Information Sciences 339 (2016) 237–253

Contents lists available at ScienceDirect

Information Sciences

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

Image encryption using 2D Logistic-adjusted-Sine map

Zhongyun Hua, Yicong Zhou*

Department of Computer and Information Science, University of Macau, Macau 999078, China

ARTICLE INFO

Article history:
Received 23 April 2015
Revised 21 December 2015
Accepted 3 January 2016
Available online 11 January 2016

Keywords:
Chaotic map
Chaotic encryption
Confusion and diffusion
Image encryption

ABSTRACT

With complex properties of ergodicity, unpredictability and sensitivity to initial states, chaotic systems are widely used in cryptography. This paper proposes a two-dimensional Logistic-adjusted-Sine map (2D-LASM). Performance evaluations show that it has better ergodicity and unpredictability, and a wider chaotic range than many existing chaotic maps. Using the proposed map, this paper further designs a 2D-LASM-based image encryption scheme (LAS-IES). The principle of diffusion and confusion are strictly fulfilled, and a mechanism of adding random values to plain-image is designed to enhance the security level of cipher-image. Simulation results and security analysis show that LAS-IES can efficiently encrypt different kinds of images into random-like ones that have strong ability of resisting various security attacks.

1. Introduction

With the fast development of digital technologies and communication networks, more and more digital data carrying all kinds of information are generated and transmitted over the networks. Among these data, digital images are a typical type of two-dimensional (2D) data, which contain a large amount of information. Two examples are as follows: a warship photo may tell not only its size and weapon configurations, but also its rough location and military mission; a personal photo may not only display what he/she looks like, but also his/her rough age and health condition. Because a digital image may contain much inferable information, image security attracts more and more attention. Among all kinds of image security technologies, image encryption is a visualized way by transforming a meaningful original image into an unrecognizable and noise-like cipher- image [29,47,48].

The most direct strategy of image encryption is to treat a digital image as a binary stream, and encrypt it with the developed data encryption schemes, such as the Data Encryption Standard and Advanced Encryption Standard [9,10]. However, a pixel is commonly represented by 8 or more bits and strong correlation may exist between adjacent pixels. When encrypting a digital image as a binary stream without considering the property of pixels, the strong correlation may still remain and the encryption efficiency may be quite low. Therefore, considering the special properties of digital images, many image encryption schemes were proposed using different kinds of methods, such as chaotic maps [17,26,49], wave perturbations [40], wavelet transform [3,35], and magic cube [7,19].

As many studies have pointed out that many properties of chaotic systems are similar to the counterparts in cryptography since the early 1990s [11,16,36,45,52], chaotic systems are quite suitable for cryptography and have been widely used in image encryption [19,50,51]. When chaotic systems are used in image encryption, the security levels of image encryption schemes are highly dependent on performance of the used chaotic systems. For some one-dimensional (1D) chaotic systems,

* Corresponding author. Tel.: +853 88228458; fax: +853 88222426.
E-mail addresses: huazyum@gmail.com (Z. Hua), yicongzhou@umac.mo (Y. Zhou).

http://dx.doi.org/10.1016/j.ins.2016.01.017
0020-0255/

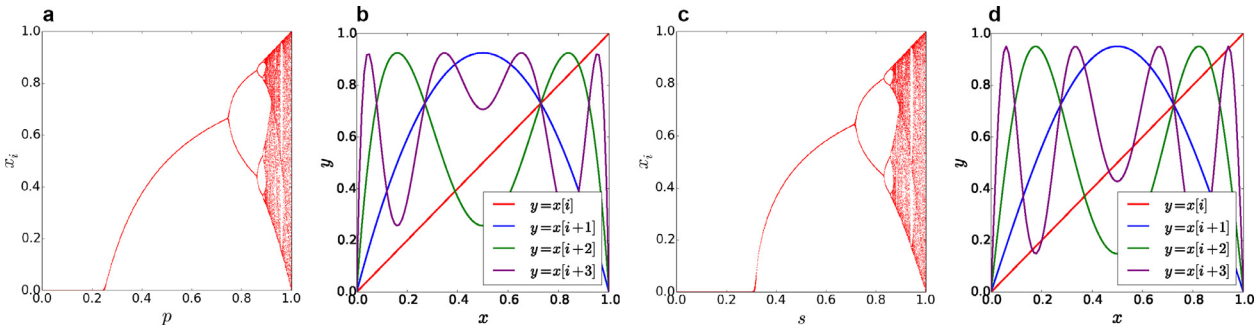

Fig. 1. Logistic map's (a) bifurcation and (b) iteration function diagrams; Sine map's (c) bifurcation and (d) iteration function diagrams.

their chaotic orbits are quite simple and may be predicted easily. Once some information is extracted [2,18,31], their initial states may be estimated using some techniques [6,25,28,37]. Using a chaotic system with a simple chaotic behavior, the corresponding image encryption scheme may be easily attacked [2,20,21,34]. The high-dimensional chaotic systems have complex chaotic behaviors and their chaotic orbits are difficult to be predicted. However, they also have some weaknesses, such as complex performance analysis and high implementation costs [44].

This paper first proposes a new 2D chaotic map, called the 2D Logistic-adjusted-Sine map (2D-LASM). It uses the Logistic map to adjust the input of the Sine map and then extends its phase plane from 1D to 2D. Performance evaluations show that 2D-LASM has a wider chaotic range, better ergodicity and unpredictability than several existing chaotic maps. Using 2D-LASM, this paper further designs a 2D-LASM-based image encryption scheme (LAS-IES). It performs confusion and diffusion operations in the bit level. An additional mechanism of adding random values to the plain-image is designed to ensure that each encrypted result is different. Simulation results and security analysis show that LAS-IES can encrypt different kinds of digital images into random-like ones, and it has strong capability against various attacks.

The rest of this paper is organized as follows. Section 2 reviews two traditional 1D chaotic maps. Section 3 proposes 2D-LASM and analyzes its properties. Section 4 introduces LAS-IES using 2D-LASM. Section 5 provides simulation results of LAS-IES and discusses its properties. Section 6 evaluates the security performance of LAS-IES and Section 7 reaches a conclusion.

2. Preliminary knowledge of existing chaotic maps

This section reviews two 1D existing chaotic maps, the Logistic and Sine maps, which are the basic components of generating 2D-LASM.

2.1. Logistic map

The Logistic map is a discrete-time analog of the logistic equation for population growing [27]. Mathematically, the Logistic map is defined as

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

where parameter p is within the range of [0, 1]. When $p \in [0.89, 1]$, Logistic map is chaotic.

Bifurcation diagram shows the output distribution of a chaotic map along its control parameter, while iteration function describes the output distributions along its inputs. Fig. 1(a) and (b) show the bifurcation and several iteration function diagrams of Logistic map, respectively. It is noticed that the outputs of Logistic map distribute in a larger area when p approaches to 1.

2.2. Sine map

When sine function has inputs within the range of $[0, \pi]$, its outputs fall into the range of [0, 1]. Sine map is derived from sine function by transforming its inputs into [0, 1]. It is defined as

$$x_{i+1} = s\sin(\pi x_i), \tag{2}$$

where parameter $s \in [0, 1]$. Sine map is chaotic when $s \in [0.87, 1]$.

The bifurcation and few iteration function diagrams of Sine map are depicted in Fig. 1(c) and (d), respectively. Although Logistic and Sine maps have totally different mathematical definitions, their chaotic behaviors are quite similar, which can be seen from their bifurcation diagrams shown in Fig. 1(a) and (c).

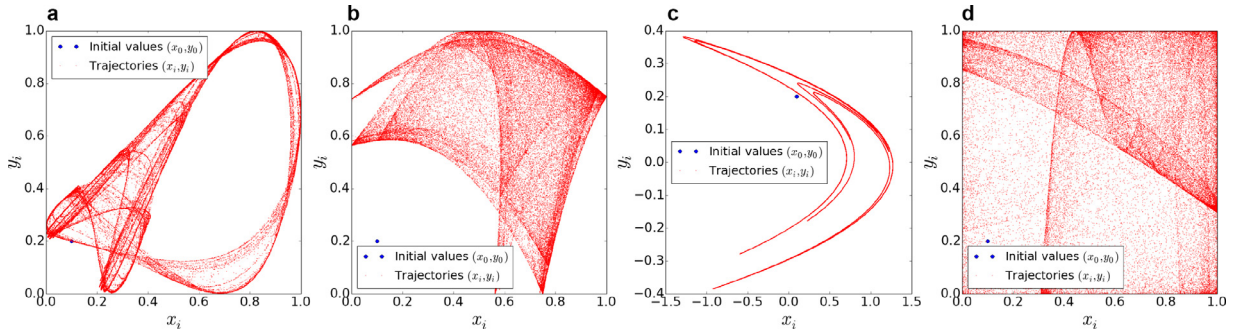

Fig. 2. Trajectories of different 2D chaotic maps: (a) 2D Logistic map with parameter $r = 1.19$; (b) 2D-SLMM with parameters $\alpha = 1,\ \beta = 3$; (c) Hénon map with parameter $a = 1.4,\ b = 0.3$; (d) 2D-LASM with parameter $\mu = 0.9$.

3. 2D Logistic-adjusted-Sine map

We give the mathematical definition of 2D-LASM,

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

where parameter $\mu \in [0, 1]$. 2D-LASM is derived from Sine and Logistic maps. The logistic equation $x_i(1 - x_i)$ is first scaled by a factor of μ, and fed into the input of Sine map. The phase plane is then extended from 1D to 2D. In 2D-LASM, two inputs are interactively influenced and the output pairs (x_{i+1}, y_{i+1}) distribute into the 2D phase plane. Compared with Sine and Logistic maps, it has a more complicated structure and its outputs are more difficult to be predicted.

