Image encryption using josephus problem and filtering diffusion, IEEE Access 7 (2019) 8660–8674.
[9] Z. Hua, Y. Zhou, Image encryption using 2D Logistic-adjusted-Sine map, Inf. Sci. 339 (2016) 237–253.
[10] Z. Hua, Y. Zhou, C.M. Pun, C.L.P. Chen, 2D Sine Logistic modulation map for image encryption, Inf. Sci. 297 (2015) 80–94.
[11] C.K. Huang, H.H. Nien, Multi chaotic systems based pixel shuffle for image encryption, Opt. Commun. 282 (2009) 2123–2127.
[12] A. Kadir, A. Hamdulla, W.Q. Guo, Color image encryption using skew tent map and hyper chaotic system of 6th-order cnn, Optik-Int. J. Light Electron Opt. 125 (2014) 1671–1675.
[13] M. Kumar, G. Sathish, M. Alphonse, R.A.M. Lahcen, A new RGB image encryption using generalized heat equation associated with generalized Vigenere-type table over symmetric group, Multimedia Tools Appl. 78 (2019) 28025–28061.
[14] J.A. Lazzús, M. Rivera, C.H. López-Caraballo, Parameter estimation of lorenz chaotic system using a hybrid swarm intelligence algorithm, Phys. Lett. A 380 (2016) 1164–1171.
[15] C. Li, B. Feng, S. Li, J. Kurths, G. Chen, Dynamic analysis of digital chaotic maps via state-mapping networks, IEEE Trans. Circuits Syst. I Regul. Pap. 66 (2019) 2322–2335.
[16] S. Li, W. Ding, B. Yin, T. Zhang, Y. Ma, A novel delay linear coupling logistics map model for color image encryption, Entropy 20 (2018) 463.
[17] Y. Li, C. Wang, H. Chen, A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation, Opt. Lasers Eng. 90 (2017) 238–246.
[18] H. Liu, A. Kadir, Asymmetric color image encryption scheme using 2D discrete-time map, Signal Processing 113 (2015) 104–112.
[19] L. Liu, Q. Zhang, X. Wei, A RGB image encryption algorithm based on DNA encoding and chaos map, Computers Electr. Eng. 38 (2012) 1240–1248.
[20] M. Liu, S. Zhang, Z. Fan, S. Zheng, W. Sheng, Exponential H_∞) synchronization and state estimation for chaotic systems via a unified model, IEEE Trans. Neural Networks Learn. Syst. 24 (2013) 1114–1126.
[21] P. Liu, T. Zhang, X. Li, A new color image encryption algorithm based on DNA and spatial chaotic map, Multimedia Tools Appl. 78 (2019) 14823–14835.
[22] W. Liu, K. Sun, C. Zhu, A fast image encryption algorithm based on chaotic map, Opt. Lasers Eng. 84 (2016) 26–36.
[23] V.A. Memos, K.E. Psannis, Y. Ishibashi, B.G. Kim, B.B. Gupta, An efficient algorithm for media-based surveillance system (EAMSuS) in IoT smart city framework, Future Generation Computer Syst. 83 (2018) 619–628.
[24] M. Mollaeefar, A. Sharif, M. Nazari, A novel encryption scheme for colored image based on high level chaotic maps, Multimedia Tools Appl. 76 (2017) 607–629.
[25] A.Y. Niyat, M.H. Moattar, M.N. Torshiz, Color image encryption based on hybrid hyper-chaotic system and cellular automata, Opt. Lasers Eng. 90 (2017) 225–237.
[26] C. Pak, L. Huang, A new color image encryption using combination of the 1D chaotic map, Signal Processing 138 (2017) 129–137.
[27] K.A.K. Patro, B. Acharya, Secure multi–level permutation operation based multiple colour image encryption, J. Inform. Security Appl. 40 (2018) 111–133.
[28] K.A.K. Patro, B. Acharya, An efficient colour image encryption scheme based on 1-D chaotic maps, J. Inform. Security Appl. 46 (2019) 23–41.
