Signal Processing 171 (2020) 107457

Contents lists available at ScienceDirect

Signal Processing

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

Designing a 2D infinite collapse map for image encryption

Weijia Cao [a,b], Yujun Mao [b], Yicong Zhou [b,*]

[a] Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing, China
[b] Department of Computer and Information Science, University of Macau, Macau, China

ARTICLE INFO

Article history:
Received 23 August 2019
Revised 17 December 2019
Accepted 5 January 2020
Available online 11 January 2020

Keywords:
2D infinite collapse map
confusion and diffusion
Image encryption

ABSTRACT

Due to the unpredictability and complexity properties, chaotic maps are widely applied in security, communication, and system control. Existing one-dimensional (1D) chaotic maps can be easily predicted and high-dimensional (HD) ones have more complex structures and higher computation costs. In order to enhance the chaotic performance, this paper proposes a new two-dimensional infinite collapse map (2D-ICM). Compared with existing 2D chaotic maps, 2D-ICM has better ergodicity, hyperchaotic property, unpredictability, and a wider chaotic region. To investigate its application, we further propose an image encryption algorithm using 2D-ICM. Simulation demonstrates that the proposed image encryption algorithm has excellent performance for protecting various kinds of images.

1. Introduction

With the rapid improvement of network communication and multimedia techniques, an increasing number of digital images are stored, copied, and transmitted over various types of third-party platforms or unsecured channels. Since these images often carry private or sensitive information, image security has received increasing attention recently [1–3]. To ensure security of digital images, many image encryption algorithms have been developed including data stream encryption [4,5], multimedia scrambling [6], wave perturbation [7], reversible cellular automata [8], bitplane-based image encryption [9,10], and chaos-based image encryption algorithms [11–13]. Among these algorithms, the chaos-based image encryption methods have become a compelling way for image encryption because of the attractive properties of chaotic maps such as ergodic, complexity, and sensitivity [14–17]. They also show good secure performance and low computation costs [18–20].

In fact, the security of chaos-based image encryption approaches is heavily dependent on the chaos performance of their chaotic maps. Existing chaotic maps can be divided into two categories: one-dimensional (1D) and high-dimensional (HD) chaotic maps. For 1D chaotic maps, they possess simple trajectories and few variables, and thus their initial conditions and orbits can be easily deduced [21,22]. Moreover, the chaos performance of a chaotic map will be decreased or vanished when its parameter was in some intervals [23,24]. To cope with this problem, several HD chaotic maps with hyper-chaotic property were designed [23–26]. the simulation results show that these existing HD chaotic maps fail to pass some security tests for image encryption [25]. They also have more complex structures and higher computation costs with expensive hardware implementation. Some HD chaotic maps appear non-chaotic or low-chaotic performance in specific specific intervals [23,24,27]. Therefore, it becomes meaningful to design a chaotic map that has unpredictable and robust chaotic performance with a low computation cost.

In this paper, we propose a two-dimensional (2D) hyper-chaotic map, called 2D infinite collapse map (2D-ICM). 2D-ICM is constructed using two 1D infinite collapse maps with the modulation operation. Performance evaluation and comparison are carried out using the trajectory distribution, Lyapunov exponent, correlation dimension, and Kolmogorov entropy. The results show that 2D-ICM has more unpredictable characteristics, better ergodicity, and a larger chaotic range than several state-of-the-art 2D chaotic maps. Owing to these excellent hyper-chaotic properties of 2D-ICM, we also propose a 2D-ICM based image encryption algorithm (ICMIE). Applying the chaotic sequences generated by 2D-ICM, ICMIE performs the confusion and diffusion operations to encrypt images. Simulation results and security analysis show that ICMIE can efficiently encrypt various types of images with a high level of security.

The rest of this paper is organized as follows. Section 2 proposes 2D-ICM and evaluates its chaotic performance. Section 3 introduces ICMIE and gives experimental results of different kinds of images. Section 4 analyzes security of ICMIE. Section 5 reaches a conclusion.

* Corresponding author.
E-mail address: yicongzhou@um.edu.mo (Y. Zhou).

https://doi.org/10.1016/j.sigpro.2020.107457
0165-1684/

2. 2D infinite collapse map

This section introduces the 2D infinite collapse map (2D-ICM) and investigates its chaotic behaviors.

2.1. Mathematical definition

An infinite collapse map is a 1D chaotic map that has the best chaotic performance among existing 1D chaotic maps [28]. Its mathematical definition is given by

$$x_{n+1} = \sin\left(\frac{a}{x_n}\right), \tag{1}$$

where x_n and x_{n+1} are its input and output, and the control parameter $a \neq 0$.

A traditional 1D chaotic map usually has a simple structure and its trajectory is easy to be predicted using some estimation technologies [19]. To tackle with this problem, we propose a 2D infinite collapse map (2D-ICM) by integrating two 1D infinite collapse maps with different parameters, which is defined by

$$\begin{cases} x_{n+1} = \sin\left(\frac{a}{y_n}\right) \cdot \sin\left(\frac{b}{x_n}\right), \\ y_{n+1} = \sin\left(\frac{a}{x_n}\right) \cdot \sin\left(\frac{b}{y_n}\right), \end{cases} \tag{2}$$

where the control parameters a and b are real numbers, $a \neq 0$, $b \neq 0$. From the definition of 2D-ICM, we can see that the magnitude of an original infinite collapse map $sin\ (a/x)$ is modulated by another infinite collapse map $sin\ (b/y)$ with different parameters.

2.2. Performance evaluation

To evaluate chaotic behaviors of 2D-ICM, we adopt several measures including the attractor, Lyapunov exponent, correlation dimension, and Kolmogorov entropy in this section. Moreover, the proposed 2D-ICM is compared with five existing 2D chaotic maps, i.e. 2D Logistic map (2D-Logistic) [29], 2D Sine Logistic modulation map (2D-SLMM) [25], 2D Logistic-adjusted-Sine map (2D-LASM) [26], 2D Sine modulation map (2D-SIMM) [23], and 2D Logistic cascade map (2D-LICM) [24]. Here we simplify the definitions of these maps and select their parameters for their best chaotic performance. Their simplified definitions are shown as follows.

For 2D logistic map, it contains only one parameter λ, simply replacing it by a, then the definition can be rewritten as Eq. (3) [29],

$$\begin{cases} x_{n+1} = a(3y_i + 1)x_i(1 - x_i), \\ y_{n+1} = a(3x_{i+1} + 1)y_i(1 - y_i). \end{cases} \tag{3}$$

For 2D-SLMM, the best chaotic performance appears at $\beta = 3$, after replacing the other parameter α by a, the definition is rewritten as Eq. (4) [25],

$$\begin{cases} x_{n+1} = a((\sin(\pi y_i) + 3)x_i(1 - x_i), \\ y_{n+1} = a((\sin(\pi x_{i+1}) + 3)y_i(1 - y_i). \end{cases} \tag{4}$$

For 2D-LASM, it contains only one parameter μ, simply replacing it by a, then the definition can be rewritten as Eq. (5) [26],

$$\begin{cases} x_{n+1} = \sin(\pi a(y_i + 3)x_i(1 - x_i)), \\ y_{n+1} = \sin(\pi a(x_{i+1} + 3)y_i(1 - y_i)). \end{cases} \tag{5}$$

For 2D-SIMM, the best chaotic performance appears at $b = 5$ and the other parameter is a, the definition can be rewritten as Eq. (6) [23],

$$\begin{cases} x_{n+1} = a\sin(\pi y_i)sin(5/x_i), \\ y_{n+1} = a\sin(\pi x_{i+1})sin(5/y_i). \end{cases} \tag{6}$$

For 2D-LICM, the best chaotic performance appears at $a = 0.6$, after replacing the other parameter k by a, the definition can be rewritten as Eq. (7) [24],

$$\begin{cases} x_{n+1} = \sin(21/(0.6(y_i + 3)ax_i(1 - ax_i))), \\ y_{n+1} = \sin(21/(0.6(ax_{i+1} + 3)ax_i(1 - y_i))). \end{cases} \tag{7}$$

2.2.1. Attractor

The attractor of a chaotic map is a set of numerical values toward which the map tends to evolve under a large variety of initial points. For a 2D chaotic map, its attractor can be described by a group of points that occupy a region in a 2D phase space. A chaotic map with better chaotic performance usually has an attractor that is geometrically complicated and occupies a large region in the phase space. To visually demonstrate the attractors of these chaotic maps mentioned above, we choose (0.6, 0.3) as the initial point and iterate 40000 times for each map respectively. These 40000 generated points of each map are then plotted in the 2D space to represent the attractor of each map. Fig. 1 compares the attractors of 2D-ICM with five 2D chaotic maps.

As can be seen in Fig. 1(f), the attractor of 2D-ICM fully occupies a 2D phase space ranging $(-1, 1)$. This means that 2D-ICM can produce more unpredictable results and has the better or competitive ergodicity property than these existing maps.

2.2.2. Lyapunov exponent (LE)

Lyapunov exponent is used to evaluate the chaotic properties of a dynamical system. It is a quantitative measure of the separation rate of two infinitely close trajectories. For a high-order dynamical system, there are more than one Lyapunov exponents and the number of Lyapunov exponents is equal to the order of the system, since different orientations of the initial separation vector will result in different separation rates. The Lyapunov exponent of a dynamical system can be used to determine whether the system is chaotic or not. A system with a positive LE is considered to be chaotic, and a system with more than one positive LE is considered to be hyper-chaotic. A hyperchaotic system will have an unpredictable and good chaotic performance.