3.1. Trajectory

For a dynamical system, a trajectory shows the movement path of its outputs. Fig. 2 shows the trajectories of different 2D chaotic maps. The 2D Logistic map is defined as

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

where r is the control parameter [39]. The 2D Sine Logistic modulation map (2D-SLMM) is defined as

$$\begin{cases} x_{i+1} = \alpha(\sin(\pi y_i) + \beta)x_i(1 - x_i), \\ y_{i+1} = \alpha(\sin(\pi x_{i+1}) + \beta)y_i(1 - y_i), \end{cases}$$

where α and β are parameters, $\alpha \in [0, 1]$ and β is usually fixed as 3 [19]. The Hénon map is defined as

$$\begin{cases} x_{i+1} = 1 - ax_i^2 + y_i, \\ y_{i+1} = bx_i, \end{cases}$$

where a and b are parameters [14]. When generating these trajectories presented in Fig. 2, all initial values are set as (0.1, 0.2) and all parameters are set as the values that make the outputs of corresponding chaotic maps distribute in the area as large as possible. From the figures, we can see that output pairs (x_{i+1}, y_{i+1}) of 2D-LASM distribute in the whole data range of the 2D phase plane. They have a much larger distribution area than outputs of other 2D chaotic maps. Therefore, 2D-LASM has better ergodicity and its outputs are more random.

3.2. Lyapunov exponent

The chaos phenomenon can be described as unpredictability and sensitivity to initial states. The Lyapunov exponent (LE) is a widely accepted indictor to measure chaotic behavior of a dynamical system [32,33]. For two close trajectories of a dynamical system, LE describes their degree of divergence. A positive LE means that no matter how close the two trajectories are, their difference divergently increase in each iteration to make them totally different eventually. Therefore, a dynamical system with a positive LE is chaotic. A multi-dimensional dynamical system may have more than one LE. If it has more than one positive LE, its close trajectories exponentially diverge in several dimensions. This phenomenon is called hyperchaotic behavior. A dynamical system with hyperchaotic behavior has extremely good chaos performance and its outputs are difficult to be predicted.

A 2D discrete chaotic map has two LEs. For the 2D Logistic map, 2D-SLMM, Hénon map and 2D-LASM, Fig. 3 presents how their LE values, λ_1 and λ_2, change with respect to the corresponding control parameters. We can observe the following phenomena: 2D Logistic map has chaotic behavior when its parameter $r \in [1.11, 1.15] \cup [1.18, 1.19]$; 2D-SLMM has

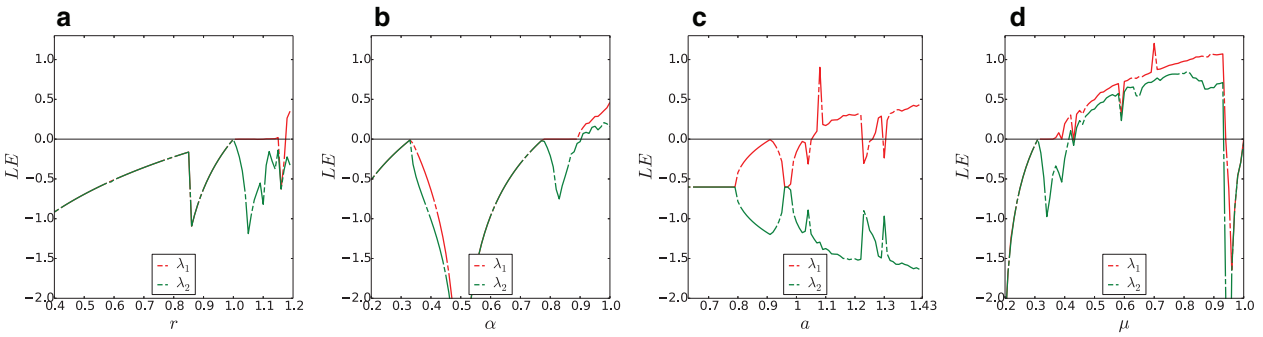

Fig. 3. LEs of different 2D chaotic maps: (a) 2D Logistic map; (b) 2D-SLMM with parameter $\beta = 3$; (c) Hénon map with parameter $b = 0.3$; 2D-LASM.

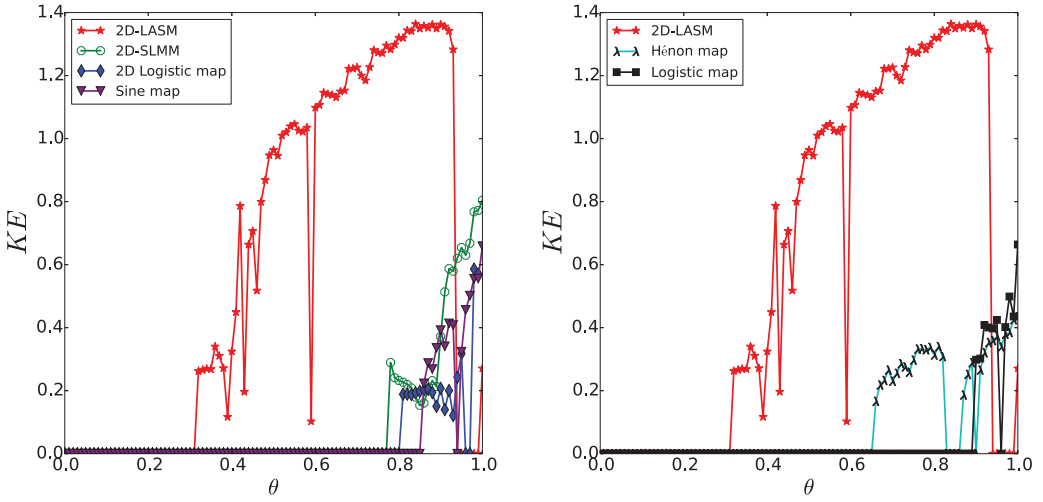

Fig. 4. KEs of different chaotic maps, where parameter θ denotes μ, α, $r - 0.2$, $a - 0.4$, p and s for 2D-LASM, 2D-SLMM, 2D Logistic map, Hénon map, Logistic map and Sine map, respectively.

chaotic behavior when $\beta = 3$ and $\alpha \in [0.87, 1]$; Hénon map has chaotic behavior when its parameters $b = 0.3$ and $a \in [1.06, 1.22] \cup [1.27, 1.29] \cup [1.31, 1.42]$; 2D-LASM has chaotic behavior when $\mu \in [0.37, 0.38] \cup [0.4, 0.42] \cup [0.44, 0.93] \cup \{1\}$. Therefore, 2D-LASM has a much wider chaotic range than other three 2D chaotic maps. In addition, 2D-LASM and 2D-SLMM have hyerchaotic behaviors when their corresponding parameters $\alpha \in [0.905, 1]$ and $\mu \in [0.44, 0.93]$. The hyperchaotic range of 2D-LASM is much larger than that of 2D-SLMM.

3.3. Kolmogorov entropy

Kolmogorov entropy (KE) is a kind of entropy that provides a quantitative explication of randomness of a signal [8]. It can be used to measure how much extra information is needed to predict trajectory of a dynamical system. Its mathematical definition is given as

$$KE = \lim_{\tau \to 0} \tau^{-1} \lim_{\varepsilon \to 0} \lim_{m \to \infty} K_{m,\tau}(\varepsilon), \tag{4}$$

where m is the embedding dimension,

$$K_{m,\tau}(\varepsilon) = - \sum_{i_1, i_2, \ldots, i_m \leqslant n(\varepsilon)} p(i_1, i_2, \ldots, i_m) \log p(i_1, i_2, \ldots, i_m),$$

where $p(i_1, i_2, \ldots, i_m)$ representees the joint probability of correctly predicting the trajectory in partition ϕ_{i_1} at time τ, in partition ϕ_{i_2} at time 2τ,..., in partition ϕ_{i_m} at time $m\tau$, and $\phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_m}$ are m nonoverlapping partitions in the phase plane.

A positive KE means that extra information is needed to predict the trajectory of a dynamical system. Thus, if a dynamical system has a positive KE, its outputs will be unpredictable, and a larger KE indicates better unpredictability. Our experiment uses the method proposed in [15] to calculate KEs. Fig. 4 depicts the KEs of different chaotic maps along their control parameters. To provide a visualized comparison, we shift the parameters of 2D Logistic map and Hénon map into the range

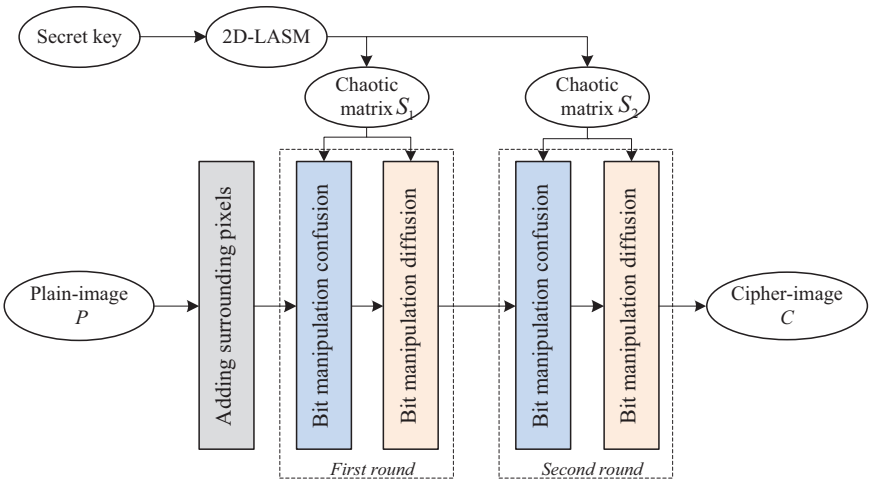

Fig. 5. The structure of LAS-IES.

of [0, 1]. Compared with other chaotic maps, 2D-LASM has a much wider chaotic range with positive KEs, and its positive KEs are much larger under most control parameters. Thus, the outputs of 2D-LASM are more unpredictable.

4. 2D-LASM-based image encryption scheme

Using 2D-LASM, this section further designs a new image encryption scheme, LAS-IES, whose secret key is used to set the initial states of 2D-LASM to generate chaotic matrices S_1 and S_2. Random values are first added to surroundings of the plain-image. Confusion and diffusion operations are then designed to randomly shuffle the pixel positions and change the pixel values, respectively. After two rounds of confusion and diffusion operations, a plain-image can be encrypted into an unrecognizable random-like cipher-image with a high security level. The overall structure of LAS-IES is shown in Fig. 5.

4.1. Secret key generation

To resist the brute-force attack, key space of a chaos-based encryption scheme should be larger than 2^{100} [1]. To satisfy this requirement and adapt to the structure of LAS-IES, we set the secret key as 232 bits, $K = \{x_0, y_0, \mu, w, \gamma_1, \gamma_2\}$. It consists of six parts, where γ_1, γ_2 are two interference strengths, (x_0, y_0, μ) are the original values, and w is the interference parameter. The generation procedures of initial states for 2D-LASM are shown in Algorithm 1, from which two groups of

Algorithm 1 The generation of initial states for 2D-LASM.