[29] K.E. Psannis, C. Stergiou, B.B. Gupta, Advanced media-based smart big data on intelligent cloud systems, IEEE Trans. Sustainable Computing 4 (2018) 77–87.
[30] M.L. Sahari, I. Boukemara, A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption, Nonlinear Dyn. 94 (2018) 723–744.
[31] S.M. Seyedzadeh, S. Mirzakuchaki, A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map, Signal Processing 92 (2012) 1202–1215.
[32] W. Song, Y. Zheng, C. Fu, P. Shan, A novel batch image encryption algorithm using parallel computing, Inf. Sci. 518 (2020) 211–224.
[33] S. Stalin, P. Maheshwary, P.K. Shukla, M. Maheshwari, B. Gour, A. Khare, Fast and secure medical image encryption based on non linear 4D logistic map and DNA Sequences, J. Med. Syst. 43 (2019) 267.
[34] C. Stergiou, K.E. Psannis, Efficient and secure big data delivery in cloud computing, Multimedia Tools Appl. 76 (2017) 22803–22822.
[35] C. Stergiou, K.E. Psannis, Recent advances delivered by mobile cloud computing and internet of things for big data applications: a survey, Int. J. Network Manage. 27 (2017) article ID: e1930..
[36] C. Stergiou, K.E. Psannis, B.G. Kim, B. Gupta, Secure integration of iot and cloud computing, Future Generation Computer Syst. 78 (2018) 964–975.
[37] C. Stergiou, K.E. Psannis, A.P. Plageras, Y. Ishibashi, B.G. Kim, Algorithms for efficient digital media transmission over iot and cloud networking, J. Multimedia Inform. Syst. 5 (2018) 1–10.
[38] M. Wan, Z. Lai, G. Yang, Z. Yang, F. Zhang, H. Zheng, Local graph embedding based on maximum margin criterion via fuzzy set, Fuzzy Sets Syst. 318 (2017) 120–131.
[39] M. Wan, M. Li, G. Yang, S. Gai, Z. Jin, Feature extraction using two-dimensional maximum embedding difference, Inf. Sci. 274 (2014) 55–69.
[40] M. Wan, G. Yang, S. Gai, Z. Yang, Two-dimensional discriminant locality preserving projections (2DDLPP) and its application to feature extraction via fuzzy set, Multimedia Tools Appl. 76 (2017) 355–371.
[41] J. Wu, X. Luo, N. Zhou, Four-image encryption method based on spectrum truncation, chaos and the modfrft, Opt. Laser Technol. 45 (2013) 571–577.
[42] X. Wu, J. Kurths, H. Kan, A robust and lossless dna encryption scheme for color images, Multimedia Tools Appl. 77 (2018) 12349–12376.
[43] Y. Wu, J.P. Noonan, S. Agaian, et al, NPCR and UACI randomness tests for image encryption, Cyber journals: multidisciplinary journals in science and technology, J. Selected Areas Telecommunications (JSAT) 1 (2011) 31–38.
[44] Y. Zhang, The fast image encryption algorithm based on lifting scheme and chaos, Inf. Sci. 520 (2020) 177–194.

[45] Z. Zhang, Z. Lai, Z. Huang, W.K. Wong, G.S. Xie, L. Liu, L. Shao, Scalable supervised asymmetric hashing with semantic and latent factor embedding, IEEE Trans. Image Process. 28 (2019) 4803–4818.
[46] N. Zhou, H. Li, D. Wang, S. Pan, Z. Zhou, Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform, Opt. Commun. 343 (2015) 10–21.
[47] Y. Zhou, L. Bao, C.P. Chen, A new 1D chaotic system for image encryption, Signal Processing 97 (2014) 172–182.
[48] H. Zhu, Y. Zhao, Y. Song, 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption, IEEE Access 7 (2019) 14081–14098.
[49] Z.L. Zhu, W. Zhang, K.W. Wong, H. Yu, A chaos-based symmetric image encryption scheme using a bit-level permutation, Inform. Sci. 181 (2011) 1171–1186.