In our simulation results, the algorithm in [30] is applied to estimate the LE values. A 2D chaotic map generally has two LE values. If both of its LE values are larger than 0, this map will be considered as a hyper-chaotic map. The LE values of the proposed 2D-ICM are shown in Fig 2.(a). It can be clearly seen that 2D-ICM is hyper-chaotic among the entire parameter range. This means that its trajectory is extremely hard to be deduced. Fig. 2 (b) and (c) show the comparison results between the larger and smaller LE values of various 2D chaotic maps. Since different maps have different parameter ranges. We normalize all the ranges of their parameters into [0, 1]. From the results, we can see that the LE values of the proposed 2D-ICM are the largest one among these competing maps in both comparisons of larger and smaller LE values. This shows its better performance compared to other existing maps. Another important property of 2D-ICM is that its LE values increase as each of the its parameters increases. It means that we can obtain as large LE values as possible by adjusting its parameters.

2.2.3. Correlation dimension (CD)

In chaos theory, the correlation dimension is a type of fractal dimension that measures the dimensionality of the space occupied by a set of random points. It can be used to characterize the attractor strangeness (degrees of freedom) of a dynamic system [30].

Here we use the algorithm in [31] to estimate the CD values. CD is a kind of fractal dimension that describes the shape complexity of an object. It is expected that a 2D object should have a

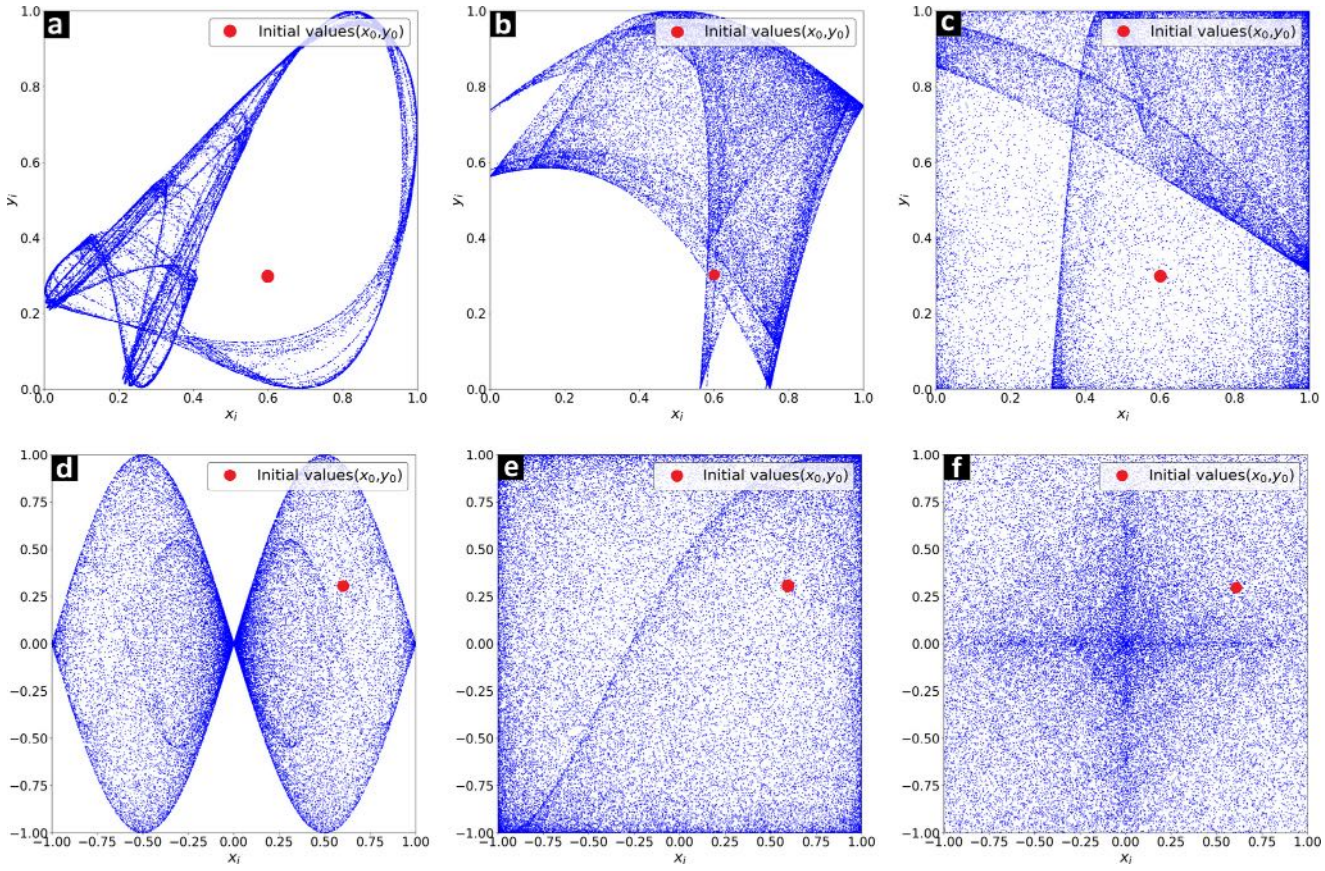

Fig. 1. Attractors of different 2D chaotic maps: (a) 2D-logistic-map; (b) 2D-SLMM; (c) 2D-LASM; (d) 2D-SIMM; (e) 2D-LICM; (f) the proposed 2D-ICM.

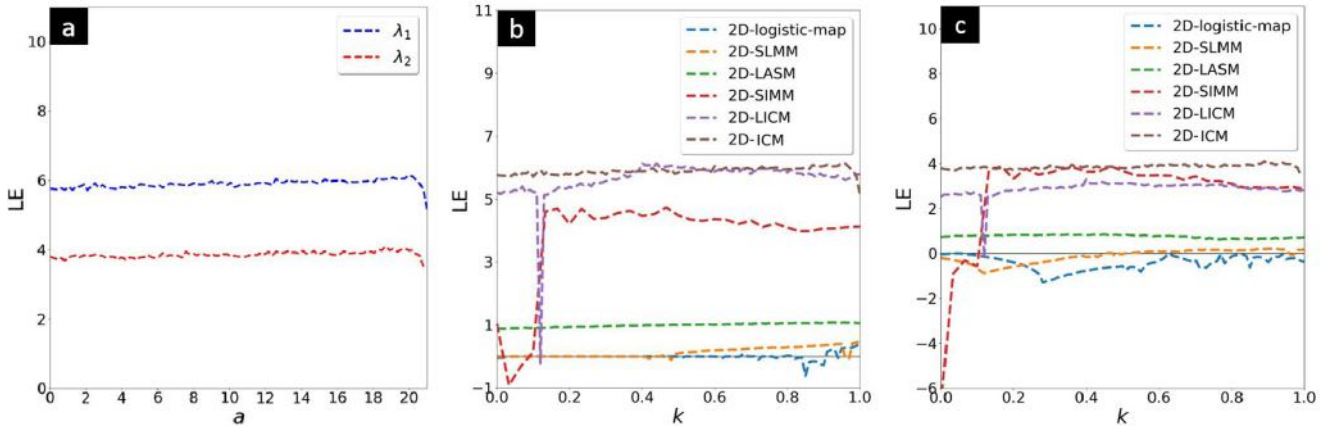

Fig. 2. Lyapunov exponent distributions of different 2D chaotic maps: (a) 2D-ICM ($b = 21$); (b) comparison of larger LE values of various 2D maps; (c) comparison of smaller LE of various 2D maps. In (b) and (c) $k = 5 \times (a - 0.99)$ for 2D-logistic-map, $k = 5 \times (a - 0.8)$ for 2D-SLMM, $k = 5 \times (a - 0.72)$ for 2D-LASM, $k = \frac{10}{3} \times (a - 0.7)$ for 2D-SIMM, $k = (a - 0.6)$ for 2D-LICM and $k = \frac{1}{10} \times (a - 11)$ for 2D-ICM.

CD value around 2. From the estimation results in Fig. 3 (a), we can see 2D-ICM is the only one whose CD values are larger than 2. This means that the attractor of 2D-ICM is extremely complex and may not be fully described under a 2D coordination system even it is a 2D map. The CD simulation results also show that the proposed 2D-ICM has the better chaotic property compared with other 2D chaotic maps.

2.2.4. Kolmogorov entropy (KE)

The Kolmogorov entropy value is to evaluate the extra information needed to predict the trajectories of a dynamic system and a bigger KE value indicates more information is needed. So the larger the KE is, the more chaotic and unpredictable the system is. We use the method in [32] to calculate the KE values of various chaotic maps. The comparison between different maps is shown in Fig. 4(b). 2D-ICM has the largest KE values compared to other existing 2D maps and thus its trajectory is the most difficult to be estimated. The KE simulation results show that the proposed 2D-ICM has the better chaotic property compared with the existing maps.

In summary, the trajectory and trend of 2D-ICM are hard to predict due to its decent ergodicity property. It also demonstrates 2D-ICM has a larger chaotic range, better ergodicity, and more unpredictable chaotic characteristics than these existing 2D chaotic maps

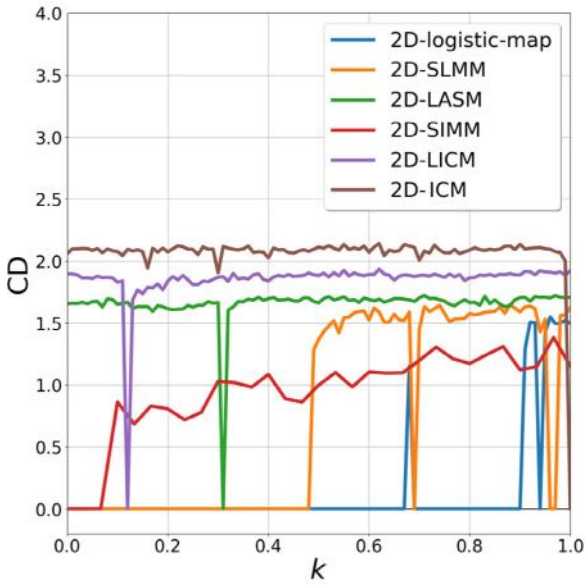

Fig. 3. Comparison of correlation dimensions of various 2D maps.