Input: Secret key K with length of 232 bits.
Output: Initial states (x_0^1, y_0^1, μ_1) and (x_0^2, y_0^2, μ_2).

$x_0 = (\sum_{i=1}^{52} K[i] \times 2^{i-1})/2^{52}$;
$y_0 = (\sum_{i=53}^{104} K[i] \times 2^{i-53})/2^{52}$;
$\mu = (\sum_{i=105}^{156} K[i] \times 2^{i-105})/2^{52}$;
$w = (\sum_{i=157}^{208} K[i] \times 2^{i-157})/2^{52}$;
$\gamma_1 = \sum_{i=209}^{220} K[i] \times 2^{i-209}$;
$\gamma_2 = \sum_{i=221}^{232} K[i] \times 2^{i-221}$;
for $i = 1$ to 2 **do**
  $x_0^i = (x_0 + w \times \gamma_i) \mod 1$;
  $y_0^i = (y_0 + w \times \gamma_i) \mod 1$;
  $\mu_i = ((\mu + w \times \gamma_i) \mod 0.4) + 0.5$;
  if $x_0^i = 0$ **then**
    $x_0^i = 0.4$;
  end if
  if $y_0^i = 0$ **then**
    $y_0^i = 0.4$;
  end if
end for

a

190	190	...	87	90
190	190	...	99	76
...	...	...	...	...
72	71	...	167	167
71	71	...	167	167

b

14	136	200	...	240	34	146
121	190	190	...	87	90	**4**
87	190	190	...	99	76	**42**
...	...	...	...	...	...	...
22	72	71	...	167	167	**59**
234	71	71	...	167	167	**40**
212	138	21	...	114	28	247

Fig. 6. An example of adding surrounding pixels: (a) plain-image P; (b) operation result.

initial states (x_0^1, y_0^1, μ_1) and (x_0^2, y_0^2, μ_2) are generated. For example, a randomly generated 232-bit secret key is shown as

$$K = AFE16E25A23D9D178D059526D0B5C63471429DB435794F8A359004B490.$$

According to Algorithm 1, we can obtain that $(x_0, y_0, \mu) = (0.60846485,\ 0.04450474,\ 0.85772949)$, $w = 0.03778565$, and $(\gamma_1, \gamma_2) = (3360, 146)$. Then the two groups of initial states can be generated, namely, $(x_0^1, y_0^1, \mu_1) = (0.56823603, 0.00427592, 0.71750067)$ and $(x_0^2, y_0^2, \mu_2) = (0.1251692, 0.56120908, 0.87443383)$.

Using the two groups of initial states, two chaotic matrices S_1 and S_2 can be generated by 2D-LASM. They are used to perform confusion and diffusion in the subsequent processes. It is noticed that elements of chaotic matrices S_1 and S_2 have the same representation format as the pixels in plain-image P and that the confusion and diffusion operations are manipulated in the bit level. The encrypted results always have the same representation format as the original images. Thus, LAS-IES can be applied to digital images of any representation format.

4.2. Adding surrounding pixels

Some random values are generated and added to surroundings of the plain-image. These values can influence all the pixels after the confusion and diffusion operations. Because these values are randomly generated and different in each encryption round, to encrypt a plain-image several times with the same secret key, the generated cipher-images are different from each other. With this significant property, LAS-IES can achieve good performance of resisting common security attacks, such as the chosen-plaintext and brute-force attacks.

If the plain-image P is with size $M \times N$, two random matrices, RI of size $2 \times (N+2)$ and CI of size $M \times 2$, are generated using a pseudo-random number generator. The elements of RI and CI have the same representation format as the pixels of P. Fig. 6 shows a numerical example of adding surrounding pixels for the 8-bit grayscale image, where

$$RI = \begin{pmatrix} 14 & 136 & 200 & \cdots & 240 & 34 & 146 \\ 212 & 138 & 21 & \cdots & 114 & 28 & 247 \end{pmatrix}_{2\times(N+2)},$$

$$CI = \begin{pmatrix} 121 & 87 & \cdots & 22 & 234 \\ 4 & 42 & \cdots & 59 & 40 \end{pmatrix}^T_{2\times M}.$$

Fig. 6(b) shows the operation result. As can be seen, the underlined values come from RI and the values of bold typeface belong to CI.

4.3. Bit manipulation confusion

The confusion property indicates that the distribution of outputs should be sensitively dependent on the secret key [43]. The bit manipulation confusion randomly shuffles the pixel positions within the image according to the chaotic matrix generated by 2D-LASM.

Suppose P is the adding surrounding pixel result and S is the generated chaotic matrix. Each of their elements is represented by p bits. The bit manipulation confusion is defined by

$$T = \mathcal{B}(P, S). \tag{5}$$

Algorithm 2 describes the detailed processes of bit manipulation confusion and Fig. 7 shows a numerical example. As can be seen in Fig. 7, I is the index matrix, whose elements are the index numbers of the corresponding pixels in P. S is the chaotic matrix generated by 2D-LASM. Its elements have the same representation format as the pixels in P. The

Algorithm 2 Bit manipulation confusion $T = \mathcal{B}(P, S)$.

Input: Image P and chaotic matrix S. They are of size $Q \times W$ and their elements are represented by p bits.
Output: Bit manipulation confusion result T.

```
Initial a matrix R of size Q × W;
q = ⌈log2(QW)⌉;
for i = 1 to Q do
    for j = 1 to W do
        t = (i − 1)W + j;
        tb = Bin(t, q); {Bin(x, n) transforms the integer number x into n bits.}
        R_{i,j} = Joint(S_{i,j}, tb, P_{i,j}); {Joint(x1, x2, x3) joints the 3 binary sequences x1, x2, x3 into one binary sequence by order.}
    end for
end for
R = SortR(R); {SortR(X) sorts the matrix X along horizontal direction.}
R = SortC(R); {SortC(X) sorts the matrix X along vertical direction.}
T = FetEnd(R_{1:Q,1:W}, p); {FetEnd(x, n) fetches the last n bits from the binary sequence x.}
```

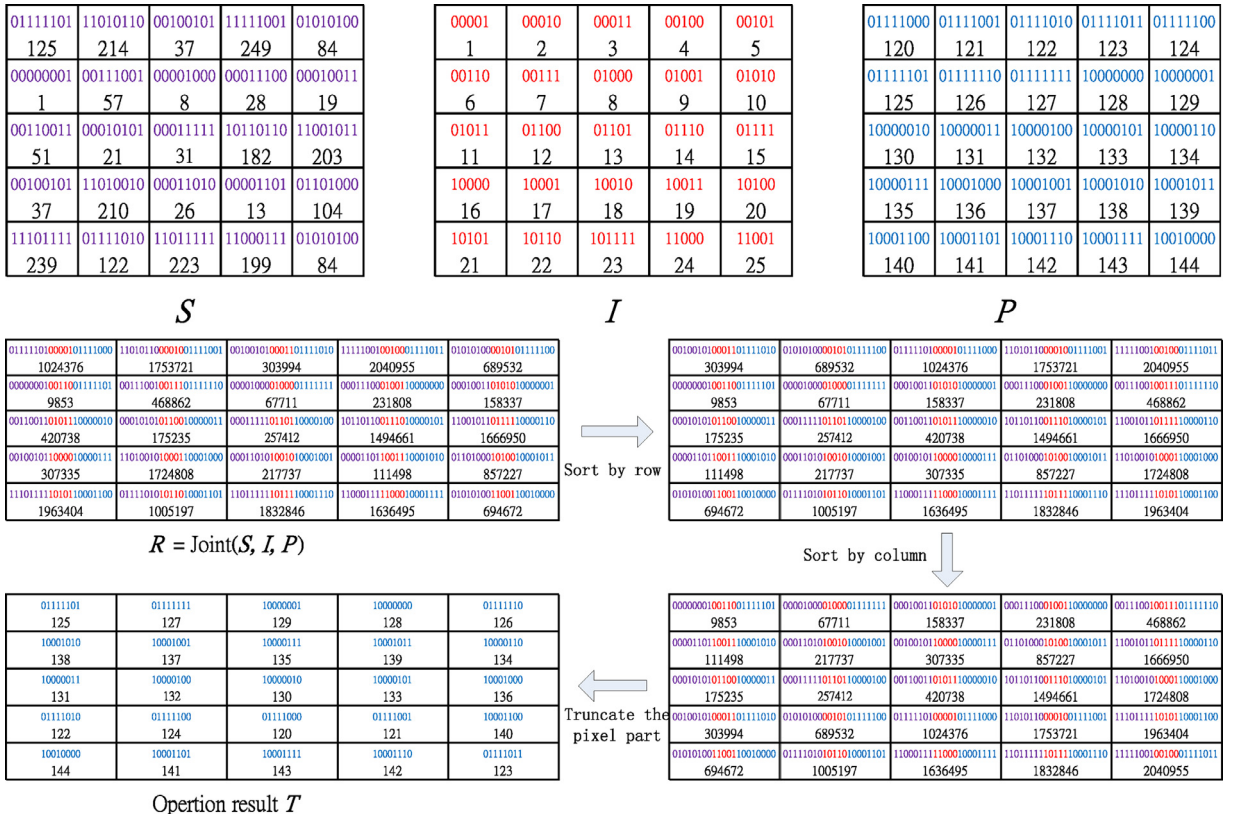

Fig. 7. A numerical example of bit manipulation confusion.

binary streams from S are placed in the most significant bit positions. Thus, S dominates the change of positions. In the bit manipulation confusion, a pixel can be permutated to any position of the image. From Fig. 7, we can observe that the pixels in the operation result are sufficiently shuffled after one-time bit manipulation confusion.

4.4. Bit manipulation diffusion

The diffusion property demonstrates that the ciphertext should be extremely sensitive to change of the plaintext, which means that one bit change in the plaintext can cause each bit in the ciphertext be changed with a probability of 50% [43]. LAS-IES uses the previous pixel and an element of the chaotic matrix S to change the current pixel. After two rounds of operations, the change in one pixel can be spread all over the entire image. Suppose the chaotic matrix S and bit manipulation

confusion result T are of size $Q \times W$, the bit manipulation diffusion is defined as

$$O_{i,j} = \begin{cases} T_{i,j} \oplus T_{Q,W} \oplus S_{i,j}, & \text{for } i = 1, j = 1; \\ T_{i,j} \oplus O_{i-1,W} \oplus S_{i,j}, & \text{for } i \neq 1, j = 1; \\ T_{i,j} \oplus O_{i,j-1} \oplus S_{i,j}, & \text{for } j \neq 1, \end{cases} \tag{6}$$

where O is the bit manipulation diffusion result, $\oplus$ is the bitwise XOR operation. The decryption process of this part is to do the inverse operation, which is defined as

$$T_{i,j} = \begin{cases} O_{i,j} \oplus O_{i,j-1} \oplus S_{i,j}, & \text{for } j \neq 1; \\ O_{i,j} \oplus O_{i-1,W} \oplus S_{i,j}, & \text{for } i \neq 1, j = 1; \\ O_{i,j} \oplus T_{Q,W} \oplus S_{i,j}, & \text{for } i = 1, j = 1. \end{cases} \tag{7}$$

After performing two rounds of bit manipulation confusion and diffusion using two different chaotic matrices, a plain-image can be encrypted into an unrecognizable cipher-image.

4.5. Discussion

Because 2D-LASM has complex chaotic behavior, random values are added to surroundings of the plain-image, and the principle of confusion and diffusion are strictly followed, LAS-IES has the following advantages:

(1) It can efficiently resist the common security attacks, including chosen-plaintext attack, differential attack, and statistic attack. This is because, using the same secret key to encrypt a plain-image several times, the obtained cipher-images are random-like and totally different from each other.
(2) It can achieve good diffusion and confusion properties since the principle of diffusion and confusion are fulfilled.
(3) It can achieve a fast encryption/decryption speed, as LAS-IES uses only two rounds of confusion and diffusion operations in the bit level.
(4) It has good reliability of resisting noise or data loss attack. When a cipher-image has noise or losses some data, LAS-IES can still recover the original image with a high visual quality.

5. Simulation results and reliability

An image encryption scheme should have ability to encrypt different kinds of digital images into random-like cipher-images. Only with the correct key, a cipher-image can be correctly decrypted. This section provides the simulation results of LAS-IES and discusses its reliability.

5.1. Simulation results

Here, we use Python programming language to implement LAS-IES and apply it to different types of digital images. Fig. 8 shows the simulation results of one binary image and one grayscale image. Fig. 9 presents the simulation results of an RGB color image. From Fig. 8, we can see that LAS-IES can encrypt images into random-like cipher-images with a uniform distribution. Using the correct key, it can also completely reconstruct the original images. As shown in Fig. 9, the histograms of the original color image have many patterns in every color channel, but the histograms of cipher-image distribute randomly. Attackers have difficulty to obtain any information by statistical methods.

When simulating LAS-IES in the computer with Intel(R) Core(TM)i7-4770 CPU @ 3.4 GHz, the actual average encryption time is 0.8342 ± 0.050733s for 6 grayscale images of size 256×256. Thus, the encryption speed of LAS-IES is about 0.5994 Mb/s (Megabit/second). As each operation in the encryption process has the same time complexity for different secret keys, LAS-IES is robust against the timing attack.

5.2. Reliability of resisting noise and data loss

When digital images are transmitted through networks, analog-to-digital convert errors or bit errors may happen. These may change values of some image pixels and blur them [4]. Besides, digital images may also loss data if they are corrupted due to intrusion. Because the bit manipulation diffusion operation is asymmetric, LAS-IES has the ability of resisting noise or data loss. This means that when a cipher-image is blurred or losses some data, LAS-IES can still recover the original image without significantly decreasing its visual quality. In the encryption process, random values are added to surroundings of the plain-image in each encryption and these values can be spread over all the cipher-image after two rounds of operations. However, in the decryption process, the change of one pixel in the cipher-image can affect only two pixels, and can further affect at most four pixels after two rounds of operations. By this principle, if a portion of pixels in the cipher-image are lost, the original image can still be reconstructed with a high visual quality. Fig. 10 shows the straightforward asymmetry of the bit manipulation diffusion in Eq. (6) and its inverse operation in Eq. (7), where S is the chaotic sequence, T denotes the input and output, and Q represents the output and input in the bit manipulation diffusion its inverse operation.

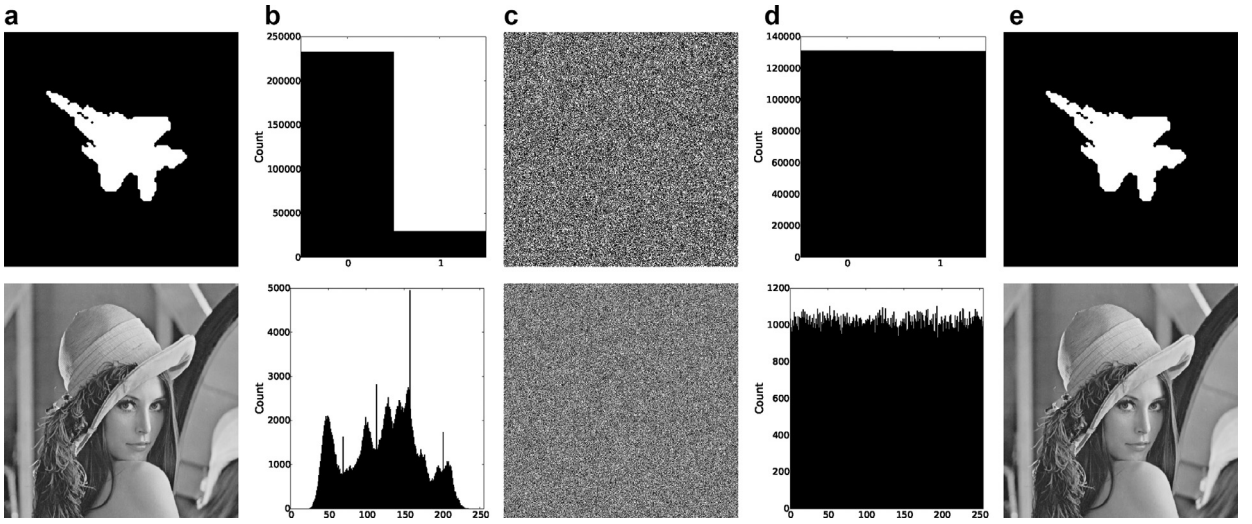

Fig. 8. Simulation results of LAS-IES. The top and bottom rows are the simulation procedures of binary and grayscale images, respectively: (a) plain-images; (b) histograms of (a); (c) cipher-images; (d) histograms of (c); (e) decrypted results.

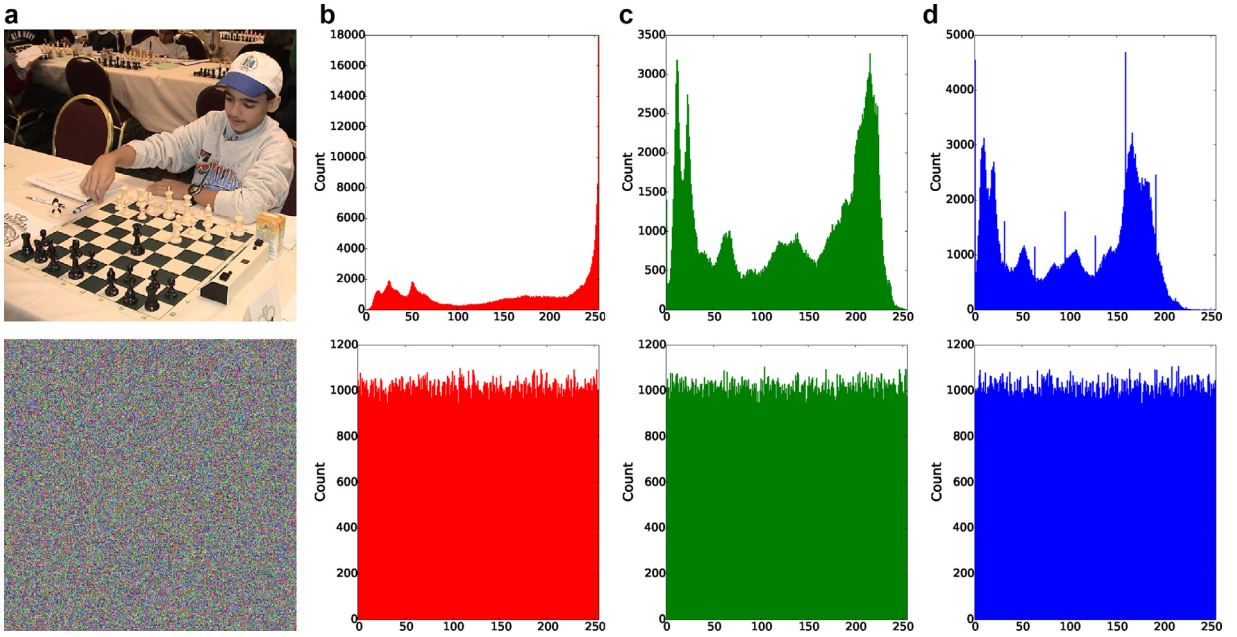

Fig. 9. Simulation results of LAS-IES for color image: (a) color image and its encrypted one; (b)–(d) histograms of (a) the red, green and blue components, respectively. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

Fig. 11 shows the experimental results of noise and data loss attacks to the cipher-images. When the cipher-images suffer from different kinds of data loss and the numbers of changed pixels are approximately the same, the decrypted images have similar visual quality, which can be seen from Fig. 11(b)–(d). When the data loss happened in the frequency domain, the changes can spread over to more pixels in the corresponding spatial domain. Then, the decrypted image has a lot of noise with a quite low visual quality, which can be observed from Fig. 11(e). If a large portion of pixels in the cipher-image are lost, e.g., 90.1% pixels are lost, the decrypted image is noise-like, which can be seen from Fig. 11(f).