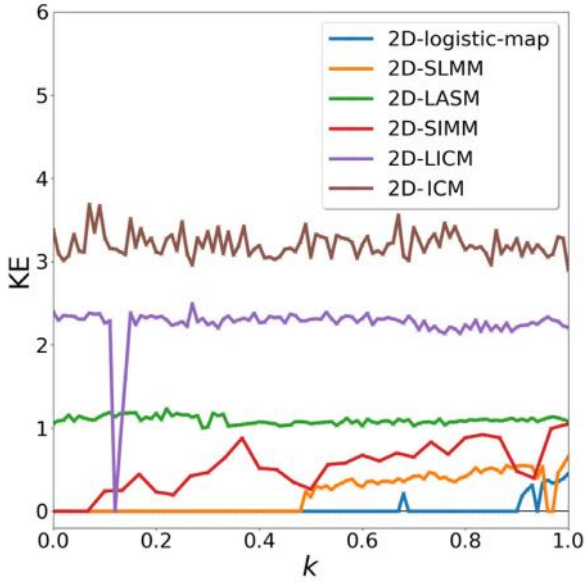

Fig. 4. Comparison of Kolmogorov entropy of various 2D maps.

in terms of the assessment and comparative results of LE, CD, and KE.

3. 2D-ICM based image encryption and decryption algorithm

A 2D-ICM based Image Encryption Algorithm (ICMIE) is proposed in this section. Fig. 5 shows the structure of ICMIE. Using the initial parameters generated by the security key, ICMIE contains two main parts: confusion and diffusion. The confusion part can shuffle the pixel positions of an image effectively while the diffusion part can change the pixel values dramatically. In the diffusion part, ICMIE also can spread the changes from few pixels of the plaintext image to the whole ciphertext image. To balance security and computation efficiency, in this paper, ICMIE uses two rounds of confusion and diffusion processes to obtain image encryption results. The users have flexibility to perform more round to achieve a higher level of security. The decryption process is the reverse of each ICMIE encryption step.

Algorithm 1 The diffusion process of ICMIE

Input: The confusion image F and 2D-chaotic matrices X and Y. They are of size $M \times N$.

1: Rearrange F, X, and Y into 1D matrices F_{1D}, X_{1D}, and Y_{1D}, respectively;
2: sort the X_{1D} with an ascending order and obtain the index matrix x;
3: sort the F_{1D} with x as a matrix A;
4: do the diffusion with the value matrix Y_{1D} by Eq. (10);
5: rearrange D into a 2D matrix E with size of $M \times N$;

Output: the diffusion image E.

3.1. Initial conditions

To withstand the brute-force attack, an image encryption algorithm should have a security key length larger than 100 bits [33]. Here we use a binary string with 240 bits as the security key of the proposed ICMIE. This security key is used to generate the initial conditions of 2D-ICM. It contains 7 parts $\{a, b, x_0, y_0, T, C_1, C_2\}$. They are lengths of 40 bits, 40 bits, 40 bits, 40 bits, 40 bits, 20 bits and 20 bits, respectively.

The first 40-bit binary strings in the security key $\{s_1, s_2, ..., s_{40}\}$ are used to generate decimal numbers a_0, b_0, x, y and T using IEEE 754 format:

$$d = \frac{\sum_{i=1}^{40} s_i 2^{40-i}}{2^{40}}. \tag{8}$$

The last two 20-bit binary strings of the security key are used to generate the integer coefficients C_1 and C_2. The initial condition of 2D-ICM can be calculated as follows,

$$\begin{cases} a = (a_0 + T \times C_1) \bmod 5 + 16, \\ b = (b_0 + T \times C_2) \bmod 5 + 16, \\ x_0 = (x + T \times C_1) \bmod 2 - 1, \\ y_0 = (y + T \times C_2) \bmod 2 - 1. \end{cases} \tag{9}$$

3.2. Confusion process

We propose a new confusion method using two chaotic matrices to randomly scramble the positions of all pixels in a plaintext image. First, 2D-ICM generates two chaotic matrices X and Y. An example is shown in Fig. 6, Matrix S can be obtained by manipulating X and Y into a single matrix $S = X * Y$. Its index matrix I can be deducted by sorting S with an ascending order. The pixel locations of plaintext image P are re-arranged using the index matrix I. After all the pixels are re-arranged into their new locations, the confusion image F is obtained. It can be seen that all pixels of P are scrambled after a round of ICMIE confusion.

Fig. 7 shows an image confusion results by ICMIE and the confused image F is noise-like and unrecognized. As ICMIE confusion process only changes the positions of image pixels, the histogram of F is same as the P.

3.3. Diffusion process

The chosen-plaintext attack is designed to break a cryptosystem via investigating how a tiny change in plaintexts affects the encryption results of the cryptosystem. A good diffusion process can help an image encryption method to defeat this attack. According to this principle, ICMIE designs a diffusion process to change the pixel values of the confusion image F. Its detail process can be described as follows.

The detail diffusion process is described in Algorithm 1 and a numerical example is shown in Fig. 8. Matrices X and Y generated

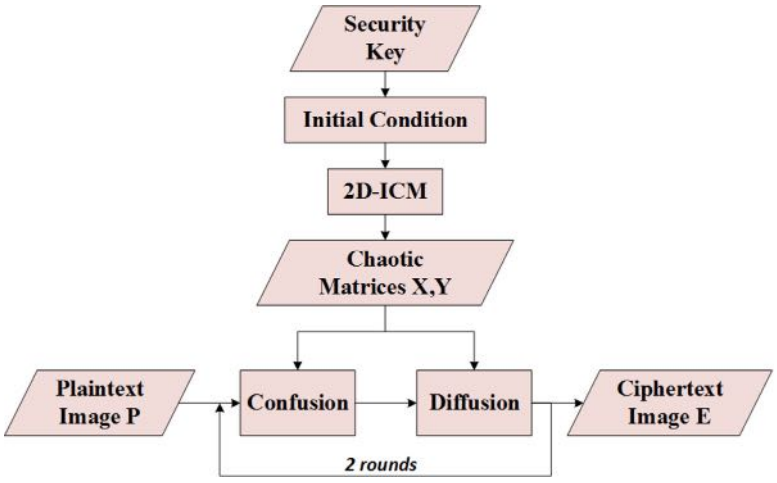

Fig. 5. Structure of ICMIE encryption process.

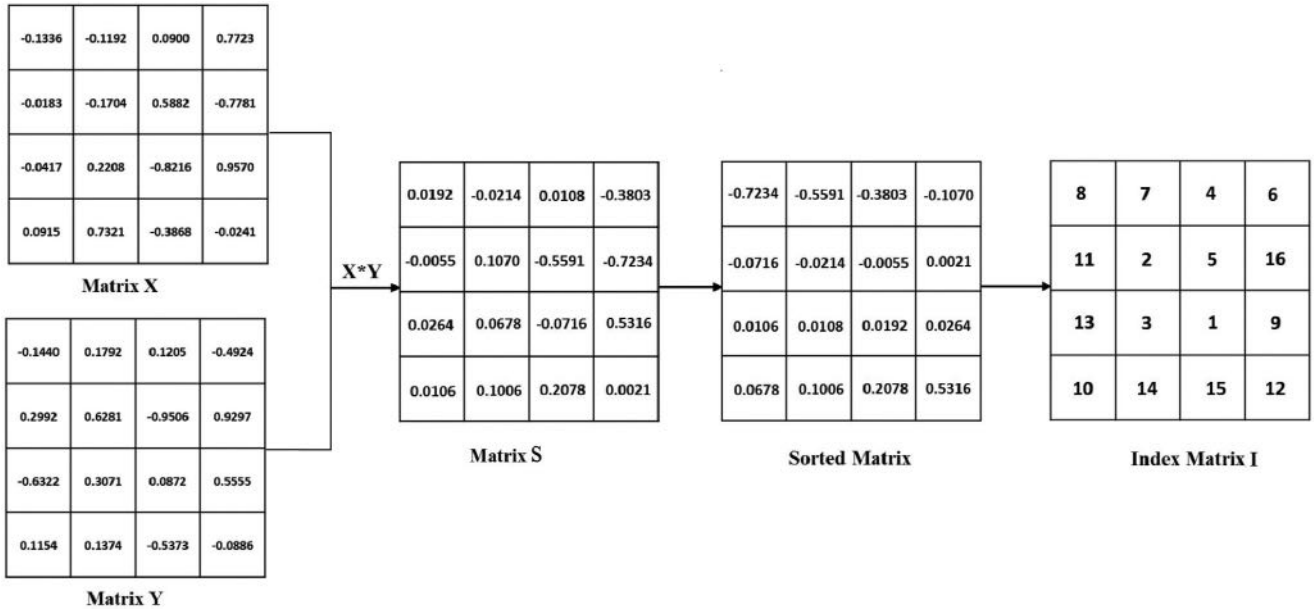

Fig. 6. An example of generating Matrix *S* and its index matrix.