6. Security analysis

To study the security level of LAS-IES, this section analyzes performance of its secret key and investigates its ability of resisting some common security attacks. The test binary images are selected from the MPEG7 CE Shape-1 Part B image dataset and the test grayscale images are obtained from the USC-SIPI 'Miscellaneous' image dataset. To show the

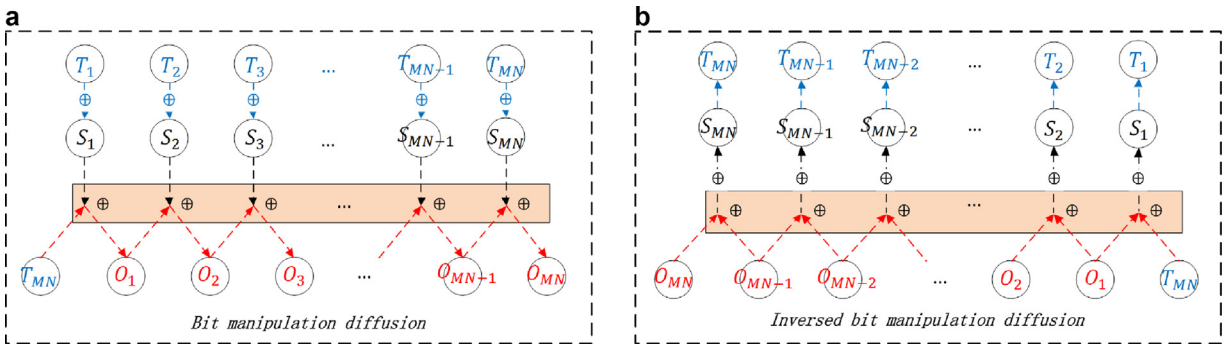

Fig. 10. The straightforward asymmetry of bit manipulation diffusion: (a) the bit manipulation diffusion in Eq. (6); (b) the inverse bit manipulation diffusion in Eq. (7).

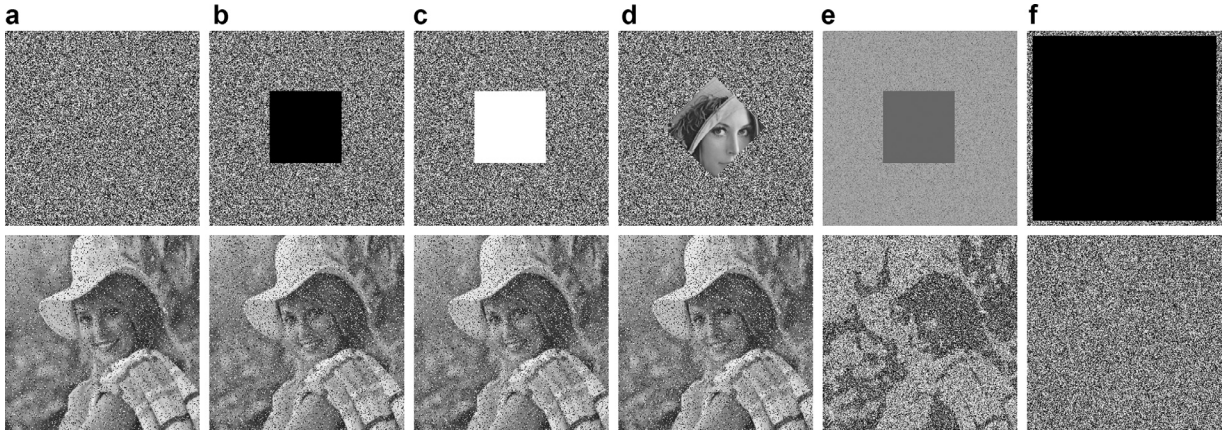

Fig. 11. Reliability analysis results of LAS-IES. The first row shows the cipher-images with noise and different kinds of data loss, and the second row shows their corresponding decrypted images: (a) 5% Saltand Pepper noise; (b) 13.56% data loss; (c) 13.56% data loss with a white square; (d) 13.56% data modification with a rotated square; (e) 13.56% data loss in the frequency domain; (f) 90.1% data loss.

advantages of LAS-IES, we also compare it with several state-of-the-art image encryption schemes. Among the reference papers [5,13,19,24,38,39,41,50], some reported simulation results and some provided source codes. To provide a relatively fair comparison, we use the following rules:

(1) If the simulation results were reported, we directly referenced the results;
(2) If the simulation results were not reported and the source codes were provided, we directly ran their source codes on the test images;
(3) If neither the simulation results nor the source codes are available, we implemented the schemes to obtain the test results.

6.1. Secret key

First, the secret key should have a large enough key space to resist brute-force attack. As discussed in Section 4.1, the secret key of 232 bits is large enough to satisfy the size requirement of key space. On the other hand, the secret key should be sensitive in the encryption and decryption processes. This means that even one bit difference of two secret keys result in totally different cipher-images in the encryption process and generate totally different decrypted images in the decryption process.

Figs. 12 and 13 show the key sensitivity analysis in the encryption and decryption processes, respectively. K_2 and K_3 are two secret keys that have one bit difference with K_1, where

$$K_1 = AFE16E25A23D9D178D059526D0B5C63471429DB435794F8A359004B490,$$
$$K_2 = AFE16E25A23D9D178D059526D0B5C63471429DB435794F8A359004B491,$$
$$K_3 = AFE16E25A23D9D178D059526D0B5C63471429DB435794F8A359004B492.$$

As shown in Fig. 12, when the plain-image is encrypted with K_1, K_2 and K_3, respectively, the obtained cipher-images are totally different. Fig. 13 demonstrates that the cipher-image can be completely reconstructed only by the correct secret key,

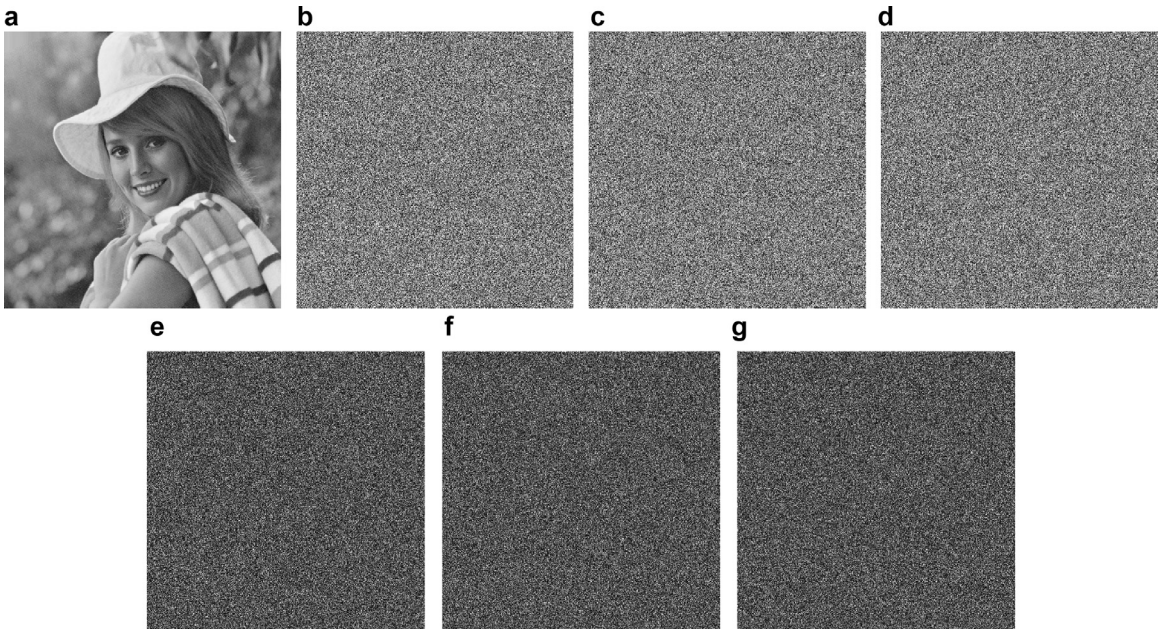

Fig. 12. Key sensitivity analysis in the encryption process: (a) plain-image P; (b) $C_1 = \mathrm{Enc}(P, K_1)$; (c) $C_2 = \mathrm{Enc}(P, K_2)$; (d) $C_3 = \mathrm{Enc}(P, K_3)$; (e) $|C_1 - C_2|$; (f) $|C_1 - C_3|$; (g) $|C_2 - C_3|$.

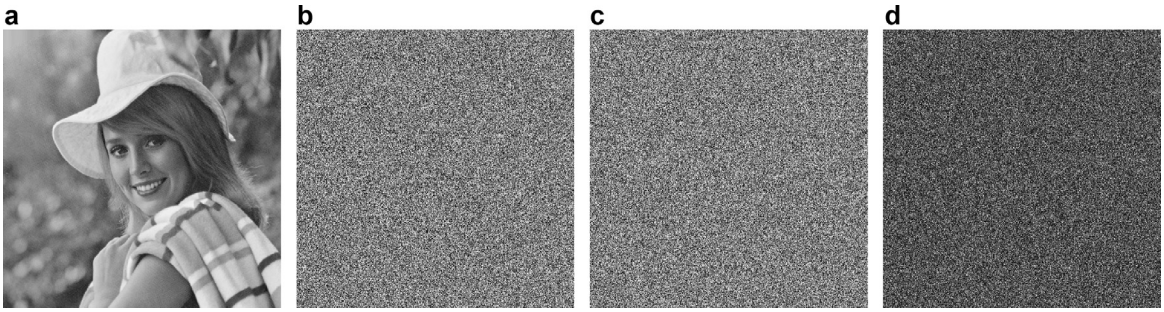

Fig. 13. Key sensitivity analysis in the decryption process: (a) $D_1 = \mathrm{Dec}(C_1, K_1)$; (b) $D_2 = \mathrm{Dec}(C_1, K_2)$; (c) $D_3 = \mathrm{Dec}(C_1, K_3)$; (d) $|D_2 - D_3|$, where C_1 is the cipher-image in Fig. 12(b).

little difference in the secret keys yields totally different decrypted images, which can be seen from Fig. 13(d). Thus, LAS-IES is highly sensitive to change of its secret key.

6.2. Ability of resisting chosen-plaintext and chosen-ciphtertext attacks

The chosen-plaintext and chosen-ciphertext attacks are two efficient and widely used security attack models in cryptanalysis. The former assumes that the attackers have the ability to choose arbitrary plaintexts and obtain the corresponding ciphertexts, while the latter indicates that the attackers can choose any ciphertext and obtain its decrypted result thought some ways [46]. By choosing the known plaintexts to encrypt and analyzing the corresponding ciphertexts in the chosen-plaintext attack, or collecting the interested ciphertexts and obtaining the corresponding decrypted results in the chosen-ciphertext attack, the attackers can disclose the relation between the plaintexts and ciphertexts, and even deduce the secret key if the encryption structure is not sufficiently secure. Many successful cryptanalysis cases using the chosen-plaintext or chosen-ciphertext attack were reported in [22,23,30].

In LAS-IES, special structures are designed to resist the chosen-plaintext and chosen-ciphertext attacks: (1) random values are added to surroundings of the plain-images. As a result, the obtained cipher-images are totally different from each other even using the same secret key to encrypt a plain-image several times; (2) the principle of confusion and diffusion introduced by Shannon in [31] are fulfilled. A pixel in the plain-image can be permuted to any position and a small change can be spread over all pixels in the cipher-image.

Table 1
NPCR/UACI results of binary images for LAS-IES.

File name	NPCR/UACI (%)	File name	NPCR/UACI (%)
Bone-16	50.0938	horse-1	50.0336
camel-11	50.0660	horse-10	50.1875
classic-1	49.8290	Misk-1	50.1791
cup-11	50.1729	octopus-1	49.6079
device4-20	49.9429	**Mean**	**50.0008**
hammer-20	49.8948	**Std**	**0.001852**

6.3. Ability of resisting differential attack

The differential attack is to study how the difference in inputs can affect that of the corresponding outputs [41]. It is a general form of cryptanalysis and a secure encryption scheme should have strong ability of resisting this attack. For an image encryption scheme, its ability of resisting differential attack can be measured by the number of pixel changing rate (NPCR) and unified average changed intensity (UACI). For a plain-image P, randomly change one bit of a pixel and obtaining another plaintext image P_2. Let C_1 and C_2 denote two cipher-images encrypted from P and P_2, respectively. Then, NPCR and UACI are defined by

$$\mathrm{NPCR}(C_1, C_2) = \sum_{i,j} \frac{A(i,j)}{G} \times 100\%, \tag{8}$$

and

$$\mathrm{UACI}(C_1, C_2) = \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{(L-1) \times G} \times 100\%, \tag{9}$$

respectively, where G denotes the total number of pixels, L is the grayscale level of the image, and

$$A(i,j) = \begin{cases} 0, & \text{if } C_1(i,j) = C_2(i,j), \\ 1, & \text{if } C_1(i,j) \neq C_2(i,j). \end{cases}$$

Recently, the expected NPCR and UACI scores of resisting differential attack were provided in [12], which are given by

$$\mathrm{NPCR}_{expected} = \left(1 - \frac{1}{2^{\log_2^L}}\right) \times 100\%, \tag{10}$$

and

$$\mathrm{UACI}_{expected} = \frac{1}{L^2}\left(\frac{\sum_{i=1}^{(L-1)} i(i+1)}{L-1}\right) \times 100\%, \tag{11}$$

respectively. From Eqs. (10) and (11), we can observe that the expected scores of NPCR and UACI are dependent on the grayscale value L. When the test image is a binary image, namely $L = 2$, we have $\mathrm{NPCR}_{expected} = \mathrm{UACI}_{expected} = 50\%$. When the test image is a 8-bit grayscale image, namely $L = 256$, we can get $\mathrm{NPCR}_{expected} = 99.6094\%$ and $\mathrm{UACI}_{expected} = 33.4635\%$.

For a binary image, the NPCR and UACI values are the same, which can be seen from their definitions in Eqs. (8) and (9). Table 1 shows the NPCR/UACI results of 10 binary images selected from the MPEG7 CE Shape-1 Part B image dataset, all the NPCR/UACI results are quite close to the expected score, 50%. For the 8-bit grayscale images chosen from the USC-SIPI 'Miscellaneous' image dataset, their NPCR and UACI scores for different image encryption schemes are listed in Tables 2 and 3, respectively. In our experiments, we directly referred to the simulation results of the schemes in [39,50], and implemented other schemes to calculate their scores of NPCR and UACI. Among all the six image encryption schemes, LAS-IES achieves the closest average scores of NPCR and UACI to the expected ones. Thus, we can conclude that LAS-IES has good ability of resisting differential attack.

6.4. Randomness test

For a cipher-image with ideal security performance, its pixel values are expected to be uniformly distributed to achieve high randomness. The randomness of an image can be measured by the local Shannon entropy (LocSE) [42]. It tests the randomness of an image from the local viewpoint. By randomly choosing k non-overlapping image blocks with T_B pixels from an image, the LocSE value is defined as

$$\overline{H_{k,T_B}} = \sum_{i=1}^{k} \frac{H(S_i)}{k}, \tag{12}$$

Table 2
NPCR scores of 8-bit grayscale images for different image encryption schemes.

File name	Wu et al. [39]	Zhou et al. [50]	Wu et al. [38]	Liao et al. [24]	Hua's [19]	LAS-IES
5.1.09	99.5804	99.60	99.6094	49.8093	99.6658	99.6064
5.1.10	99.5865	99.61	99.5956	99.6140	99.6475	99.6154
5.1.11	99.5972	99.64	99.6109	49.8138	99.6674	99.6244
5.1.12	99.6201	99.60	99.6063	49.8280	99.5941	99.5703
5.1.13	99.6414	99.63	99.6140	99.5972	99.6445	99.6109
5.1.14	99.5773	99.62	99.6582	99.6368	99.5975	99.6364
5.2.08	99.6300	99.61	99.6101	99.6208	99.6281	99.5870
5.2.09	99.6346	99.60	99.6019	99.6174	99.6197	99.6260
5.2.10	99.6178	99.61	99.5979	99.6292	99.6288	99.6124
7.1.01	99.5861	99.59	99.5842	49.8005	99.6273	99.5992
7.1.02	99.6178	99.62	99.6117	49.8039	99.5892	99.6075
7.1.03	99.6117	99.59	99.6201	49.8096	99.6201	99.6079
7.1.04	99.5808	99.62	99.6201	99.6094	99.5894	99.5988
7.1.05	99.5998	99.61	99.6185	99.6063	99.6185	99.6170
7.1.06	99.6006	99.61	99.6346	99.6048	99.6117	99.6272
7.1.07	99.6059	99.60	99.5926	99.6323	99.6223	99.5931
7.1.08	99.5918	99.58	99.6223	99.6101	99.6151	99.6094
7.1.09	99.6010	99.61	99.6166	49.8100	99.6044	99.6162
7.1.10	99.6002	99.63	99.6086	49.8199	99.6101	99.6045
boat.512	99.6037	99.61	99.5800	99.6037	99.6006	99.6154
elaine.512	99.6082	99.60	99.6128	99.6292	99.6128	99.6196
gray21.512	99.6075	99.61	99.6235	99.6254	99.6082	99.6022
numbers.512	99.5995	99.60	99.6021	99.6120	99.6059	99.6141
ruler.512	99.6147	99.61	99.6132	99.6304	99.6265	99.6120
5.3.01	99.6058	99.60	99.6118	49.8086	99.6098	99.5931
5.3.02	99.6005	99.62	99.5996	99.6163	99.6119	99.6128
7.2.01	99.6073	99.61	99.6099	49.8199	99.6156	99.6156
testpat.1k	99.6117	99.62	99.6069	99.6108	99.6124	99.6072
Mean	99.604996	99.609288	99.610478	81.819565	99.618043	**99.609356**
Std	0.015657	0.013032	0.015031	24.302271	0.019578	**0.013320**

Table 3
UACI scores of 8-bit grayscale images for different image encryption schemes.

File name	Wu et al. [39]	Zhou et al. [50]	Wu et al. [38]	Liao et al. [24]	Hua et al. [19]	LAS-IES
5.1.09	33.5253	33.14	33.5096	16.6687	33.5980	33.4456
5.1.10	33.3938	33.24	33.5587	33.5374	33.5366	33.4946
5.1.11	33.8600	33.24	33.4315	16.7015	33.4398	33.5541
5.1.12	33.6150	33.56	33.5379	17.0621	33.4228	33.4302
5.1.13	33.7250	33.56	33.6163	33.6419	33.4205	33.4438
5.1.14	33.4491	33.21	33.4617	34.2965	33.4696	33.4655
5.2.08	33.3933	33.31	33.4323	33.4267	33.4720	33.4008
5.2.09	33.5346	33.62	33.3405	33.4553	33.4921	33.4804
5.2.10	33.5265	33.31	33.4687	33.4993	33.4914	33.4563
7.1.01	33.4789	33.25	33.5444	16.8228	33.5212	33.5037
7.1.02	33.5416	33.27	33.4910	16.8126	33.4846	33.4237
7.1.03	33.4062	33.27	33.5553	16.7308	33.4647	33.4291
7.1.04	33.4845	33.21	33.4806	33.4778	33.5202	33.4739
7.1.05	33.4852	33.30	33.3965	33.4581	33.5400	33.4362
7.1.06	33.4453	33.30	33.5651	33.4489	33.5254	33.3954
7.1.07	33.4535	33.15	33.4363	33.5216	33.5205	33.4073
7.1.08	33.4760	33.26	33.4769	33.4496	33.5678	33.4332
7.1.09	33.4875	33.26	33.4085	16.7680	33.5223	33.4177
7.1.10	33.4754	33.23	33.5247	16.8557	33.4325	33.4344
boat.512	33.4994	33.42	33.4900	33.6291	33.5097	33.4654
elaine.512	33.4355	33.37	33.4439	33.4419	33.5477	33.4225
gray21.512	33.3743	33.37	33.4664	33.4770	33.3930	33.4608
numbers.512	33.4150	33.36	33.5378	33.4503	33.3993	33.4240
ruler.512	33.3807	33.43	33.4166	34.0635	33.5129	33.4262
5.3.01	33.4714	33.42	33.4498	49.8086	33.4532	33.4585
5.3.02	33.4640	33.29	33.4790	99.6163	33.4853	33.4605
7.2.01	33.4917	33.59	33.4762	33.4685	33.4965	33.4556
testpat.1k	33.5025	33.43	33.4467	33.4786	33.4455	33.4347
Mean	33.492543	33.334643	33.480104	28.177253	33.488754	**33.447648**
Std	0.102056	0.128855	0.061160	7.972915	0.050670	**0.033718**

Table 4
LocSEs of binary images and their encrypted ones generated by LAS-IES.