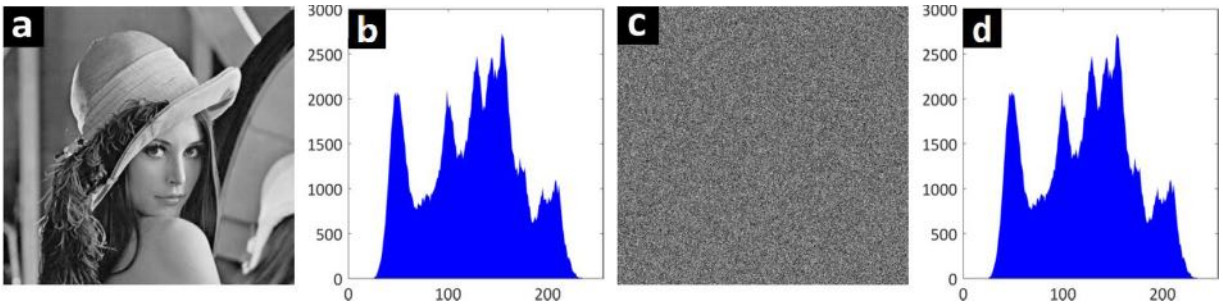

Fig. 7. ICMIE confusion:(a) *lena* image; (b) histogram of (a); (c) confusion image of (a); (d) histogram of (c).

by 2*D*-ICM are alternately used to generate the index and value matrices in two rounds of ICMIE diffusion. The index matrix x in Fig. 8 represents the corresponding data positions of X with an ascending order. Taking two adjacent pixels in the confusion image F with their corresponding index values in x, the pixel value of diffusion image is obtained by

$$D_i = \begin{cases} \lfloor (A_i + A_{M\times N} + |Y_i| \times (2^{31}-1)) \bmod 256 \rfloor & \text{if } i = 1, \\ \lfloor (A_i + D_{i-1} + |Y_i| \times (2^{31}-1)) \bmod 256 \rfloor & \text{if } i \in [2, M\times N], \end{cases} \tag{10}$$

where $\lfloor . \rfloor$ is the floor operation.

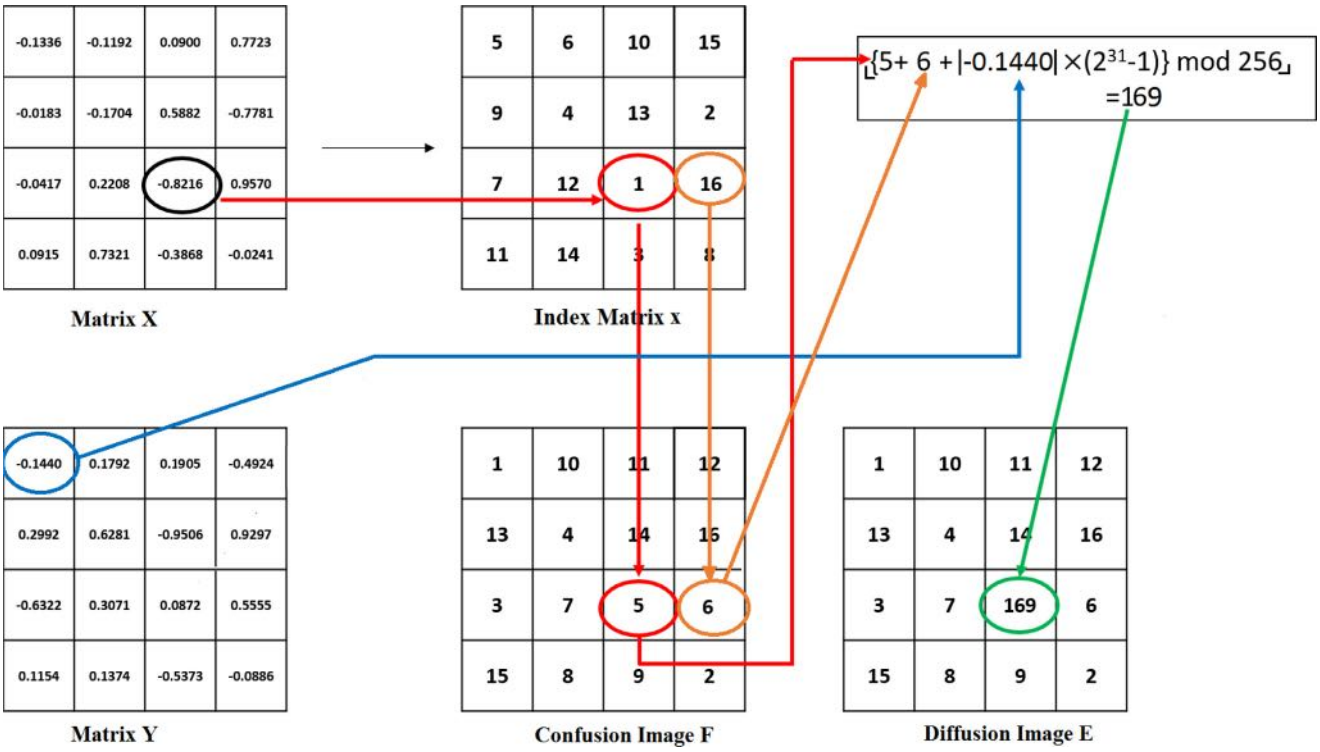

Fig. 8. An example of ICMIE diffusion.

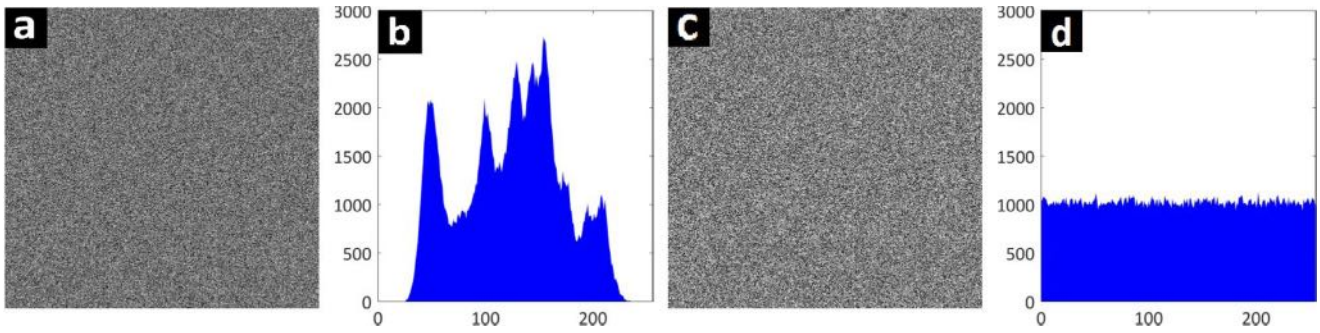

Fig. 9. ICMIE diffusion: (a) the confused *Lena* image by ICMIE confusion and (b) its histogram; (c) its diffusion image E and (d) its histogram.

As shown in Fig. 9(d), the histogram of the ciphertext image is uniformly distributed and completely different from the plaintext image. ICMIE performs two rounds of the confusion and diffusion processes to obtain the final encrypted image.

3.4. Image decryption

Generally, the decryption processes are the inverse processes of the image encryption. Using the correct key to generate the chaotic matrices X and Y, the decryption processes of ICMIE will alternatively perform the inverse diffusion and confusion processes in two rounds and then obtain the recovered image. The pixel values of the ciphertext image can be first recovered using the inverse processes of ICMIE diffusion. The processes can be defined as

$$A_i = \begin{cases} \lfloor (D_i - D_{i-1} - |Y_i| \times (2^{31}-1)) \bmod 256 \rfloor & \text{if } i \in [2, M \times N], \\ \lfloor (D_i - A_{M \times N} - |Y_i| \times (2^{31}-1)) \bmod 256 \rfloor & \text{if } i = 1. \end{cases} \quad (11)$$

The pixel positions of the ciphertext image will be then processed by the inverse confusion processes. The original image is completely reconstructed.

3.5. Simulation results and time complexity analysis

Converting different types of plaintext images into unrecognized ciphertext images is one of requirements of an attractive encryption method. This section will show several experiment and analysis results of ICMIE and its time complexity.

3.5.1. Simulation results

Fig. 10 shows the different types of images encrypted by ICMIE. All ciphertext images including encrypted of all-zero and all-one plaintext images are random-like images with uniformly distributed histograms. All information of plaintext images is well preserved. These experiment results show the good encryption performance of ICMIE. It demonstrates that ICMIE can effectively encrypt various kinds of images.

3.5.2. Time complexity analysis

The time complexity analysis is an essential method to evaluate the efficiency of an image encryption algorithm. Our experiments are performed in Matlab R2017a in a workstation with Intel Core i7-4790K CPU @4.00 GHz and 32.0 GB RAM on Windows 7