File name	Plain-images	Cipher-images	File name	Plain-images	Cipher-images
Bone-16	0.000000	0.466667	horse-1	0.000000	0.533333
camel-11	0.000000	0.533333	horse-10	0.000000	0.466667
classic-1	0.033333	0.466667	Misk-1	0.000000	0.500000
cup-11	0.033333	0.466667	octopus-1	0.000000	0.533333
device4-20	0.000000	0.666667	**Pass rate**		**9/10**
hammer-20	0.166667	0.466667	**Mean**		**0.510000**
			Std		**0.062952**

Table 5
LocSEs of 8-bit grayscale images and their encrypted ones generated by different image encryption algorithms. $(k, T_B, \alpha) = (30, 1936, 0.001)$.

File name	Plain-images	Cipher-images					
		Wu et al. [39]	Zhou et al. [50]	Wu et al. [38]	Liao et al. [24]	Hua et al. [19]	LAS-IES
5.1.09	5.948253	*7.901985*	7.903354	7.903764	7.904191	7.902127	7.902521
5.1.10	7.009960	7.902731	7.902443	7.901801	7.902371	7.903402	7.902215
5.1.11	4.913895	7.902446	7.902756	7.903306	7.900799	7.902687	7.901470
5.1.12	5.181903	7.902556	7.901526	7.904478	7.903374	7.901906	7.904045
5.1.13	1.403060	7.902688	7.904563	7.904657	7.904566	7.902825	7.902184
5.1.14	6.737685	7.903474	7.902954	7.902874	7.903111	7.902340	7.905557
5.2.08	5.818099	7.903953	7.902356	7.903218	7.901762	7.903327	7.903328
5.2.09	6.384914	7.902233	7.899853	7.903089	7.905854	7.901765	7.902551
5.2.10	4.904788	7.900714	7.902654	7.902077	7.902768	7.902748	7.902888
7.1.01	5.432175	7.902173	7.902634	7.901965	7.902145	7.901305	7.902014
7.1.02	2.384175	7.900879	7.901634	7.904970	7.902157	7.901578	7.902254
7.1.03	4.848621	7.902543	7.905423	7.891503	7.900645	7.903099	7.903894
7.1.04	5.193038	7.901126	7.902125	7.903399	7.904141	7.902607	7.902539
7.1.05	5.966493	7.903579	7.883653	7.901301	7.900027	7.905305	7.902851
7.1.06	6.018822	7.901930	7.902356	7.903367	7.901736	7.902695	7.901960
7.1.07	5.625370	7.903000	7.902364	7.899556	7.900802	7.902896	7.901658
7.1.08	4.405719	7.903197	7.904456	7.883531	7.900944	7.901632	7.902129
7.1.09	5.446080	7.902308	7.903012	7.903201	7.905658	7.903173	7.903018
7.1.10	5.307269	7.899542	7.901598	7.901542	7.893848	7.901524	7.901114
boat.512	6.255248	7.901908	7.901879	7.903091	7.900712	7.903088	7.902407
elaine.512	6.104411	7.901122	7.902989	7.901859	7.902030	7.901720	7.901703
gray21.512	0.376627	7.900170	7.905107	7.901832	7.902149	7.902688	7.901959
numbers.512	5.947982	7.903615	7.892351	7.902144	7.903579	7.901657	7.901664
ruler.512	0.492257	7.903265	7.903001	7.901937	7.901428	7.903052	7.901596
5.3.01	5.680905	7.902727	7.902647	7.902108	7.901040	7.901772	7.902751
5.3.02	5.689569	7.903182	7.910474	7.904169	7.900981	7.903328	7.901552
7.2.01	4.857594	7.902772	7.901989	7.904945	7.904525	7.902454	7.902452
testpat.1k	1.255093	7.902806	7.901681	7.903856	7.903343	7.902752	7.902663
Pass rate		18/28	20/28	17/28	11/28	26/28	**23/28**
Mean		7.902308	7.901923	7.901769	7.902167	7.902488	**7.902462**
Std		0.001080	0.004508	0.004347	0.002263	0.000079	**0.000921**

where $S_1, S_2, \ldots, S_k$ are k chosen image blocks and $H(S_i)$ is the Shannon entropy of S_i. The Shannon entropy of image X is defined by

$$H(X) = -\sum_{i=1}^{L} \Pr(x_i) \log_2 \Pr(x_i),$$

where x_i represents the ith possible value in X, $\Pr(x_i)$ is the probability of x_i, and L denotes the grayscale level.

An image can pass the LocSE test if $\overline{H_{k,T_B}}$ falls into an interval of $(h^*_{left}, h^*_{right})$. Following the recommendation given in [42], our experiment sets the parameters $(k, T_B, \alpha) = (30, 2, 0.001)$ for the binary images and $(k, T_B, \alpha) = (30, 1936, 0.001)$ for 8-bit grayscale images. Then, the critical values $(h^*_{left}, h^*_{right}) = (0.445157888, 0.554842112)$ and the ideal LocSE is 0.5 for binary images; $(h^*_{left}, h^*_{right}) = (7.901515698, 7.903422936)$ and the ideal LocSE is 7.902469317 for 8-bit grayscale images. We tested 10 binary images selected from the MPEG7 CE Shape-1 Part B image dataset and 28 grayscale images obtained from the USC-SIPI 'Miscellaneous' image dataset. Table 4 shows the LocSE results of the 10 binary images for LAS-IES, demonstrating that 9 cipher-images encrypted by LAS-IES can pass the test and the average LocSE is close to the ideal one. For the 8-bit grayscale images, the LocSEs of their cipher-images encrypted by different image encryption schemes are listed in Table 5. As can be seen, 23 cipher-images encrypted by LAS-IES can pass the test and LAS-IES has the second-best pass rate and outperforms four schemes given in [24,38,39,50]. Moreover, LAS-IES can achieve LocSEs of average 7.902462, which

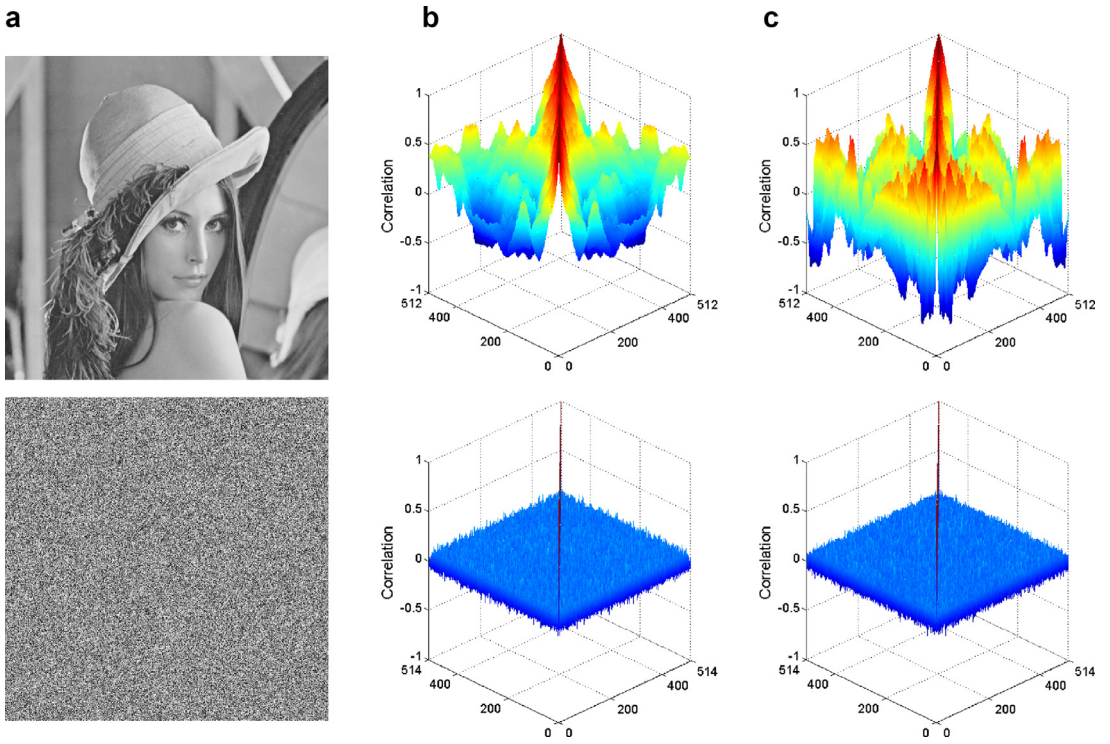

Fig. 14. Visualized correlation results: (a) the plain-image "Lena" and its cipher-image encrypted by LAS-IES; (b) the correlation between row pixels of (a); (c) the correlation between column pixels of (a).

Table 6
AC results of the plain-image "Lena" and its cipher-images encrypted by different image encryption schemes.

	Horizontal	Vertical	Diagonal
Plain-image "Lena"	0.9400	0.9709	0.9710
Image encryption schemes			
Chen et al. [5]	0.00024	0.24251	0.23644
Liao et al. [24]	0.0127	0.0190	0.0012
Fu et al. [13]	0.0368	0.0392	0.0068
Wu et al. [39]	0.0002150	0.0014913	0.0040264
Zhou et al. [50]	0.0054	0.0045	0.0031
Wu et al. [41]	0.0053365	0.0027616	0.0016621
LAS-IES	**0.0013174**	**0.0006427**	**0.0019122**

approaches the ideal LocSE mostly close. These mean that LAS-IES can encrypt different kinds of images into random-like cipher-images with high randomness.

6.5. Auto-correlation analysis

The adjacent pixels in a natural image may have strong correlation. However, the pixels in a cipher-image with high security level is expected to be randomly distributed. Therefore, an image encryption scheme should have ability to efficiently reduce the correlation among adjacent pixels. The correlation between adjacent pixels can be measured by the auto-correlation coefficient (AC), which is defined as

$$AC = \frac{E[(y_t - E[Y_t])(y_{t+1} - E[Y_t])]}{\sigma^2}, \tag{13}$$

where Y_t is a pixel sequence of the image, Y_{t+1} is another pixel sequence, in which each pixel is the adjacent pixel of Y_t along the horizontal, vertical or diagonal direction, $E[\cdot]$ is the mathematical expectation, and σ is the standard derivation of Y_t,

$$\sigma = \sqrt{E[(y_t - E[Y_t])^2]}.$$

From Eq. (13), we can observe that the AC value falls into the range of $[-1, 1]$ and a small absolute AC value means a weak correlation between two sequences.