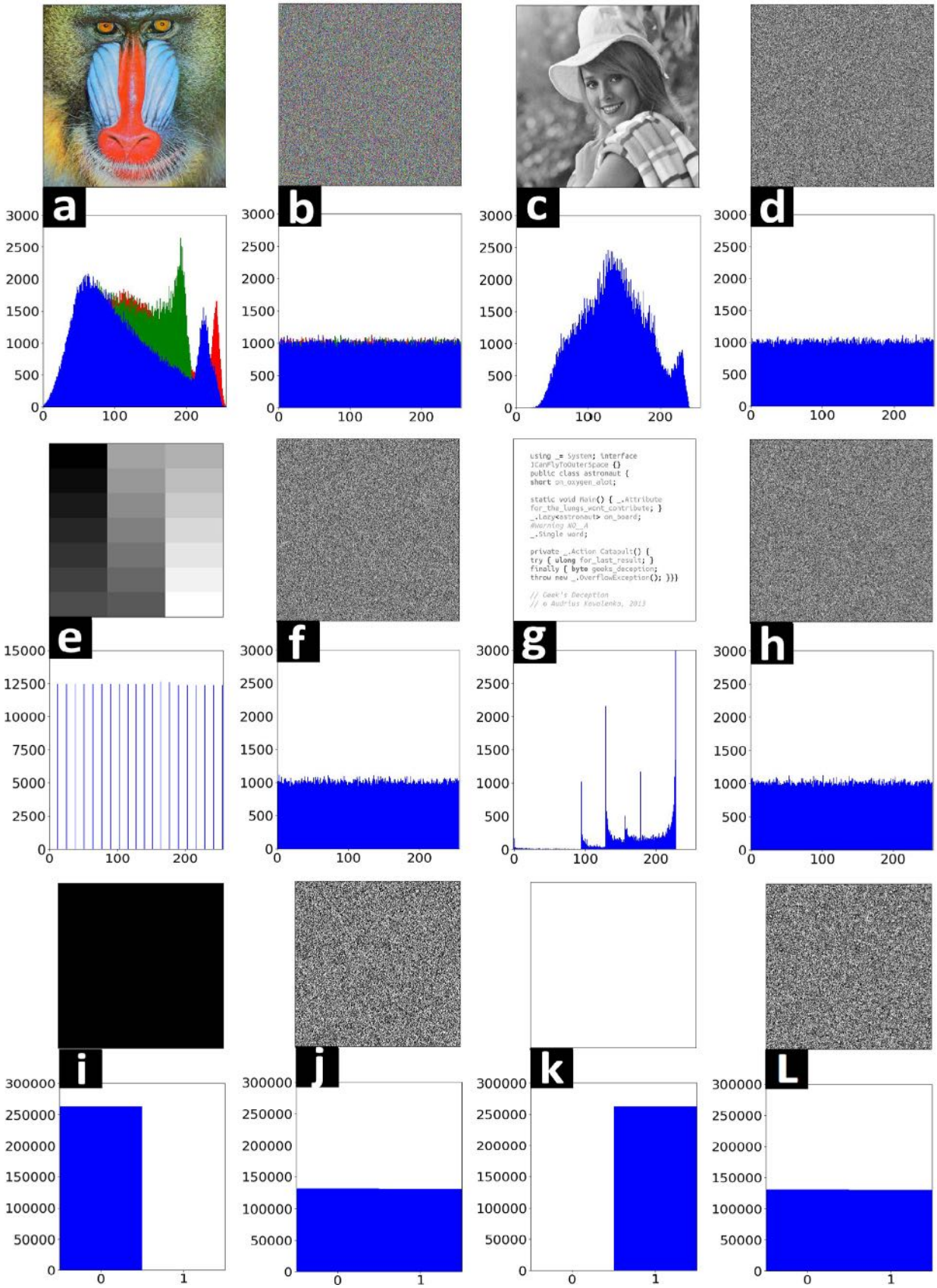

Fig. 10. ICMIE encryption results of various types of images. The odd columns show plaintext images and their histograms; the even columns show their ciphertext images and histograms: (a) color image; (c) grayscale image; (e) grayscale image with different block intensity; (g) handwriting image; (i) all-zero image; (k) all-ones image.

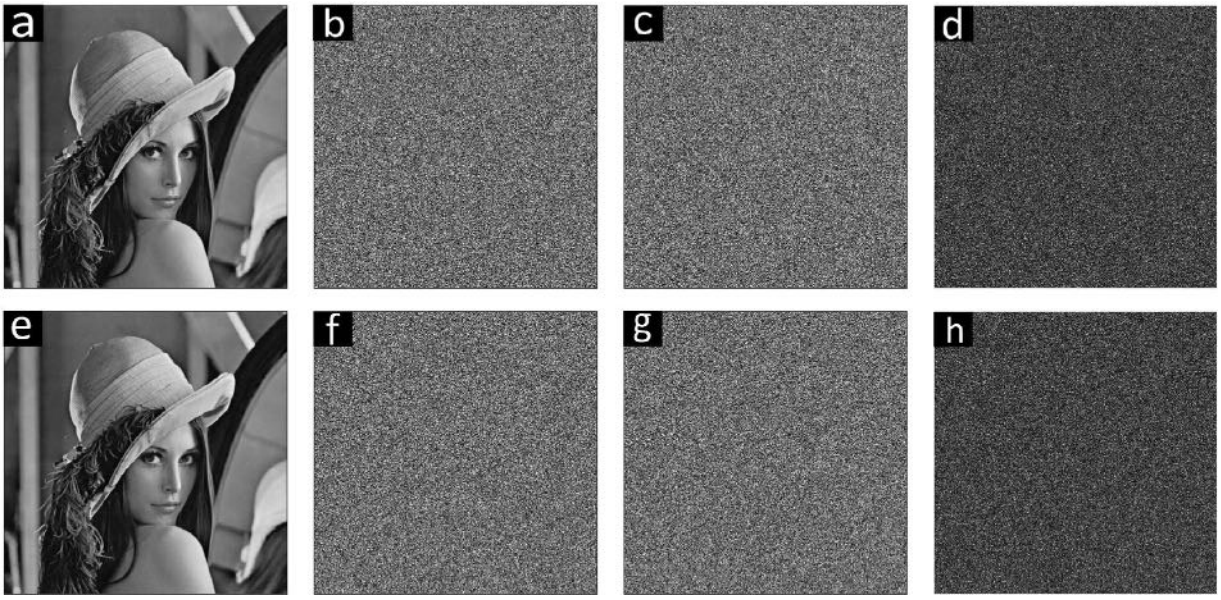

Fig. 11. Key sensitivity analysis: (a)the plaintext image P; (b) the ciphertext image E_1 encrypted by K_1; (c) the ciphertext image E_2 encrypted by K_2; (d) the difference between E_1 and E_2; (e) the decrypted image D_1 recovered from E_1 by K_1; (f) the decrypted image D_2 recovered from E_1 by K_2; (g) the decrypted image D_3 recovered from E_1 by K_3; (h) the difference between D_2 and D_3.

Table 1
Encryption times (second) of images with different sizes using various schemes.

Algorithms	256 × 256	512 × 512	1024 × 1024
LAS-IES [26]	0.0800	0.3669	1.7526
LSCM-IEA [34]	0.0772	0.3955	2.4708
LSC-IES [35]	0.0778	0.3625	1.7425
ICMIE	**0.0362**	**0.1568**	**0.7110**

OS. The encryption time of ICMIE mainly contains two parts: confusion and diffusion. The confusion time is denoted as t_c and the diffusion time is set as t_d. Then whole encryption time of ICMIE is $2(t_c + t_d)$. Here we use different sizes of images in USC-SIPI 'Miscellaneous' dataset as examples. These images are encrypted 50 times using different encryption algorithms and the average results are shown in Table. 1. Compared with other image encryption algorithms, ICMIE has the shortest encryption time. The ICMIE decryption is the inverse process of its encryption. Therefore, ICMIE has low time complexity.

4. Security analysis

4.1. Security key analysis

For a qualified image encryption algorithm, it usually has a sufficiently large security key space to resist brute-force attack and it is extremely sensitive to its key variations. ICMIE has a security key space of 2^{240} since its security key length is 240 bits. Next, we analyze how ICMIE is sensitive to its security keys.

The key sensitivity analysis can be divided into two parts: the sensitivity of illegal keys in both encryption and decryption processes. The security key is highly sensitive in the encryption process when the difference between the encrypted images is absolutely diverse using two slightly distinct keys. In the decryption process, the key sensitivity is high when the encrypted image cannot be recovered using tinily changed security keys and the incorrectly recovered images are totally different.

The key sensitivity results are shown in Fig. 11. There are two ciphertext images E_1 and E_2 (Fig. 11(b) and (c)) that generated from the same plaintext P (Fig. 11(a)) using two security keys K_1 and K_2 with 1-bit difference. The difference of that these two encryption results (Fig. 11(d)) shows the ciphertext images are totally different. As shown in Fig. 11(b), the ciphertext image can be correctly decrypted by the security key K_1 that is the same as the one in the encryption process. Fig. 11(f) and (g) show the decryption results using other two keys K_2 and K_3 that have 1-bit difference with K_1. As can be seen, the ciphertext image (Fig. 11(b)) cannot be decrypted using incorrect keys. Fig. 11(h) shows the difference between these two incorrect decrypted results. They are completely different. Therefore, ICMIE is quite sensitive to its security keys in both encryption and decryption processes.

4.2. Robustness analysis of noise and data loss

Different types of noise and data loss are easily occurred in the transmission and storage of digital images. The resistibility to the noise and data loss is a necessary property of image encryption algorithms. It requires that the image encryption method can resist the distortion of the ciphertext image. In the ICMIE decryption process, the slight changes of ciphertext images has little effect to the received images. Fig. 12 shows that ICMIE is robust against 5% salt&pepper and Gaussian noises. It also evaluates the resistibility of ICMIE against different levels of data loss at the certain or random positions. As we can see, ICMIE can decrypt ciphertext images with noise or data loss. The recovered images are still recognizable when the ciphertext image has 15% data loss. It proves that ICMIE has a strong capacity to resist noise and data loss attacks.

4.3. Histogram analysis

The distributions of pixel values can be represented by histograms. The histograms of plaintext and ciphertext images are shown in Fig. 10. It can be visually shown that the values of ciphertext images are uniformly distributed. They obviously differ from the plaintext images. Furthermore, we apply the chi-square test to quantitatively evaluate the uniformity of ciphertext images. Its statistic χ^2-value can be mathematically defined as

$$\chi^2 = \sum_{p=0}^{255} \left(\frac{E_p - Z}{Z} \right), \tag{12}$$

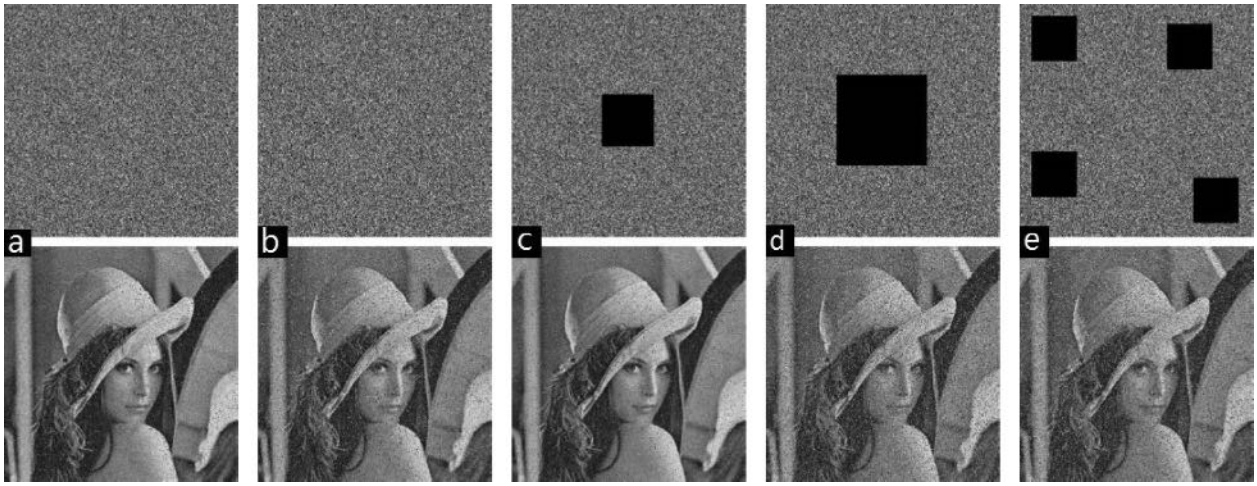

Fig. 12. Robustness analysis of ICMIE. The first row shows the ciphertext images with different types of noise and data loss, and the second row shows the corresponding decrypted images: (a) 5% Gaussian noise; (b) 5% salt&pepper noise; (c) 4% data loss at center block; (d) 15% data loss at center block; (e) 15% data loss at random block positions.

Table 2
Chi-square evaluation results of ciphertext images of ICMIE.

Images	Lena	Pepper	Binary	Elaine	Cameraman
χ^2	252.0625	223.6641	223.6641	234.5195	250.8438

where E_p and Z are the actual number and the expected frequency number of each gray level, respectively. A smaller χ^2 value means the more uniform distribution of an image histogram. When the confidence level is set to 5%, $\chi^2_{0.05} = 293.2478$. If the calculated χ^2-value of an image encryption algorithm do not exceed 293.2478, this algorithm can pass the chi-square assessment. Table 2 shows the chi-square values of various ciphertext images. All results are less than 293.2478. This indicates that the histogram distributions of the ciphertext images of our ICMIE are uniformly distributed. Therefore, it is difficult for attackers to obtain any valuable information from the ciphertext images using the statistic analysis.

4.4. Correlation analysis

The pixels in a plaintext image often have high correlations among neighbouring pixels. The image encrypted by a qualified image encryption algorithm should have a low correlation among adjacent pixels. Mathematically, the pixel correlation can be calculated by

$$C_{U,V} = \frac{E[(U-\mu_U)(V-\mu_V)]}{\sigma_U \sigma_V}, \tag{13}$$

where U and V are two input sequences, μ is the mean value, σ is the standard deviation. If these two input sequences U and V have low correlations, their correlation value will be close to 0, or else it is close to 1.

To evaluate the pixel correlations of the image encrypted by ICMIE, we randomly choose 3000 pairs of adjacent pixels from both plaintext and ciphertext images in horizontal, vertical, and diagonal directions, respectively. The distributions of these pairs and correlation coefficients of pixel pairs in plantext and cipertext images are shown in Fig. 13 and Table 3. It shows that pixels in the plaintext image are close to the diagonal line in the coordinate system, while pixel pairs in the ciphertext image are randomly disperse. Table 3 shows the quantitative results of the correlations of adjacent pixel pairs and comparison results. The results of the plaintext image are close to 1 while the results of the ciphertext images are close to 0. Comparing with the methods of LAS-IES [26], LSCM-IEA [34], and LSC-IES [35], the $C_{U,V}$ values of ICMIE are closer to 0 than other schemes. It further proves that ICMIE can break the strong correlations of pixels in plaintext images.

4.5. Randomness analysis

To test the randomness of the pseudorandom number generator (PRNG), there are some stringent randomness evaluation methods, e.g. TestU01 and FIPS 140-2 test suites. The former one can adaptively perform empirical statistical tests due to its flexible parameters, while the later can be used for the accreditation of cryptographic schemes [36]. The software package of TestU01 contains various test batteries, such as Alphabit, BlockAlphabit, and FIPS 140-2. Here we use these three batteries as examples to test sequences with different lengths by 2D-ICM. Each test obtains a P-value. It can be considered to pass the test when the P-value is within a range of $[10^{-4}, 1-10^{-4}]$. The experimental results are shown in Tables 4 and 5. The 2D-ICM sequences pass all sub-tests of Alphabit, BlockAlphabit, and FIPS 140-2. This means that 2D-ICM is a reliable PRNG and the sequences of 2D-ICM have excellent randomness property.

4.6. Local Shannon entropy

To quantitatively measure the information distribution, the local Shannon entropy (LSE) is applied to evaluate the randomness of an image encryption method [37]. LSE is used to calculate the mean Shannon entropy of n non-overlapped blocks that are randomly chosen in the ciphertext image. Its mathematical function can be defined by

$$H_{n,B_r}(L) = \sum_{i=1}^{n} \frac{H(L_i)}{n}, \tag{14}$$

where $L_1, L_2, ..., L_n$ are n selected blocks with B_r pixels in the chosen image L. If $H_{n,B_r}(L)$ is in the interval of (h^*_{min}, h^*_{max}), the ciphertext image will be considered as passing the test. The values of (h^*_{min}, h^*_{max}) can be calculated by

$$\begin{cases} h^*_{min} = \mu_{H(X)} - \Phi(\alpha/2)^{-1}\sigma_{H(X)}/\sqrt{n}, \\ h^*_{max} = \mu_{H(X)} + \Phi(\alpha/2)^{-1}\sigma_{H(X)}/\sqrt{n}, \end{cases} \tag{15}$$

where $\Phi^{-1}(\cdot)$ is the inverse cumulative distribution function (CDF) of the standard Normal distribution $\mathbb{N}(0,1)$, $\mu_{H(X)}$ and $\sigma_{H(X)}$ are the mean and standard deviation of the LSE values of n non-overlapping blocks of a random image under an ideal condition.

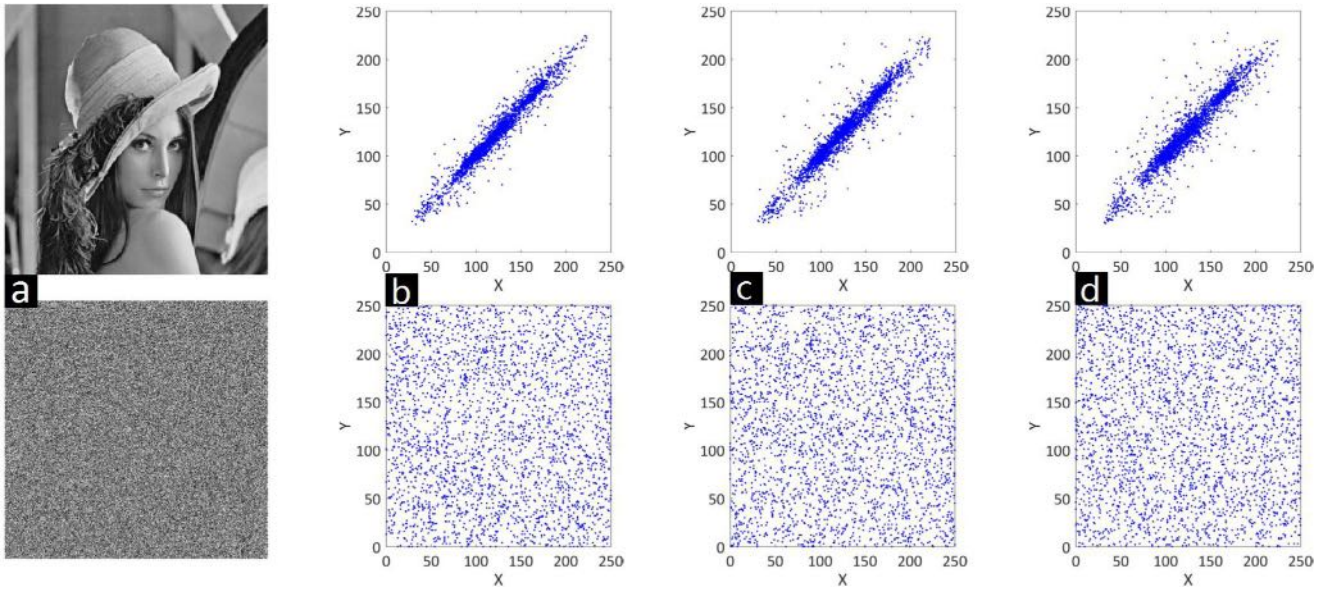

Fig. 13. The correlation distribution of the neighboring pixel pairs: (a) the plaintext image and its ciphertext image; (b) horizontal direction; (c) vertical direction; (d) diagonal direction.

Table 3
Correlation coefficients of the plaintext image and its ciphertext image by different schemes.

Images	Lena image	LAS-IES [26]	LSCM-IEA [34]	LSC-IES [35]	ICMIE
Horizontal	0.9710	−0.0023	−0.0013	0.0013	**−0.0008**
Vertical	0.9573	0.0019	−0.0023	0.0016	**−0.0013**
Diagonal	0.9404	−0.0029	0.0025	0.0026	**0.0018**

Table 4
TestU01 evaluation of the sequences with different lengths generated by 2D-ICM.

Bits lengths	Alphabit	BlockAlphabit
2^{15}	17/17	17/17
2^{20}	17/17	17/17

Table 5
FIPS 140-2 results of the sequences generated by 2D-ICM.