Table 6 lists the AC values of the plain-image "Lena" and its cipher-images encrypted by different image encryption schemes. LAS-IES has smaller absolute AC values than the schemes proposed in [13,50] in all three directions, and outperforms other schemes given in [5,24,39,41] in two directions. Fig. 14 depicts the visualized correlation results of the plain-image "Lena" and its cipher-image encrypted by LAS-IES. In the Fig. 14(b) and (c) plot the correlation values between pixel pairs in the row and column directions, respectively. The correlation between different rows and columns are quite strong in the plain-image but quite weak in the cipher-image. Thus, LAS-IES can efficiently reduce the strong correlation between adjacent pixels.

7. Conclusion

This paper designed a new 2D chaotic map, called 2D-LASM. It is generated using the output of the Logistic map to adjust the input of the Sine map, and then extending the phase plane from 1D to 2D. Various objective evaluation methods, including trajectory, LE and KE, were provided to show that 2D-LASM has better ergodicity, a wider chaotic range, and is more unpredictable than several existing 1D and 2D chaotic maps. Using 2D-LASM, this paper further proposed a novel image encryption scheme, called LAS-IES. It contains three main components, namely, adding surrounding pixels, bit manipulation confusion, and bit manipulation diffusion. The adding surrounding pixels is to add random values to the plain-image to ensure that each encrypted result is different. Multiple rounds of confusion and diffusion are performed in the bit level to fulfill the principle of confusion and diffusion. Simulation results and security analysis showed that LAS-IES can encrypt different types of images into random-like cipher-images of high security levels.

Acknowledgment

This work was supported in part by the Macau Science and Technology Development Fund under Grant FDCT/016/2015/A1 and by the Research Committee at University of Macau under Grants MYRG2014-00003-FST, MYRG113 (Y1-L3)-FST12-ZYC and MRG001/ZYC/2013/FST.

References

[1] G. Alvarez, S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, Int. J. Bifurc. Chaos 16 (8) (2006) 2129–2151.
[2] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, V. Fernandez, On the security of a new image encryption scheme based on chaotic map lattices, Chaos Interdiscip. J. Nonlinear Sci. 18 (3) (2008) 033112.
[3] L. Bao, Y. Zhou, Image encryption: Generating visually meaningful encrypted images, Inf. Sci. 324 (2015) 197–207.
[4] A.C. Bovik, Handbook of Image and Video Processing, Academic press, 2010.
[5] G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos Solitons Fractals 21 (3) (2004) 749–761.
[6] S. Chen, J. Lü, Parameters identification and synchronization of chaotic systems based upon adaptive control, Phys. Lett. A 299 (4) (2002) 353–358.
[7] A.-V. Diaconu, K. Loukhaoukha, An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher, Math. Probl. Eng. 2013 (2013) Art. ID 848392.
[8] P. Faure, H. Korn, A new method to estimate the Kolmogorov entropy from recurrence plots: its application to neuronal signals, Phys. D Nonlinear Phenom. 122 (14) (1998) 265–279.
[9] FIPS PUB 197, Advanced encryption standard (AES), 2001.
[10] FIPS PUB 46, Data encryption standard (DES), 1999.
[11] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurc. Chaos 8 (6) (1998) 1259–1284.
[12] C. Fu, J. Chen, H. Zou, W. Meng, Y. Zhan, Y. Yu, A chaos-based digital image encryption scheme with an improved diffusion strategy, Opt. Express 20 (3) (2012) 2363–2378.
[13] 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 (23) (2011) 5415–5423.
[14] J.A. Gallas, Structure of the parameter space of the Hénon map, Phys. Rev. Lett. 70 (18) (1993) 2714.
[15] P. Grassberger, I. Procaccia, Estimation of the Kolmogorov entropy from a chaotic signal, Phys. Rev. A 28 (4) (1983) 2591–2593.
[16] T. Habutsu, Y. Nishio, I. Sasase, S. Mori, A secret key cryptosystem by iterating a chaotic map, in: D. Davies (Ed.), Advances in Cryptology - EUROCRYPT'91, Lecture Notes in Computer Science, 547, Springer Berlin Heidelberg, 1991, pp. 127–140.
[17] H.-I. Hsiao, J. Lee, Color image encryption using chaotic nonlinear adaptive filter, Signal Process. 117 (0) (2015) 281–309.
[18] Z. Hua, Y. Zhou, C.L.P. Chen, A new series-wound framework for generating 1D chaotic maps, in: Proceedings of the 2013 IEEE Digital Signal Processing and Signal Processing Education Meeting (DSP/SPE), 2013, pp. 118–123.
[19] Z. Hua, Y. Zhou, C.-M. Pun, C.L.P. Chen, 2D Sine Logistic modulation map for image encryption, Inf. Sci. 297 (0) (2015) 80–94.
[20] C. Li, D. Arroyo, K.-T. Lo, Breaking a chaotic cryptographic scheme based on composition maps, Int. J. Bifurc. Chaos 20 (8) (2010) 2561–2568.
[21] C. Li, Y. Liu, L.Y. Zhang, M.Z. Chen, Breaking a chaotic image encryption algorithm based on modulo addition and XOR operation, Int. J. Bifurc. Chaos 23 (4) (2013) Art. ID 1350075.
[22] C. Li, K.-T. Lo, Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks, Signal Process. 91 (4) (2011) 949–954.
[23] S. Li, C. Li, K.-T. Lo, G. Chen, Cryptanalysis of an image scrambling scheme without bandwidth expansion, IEEE Trans. Circuits Syst. Video Technol. 18 (3) (2008) 338–349, doi:10.1109/TCSVT.2008.918116.
[24] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (9) (2010) 2714–2722.
[25] C. Ling, X. Wu, S. Sun, A general efficient method for chaotic signal estimation, IEEE Trans. Signal Process. 47 (5) (1999) 1424–1428.
[26] H. Liu, A. Kadir, Asymmetric color image encryption scheme using 2D discrete-time map, Signal Process. 113 (0) (2015) 104–112.
[27] R.M. May, et al., Simple mathematical models with very complicated dynamics, Nature 261 (5560) (1976) 459–467.
[28] H.C. Papadopoulos, G.W. Wornell, Maximum-likelihood estimation of a class of chaotic signals, IEEE Trans. Inf. Theory 41 (1) (1995) 312–317.
[29] P. Ping, F. Xu, Z.-J. Wang, Image encryption based on non-affine and balanced cellular automata, Signal Process. 105 (2014) 419–429.
[30] S.K. Rajput, N.K. Nishchal, Known-plaintext attack on encryption domain independent optical asymmetric cryptosystem, Opt. Commun. 309 (0) (2013) 231–235.

[31] C.E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J. 28 (4) (1949) 656–715.
[32] C. Shen, S. Yu, J. Lü, G. Chen, Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model, IEEE Trans. Circuits Syst. I Regul. Pap. 61 (8) (2014) 2380–2389.
[33] I.I. Shevchenko, Lyapunov exponents in resonance multiplets, Phys. Lett. A 378 (12) (2014) 34–42.
[34] A. Skrobek, Cryptanalysis of chaotic stream cipher, Phys. Lett. A 363 (12) (2007) 84–90.
[35] S. Tedmori, N. Al-Najdawi, Image cryptographic algorithm based on the Haar wavelet transform, Inf. Sci. 269 (2014) 21–34.
[36] X. Wang, W. Zhang, W. Guo, J. Zhang, Secure chaotic system with application to chaotic ciphers, Inf. Sci. 221 (0) (2013) 555–570.
[37] X. Wu, H. Hu, B. Zhang, Parameter estimation only from the symbolic sequences generated by chaos system, Chaos Solitons Fractals 22 (2) (2004) 359–366.
[38] 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.
[39] Y. Wu, G. Yang, H. Jin, J.P. Noonan, Image encryption using the two-dimensional logistic chaotic map, J. Electron. Imaging 21 (1) (2012) Art. ID 013014.
[40] Y. Wu, Y. Zhou, S. Agaian, J.P. Noonan, A symmetric image cipher using wave perturbations, Signal Process. 102 (9) (2014) 122–131.
[41] Y. Wu, Y. Zhou, J.P. Noonan, S. Agaian, Design of image cipher using latin squares, Inf. Sci. 264 (0) (2014) 317–339.
[42] 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 (0) (2013) 323–342.
[43] D. Xiao, X. Liao, S. Deng, One-way hash function construction based on the chaotic map with changeable-parameter, Chaos Solitons Fractals 24 (1) (2005) 65–71.
[44] G. Ye, Image scrambling encryption algorithm of pixel bit based on chaos map, Pattern Recognit. Lett. 31 (5) (2010) 347–354.
[45] L.Y. Zhang, X. Hu, Y. Liu, K.-W. Wong, J. Gan, A chaotic image encryption scheme owning temp-value feedback, Commun. Nonlinear Sci. Numer. Simul. 19 (10) (2014) 3653–3659.
[46] Y. Zhang, D. Xiao, W. Wen, M. Li, Breaking an image encryption algorithm based on hyper-chaotic system with only one round diffusion process, Nonlinear Dyn. 76 (3) (2014) 1645–1650.
[47] Y. Zhang, D. Xiao, W. Wen, K.-W. Wong, On the security of symmetric ciphers based on DNA coding, Inf. Sci. 289 (2014) 254–261.
[48] Y. Zhang, L.Y. Zhang, Exploiting random convolution and random subsampling for image encryption and compression, Electron. Lett. 51 (20) (2015) 1572–1574.
[49] Y.-Q. Zhang, X.-Y. Wang, A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice, Inf. Sci. 273 (0) (2014) 329–351.
[50] Y. Zhou, L. Bao, C.L.P. Chen, Image encryption using a new parametric switching chaotic system, Signal Process. 93 (11) (2013) 3039–3052.
[51] Y. Zhou, L. Bao, C.L.P. Chen, A new 1D chaotic system for image encryption, Signal Process. 97 (2014) 172–182.
[52] Y. Zhou, Z. Hua, C.-M. Pun, C.L.P. Chen, Cascade chaotic system with applications, IEEE Trans. Cybern. 45 (9) (2015) 2001–2012.