Test	S-value	P-value	FIPS Decision
Monobit	9999	0.50	Pass
Poker	27.04	0.30	Pass
0 Runs, length 1:	2553		Pass
0 Runs, length 2:	1253		Pass
0 Runs, length 3	585		Pass
0 Runs, length 4:	309		Pass
0 Runs, length 5:	170		Pass
0 Runs, length 6+:	163		Pass
1 Runs, length 1:	2539		Pass
1 Runs, length 2:	1235		Pass
1 Runs, length 3:	635		Pass
1 Runs, length 4:	318		Pass
1 Runs, length 5:	153		Pass
1 Runs, length 6+:	153		Pass
Longest run of 0:	13	0.50	Pass
Longest run of 0:	15	0.26	Pass

Number of bits: 20000.

The Shannon entropy $H(X)$ can be calculated by

$$H(X) = -\sum_{i=1}^{n} P(x_i)\log_2 P(x_i), \tag{16}$$

where X is a set of pixels and $P(x_i)$ is the possibility of the i^{th} value x_i in X.

Table 6 shows the LSE results of various image encryption algorithms on 28 images in the USC-SIPI Miscellaneous image dataset. It shows the LSE comparison results of ICMIE with the algorithms of Wu [38], Zhou [39], Wu [40], Liao [41], CMT-IEA [25], and LSCM-IEA [34]. The results marked in bold indicate that the algorithm passes the test. It can be seen that the pass rate of ICMIE outperforms that of other methods.

4.7. Differential attack

The attacker can break a vulnerable image encryption method to detect the change of the ciphertext images from different plaintext images. This attack is called the differential attack or the chosen-plaintext attack. The encryption algorithm can withstand this attack if it has a good diffusion property. The ability to resist this attack can be evaluated by the number of pixel change rate (NPCR) and unified averaged changed intensity (UACI) tests. NPCR and UACI between two ciphertext images E_1, E_2 can be defined as Eqs. (17) and (18), respectively [42],

$$NPCR = \frac{\sum_{m=1}^{M}\sum_{n=1}^{N}\mathcal{A}(m,n)}{MN} \times 100\%, \tag{17}$$

$$UACI(E_1, E_2) = \sum_{i=1}^{M}\sum_{j=1}^{N}\frac{|E_1(i,j) - E_2(i,j)|}{255 \times M \times N} \times 100\%, \tag{18}$$

where E_1 and E_2 are two $M \times N$ ciphertext images that are generated by encrypting two plaintext images with only one pixel difference, and function $\mathcal{A}(m,n)$ is the number of different pixels between E_1 and E_2.

Wu brought a new standard of NPCR and UACI measures [42] that are more suitable for evaluating the performance of image encryption algorithms. In these hypotesis tests, it can be regarded as passing the NPCR test if the NPCR value of the encryption algorithm is bigger than a criteria with a level α as

Table 6
The local Shannon entropy results of different image encryption methods with $\alpha = 0.001, n = 30, B_r = 1936$.

File name	Wu [38]	Zhou [39]	Wu [40]	Liao [41]	CMT-IEA [25]	LSCM-IEA [34]	ICMIE
5.1.09	**7.901985**	**7.903354**	7.903764	7.904191	**7.902127**	**7.902281**	**7.902710**
5.1.10	**7.902731**	**7.902443**	**7.901801**	**7.902371**	**7.903402**	**7.902198**	**7.902473**
5.1.11	**7.902446**	**7.902756**	**7.903306**	7.900799	**7.903402**	7.899982	**7.902217**
5.1.12	**7.902556**	**7.901526**	7.904478	**7.903374**	**7.901906**	**7.902827**	**7.903208**
5.1.13	**7.902688**	7.945630	7.904657	7.904566	**7.902825**	**7.902281**	**7.902951**
5.1.14	7.903474	**7.902945**	**7.902874**	**7.903111**	**7.902340**	7.903117	**7.901577**
5.2.08	7.903953	**7.902356**	**7.903218**	**7.901762**	**7.903327**	**7.902304**	**7.902681**
5.2.09	**7.902233**	7.899853	**7.903089**	7.905854	**7.901765**	**7.902022**	**7.902571**
5.2.10	7.900714	**7.902654**	**7.902077**	**7.902768**	**7.902748**	7.906701	**7.902411**
5.3.01	**7.902727**	**7.902647**	**7.902108**	7.901040	**7.901772**	**7.902119**	**7.903408**
5.3.02	**7.903182**	7.900474	7.904169	7.900981	**7.903328**	**7.902658**	**7.903093**
7.1.01	**7.902173**	**7.902634**	**7.901965**	**7.902145**	7.901305	**7.902191**	**7.901900**
7.1.02	7.900879	**7.901634**	7.904970	**7.902157**	**7.901578**	**7.902047**	**7.903003**
7.1.03	**7.902543**	7.905423	7.891503	7.900645	**7.903099**	**7.902584**	**7.902116**
7.1.04	7.901126	**7.902125**	**7.903399**	7.904141	**7.902607**	**7.901913**	**7.902998**
7.1.05	7.903579	7.883653	7.901301	7.900027	7.905305	**7.902392**	**7.903154**
7.1.06	**7.901930**	**7.902356**	**7.903367**	**7.901736**	**7.902695**	**7.902565**	**7.902009**
7.1.07	**7.903000**	**7.902364**	7.899556	7.900802	**7.902896**	7.904015	**7.903176**
7.1.08	**7.903197**	7.904456	7.883531	7.900944	**7.901632**	7.901096	**7.902837**
7.1.09	**7.902308**	**7.903012**	**7.903201**	7.905658	**7.903173**	**7.902933**	**7.902068**
7.1.10	7.899542	**7.901598**	**7.901542**	7.893848	**7.901524**	**7.902534**	**7.903141**
7.2.01	**7.902772**	**7.901989**	7.904945	7.904525	**7.902454**	**7.902529**	**7.902316**
boat.512	**7.901908**	**7.901879**	**7.903091**	7.900712	**7.903088**	7.901782	**7.901920**
elaine.512	7.901122	**7.902989**	**7.901859**	**7.902030**	**7.901720**	**7.902569**	**7.903219**
gray21.512	7.900170	7.905107	**7.901832**	**7.902149**	**7.902688**	**7.902593**	**7.903359**
numbers.512	7.903615	7.892351	**7.902144**	7.903579	**7.901657**	**7.902295**	**7.903379**
ruler.512	**7.903265**	**7.903001**	**7.901937**	7.901428	**7.903052**	7.904102	**7.901889**
testpat.1k	**7.902806**	**7.901681**	7.903856	**7.903343**	**7.902752**	7.904472	**7.903202**
Mean	**7.902308**	**7.901923**	7.903764	**7.902167**	**7.902488**	**7.902611**	**7.902678**
Pass Rate	18/28	20/28	17/28	11/28	26/28	20/28	28/28

$h^*_{min}/h^*_{max} = 7.901515698/7.903422936$.

Table 7
The NPCR results of various image encryption methods ($\alpha = 0.05$).

Image sizes NPCR	256 × 256 ≥ 99.5693	512 × 512 ≥ 99.5893	1024 × 1024 ≥ 99.5994	Pass rate
Wu [38]	6/6	18/18	4/4	28/28
Zhou [39]	6/6	17/18	4/4	27/28
Wu [40]	6/6	17/18	3/4	26/28
Liao [41]	0/6	0/18	0/4	0/28
CMT-IEA [25]	6/6	18/18	4/4	28/28
LAS-IES [26]	6/6	18/18	3/4	27/28
LSCM-IEA [34]	6/6	18/18	4/4	28/28
LSC-IES [35]	6/6	18/18	4/4	28/28
ICMIE	6/6	18/18	4/4	28/28

described in

$$\mathcal{R}^*_\alpha = \frac{M \times N - \Phi^{-1}(\alpha)\sqrt{M \times N/255}}{M \times N + 1}, \tag{19}$$

where $\Phi^{-1}()$ is inverse CDF of the standard Normal distribution $\mathbb{N}(0,1)$. An image encryption algorithm can be considered as passing the UACI test if the simulation value is in the range of $(\mathcal{A}^{*-}_\alpha, \mathcal{A}^{*+}_\alpha)$ in

$$\begin{cases} \mathcal{A}^{*-}_\alpha = \mu - \Phi^{-1}(\alpha/2)\sigma, \\ \mathcal{A}^{*+}_\alpha = \mu + \Phi^{-1}(\alpha/2)\sigma, \end{cases} \tag{20}$$

where

$$\begin{aligned} \mu &= \frac{M \times N + 2}{3 \times (M \times N) + 3}, \\ \sigma &= \frac{(M \times N + 2)((M \times N)^2 + 2 \times (M \times N) + 3)}{18 \times (M \times N + 1)^2 \times (M \times N) \times 255}. \end{aligned} \tag{21}$$

In this test, we randomly select one pixel from each plaintext image and change its value by 1-bit to generate another plaintext image, and then encrypt both plaintext images to calculate the UPCR and UACI values for six different image encryption algorithms. The results are shown in Tables 7 and 8. From the results, we can see that all 28 images encrypted by ICMIE pass both the NPCR and UACI tests. This means that the ICMIE has superior or competitive performance in defending the differential attack.

Table 8
The UACI results of various image encryption methods ($\alpha = 0.05$).

Image sizes UACI	256 × 256 33.2255-33.7016	512 × 512 33.3730-33.5541	1024 × 1024 33.4183-33.5088	Pass rate
Wu [38]	5/6	18/18	4/4	28/28
Zhou [39]	1/6	4/18	2/4	27/28
Wu [40]	6/6	15/18	4/4	26/28
Liao [41]	0/6	0/18	0/4	0/28
CMT-IEA [25]	6/6	17/18	4/4	28/28
LAS-IES [26]	6/6	18/18	4/4	28/28
LSCM-IEA [34]	6/6	18/18	4/4	28/28
LSC-IES [35]	6/6	18/18	4/4	28/28
ICMIE	6/6	18/18	4/4	28/28

4.8. Analysis of different attacks

The known-plaintext, chosen-plaintext, and chosen-ciphertext attacks are three common attack methods for attacker to break image encryption schemes. For the known-plaintext and chosen-plaintext, the all-black and all-white images are applied. The chosen-ciphertext attack can break the encryption schemes using the decryption of the chosen ciphertexts. 2D-ICM has excellent ergodicity, hyperchaotic properties, randomness. These properties can significantly enhance the capacity of ICMIE against these attacks. Fig. 10 shows that the encrypted results of all-black and all-white images are totally unrecognized. This verifies that ICMIE has an excellent permutation property. In addition, the histogram and correlation analysis demonstrates that ICMIE is immune to statistical attacks. Furthermore, the results of TestU01, FIPS 140-2, and Local Shannon entropy can prove that ICMIE has strong unpredictable properties. ICMIE also has passed the NPCR and UACI tests in resisting the differential attack. Thus, as a symmetric image encryption algorithm, ICMIE has strong randomness and robustness against the known-plaintext, chosen-plaintext, and chosen-ciphertext attacks.

5. Conclusion

This paper has proposed a 2D chaotic map, 2D-ICM that is the modulation of infinite collapse maps. The excellent hyper-chaotic performance of 2D-ICM has been proved in the evaluation of its large chaotic trajectory distribution, positive Lyapunov exponent values, big correlation dimension values, and high Kolmogorov entropy values. 2D-ICM has superior chaotic characteristics, better ergodicity, and a larger chaotic range than state-of-the-art 2D chaotic maps. We then designed a 2D-ICM based image encryption algorithm, named ICMIE. Owning to the unpredictable properties of 2D-ICM, ICMIE can encrypt various kinds of images with a high security level and perform better than several competing image encryption algorithms. ICMIE can also withstand various attacks including noise, data loss, and differential attacks as shown in the experimental results.

Author contributions

Weijia Cao designed the study and wrote the paper with contributions from all co-authors. This study was initiated from the collaboration among Weijia Cao, Yujun Mao and Yicong Zhou. Yujun Mao has participated in performing the evaluation methods of the 2D chaotic maps. Yicong Zhou gave the instruction of the proposed algorithm. He also helped to improve the grammar and expressions of this paper.

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.

Acknowledgement

This work was funded in part by The Science and Technology Development Fund, Macau SAR (File no. 189/2017/A3), and by the Research Committee at University of Macau under Grants MYRG2016-00123-FST and MYRG2018-00136-FST.

References

[1] M. Alawida, A. Samsudin, J.S. Teh, R.S. Alkhawaldeh, A new hybrid digital chaotic system with applications in image encryption, Signal Process. 160 (2019) 45–58.
[2] C. Li, Y. Zhang, E.Y. Xie, When an attacker meets a cipher-image in 2018: A year in review, J. Inf. Secur. Appl. 48 (2019) 102361.
[3] Z. Hua, B. Xu, F. Jin, H. Huang, Image encryption using Josephus problem and filtering diffusion, IEEE Access PP (2019). 1–1
[4] FIPS PUB 46, Data encryption standard (DES), 1999.
[5] FIPS PUB 197, Advanced encryption standard (AES), 2001.
[6] C. Li, D. Lin, B. Feng, J. Lü, F. Hao, Cryptanalysis of a chaotic image encryption algorithm based on information entropy, IEEE Access 6 (2018) 75834–75842.
[7] Y. Wu, Y. Zhou, S. Agaian, J.P. Noonan, A symmetric image cipher using wave perturbations, Signal Process. 102 (2014) 122–131.
[8] X. Wang, D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun. Nonlinear Sci. Numer. Simul. 18 (11) (2013) 3075–3085.
[9] W. Cao, Y. Zhou, C.L. Chen, L. Xia, Medical image encryption using edge maps, Signal Process. 132 (2017) 96–109.
[10] Y. Zhou, W. Cao, C.L. Philip Chen, Image encryption using binary bitplane, Signal Process. 100 (2014) 197–207.
[11] H. Zhu, Y. Zhao, Y. Song, 2D Logistic-modulated-Sine-coupling-Logistic chaotic map for image encryption, IEEE Access 7 (2019) 14081–14098.
[12] H. Zhu, W. Qi, J. Ge, Y. Liu, Analyzing Devaney chaos of a Sine-Cosine compound function system, Int. J. Bifurcat. Chaos 28 (14) (2018) 1850176.
[13] H. Zhu, X. Zhang, H. Yu, C. Zhao, Z. Zhu, An image encryption algorithm based on compound homogeneous hyper-chaotic system, Nonlinear Dyn. 89 (1) (2017) 61–79.
[14] Z. Xia, X. Wang, W. Zhou, R. Li, C. Wang, C. Zhang, Color medical image lossless watermarking using chaotic system and accurate quaternion polar harmonic transforms, Signal Process. 157 (2019) 108–118.
[15] M. Asgari-Chenaghlu, M.A. Balafar, M.R. Feizi-Derakhshi, A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation, Signal Process. 157 (2019) 1–13.
[16] Z. Hua, Y. Zhou, Exponential chaotic model for generating robust chaos, IEEE Transact. Syst. Man Cybernet. PP (2019) 1–12.
[17] M. Alawida, J.S. Teh, A. Samsudin, W.H. Alshoura, An image encryption scheme based on hybridizing digital chaos and finite state machine, Signal Process. 164 (2019) 249–266.
[18] X. Chai, X. Fu, Z. Gan, Y. Lu, Y. Chen, A color image cryptosystem based on dynamic DNA encryption and chaos, Signal Process. 155 (2019) 44–62.
[19] C. Li, D. Lin, J. Lü, F. Hao, Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography, IEEE MultiMedia 25 (4) (2018) 46–56.
[20] J. Chen, Z. Zhu, L. Zhang, Y. Zhang, B. Yang, Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption, Signal Process. 142 (2018) 340–353.
[21] S. Chen, J. Lü, Parameters identification and synchronization of chaotic systems based upon adaptive control, Phys. Lett. A 299 (4) (2002) 353–358.
[22] X. Wu, H. Hu, B. Zhang, Parameter estimation only from the symbolic sequences generated by chaos system, Chaos Soliton. Fract. 22 (2) (2004) 359–366.
[23] W. Liu, K. Sun, C. Zhu, A fast image encryption algorithm based on chaotic map, Opt. Lasers Eng. 84 (2016) 26–36.
[24] C. Cao, K. Sun, W. Liu, A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map, Signal Process. 143 (2018) 122–133.
[25] Z. Hua, Y. Zhou, C.-M. Pun, C.P. Chen, 2D Sine Logistic modulation map for image encryption, Inf. Sci. 297 (2015) 80–94.
[26] Z. Hua, Y. Zhou, Image encryption using 2D Logistic-adjusted-Sine map, Inf. Sci. 339 (2016) 237–253.
[27] C. Li, B. Feng, S. Li, J. Kurths, G. Chen, Dynamic analysis of digital chaotic maps via state-mapping networks, IEEE Trans. Circuit. Syst. 66 (6) (2019) 2322–2335.
[28] D. He, C. He, L.-G. Jiang, H.-w. Zhu, G.-r. Hu, Chaotic characteristics of a one-dimensional iterative map with infinite collapses, IEEE Trans. Circuit. Syst. 48 (7) (2001) 900–906.
[29] D. Fournier-Prunaret, R. Lopez-Ruiz, Basin Bifurcations in a Two-Dimensional Logistic Map, Eprint Arxiv Nlin (2003) 123–136.
[30] P. Grassberger, I. Procaccia, Measuring the strangeness of strange attractors, Phys. D Nonlinear Phenomena 9 (1-2) (1983) 189–208.
[31] J. Theiler, Efficient algorithm for estimating the correlation dimension from a set of discrete points, Phys. Rev. A 36 (1987) 4456–4462.
[32] P. Grassberger, I. Procaccia, Estimation of the Kolmogorov entropy from a chaotic signal, Phys. Rev. A 28 (1983) 2591–2593.
[33] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurcat. Chaos 16 (08) (2006) 2129–2151.
[34] Z. Hua, F. Jin, B. Xu, H. Huang, 2D Logistic-Sine-coupling map for image encryption, Signal Process. 149 (2018) 148–161.
[35] Z. Hua, Y. Zhou, H. Huang, Cosine-transform-based chaotic system for image encryption, Inf. Sci. 480 (2019) 403–419.

[36] E. Barker, A. Roginsky, R. Blank, P.D. Gallagher, U. Secretary, NIST Special Publication 800-133 Recommendation for Cryptographic Key Generation, 2012.
[37] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J.P. Noonan, P. Natarajan, Local shannon entropy measure with statistical tests for image randomness, Inf. Sci. 222 (2013) 323–342.
[38] Y. Wu, J.P. Noonan, G. Yang, H. Jin, Image encryption using the two-dimensional logistic chaotic map, J. Electron. Imag. 21 (1) (2012) 1–17.
[39] Y. Zhou, L. Bao, C.L.P. Chen, Image encryption using a new parametric switching chaotic system, Signal Process. 93 (11) (2013) 3039–3052.
[40] Y. Wu, J.P. Noonan, S. Agaian, A wheel-switch chaotic system for image encryption, in: Proceedings of the 2011 International Conference on System Science and Engineering (ICSSE), 2011, pp. 23–27.
[41] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (9) (2010) 2714–2722.
[42] Y. Wu, J.P. Noonan, S. Agaian, et al., NPCR and UACI randomness tests for image encryption, Cyber J. 1 (2) (2011) 31–38.