Multimed Tools Appl (2018) 77:21445–21462
https://doi.org/10.1007/s11042-017-5594-9

A new simple one-dimensional chaotic map and its application for image encryption

Lingfeng Liu [1] **· Suoxia Miao** [2]

Received: 11 April 2017 / Revised: 17 October 2017 / Accepted: 27 December 2017 /
Published online: 10 January 2018

Abstract In this paper, we propose a new simple one-dimensional chaotic map. The chaotic characteristics have been declared by using bifurcation analysis and Lyapunov exponent analysis. Furthermore, we propose a new image encryption algorithm based on this new chaotic map. Both shuffling algorithm and substitution algorithm are related to this map. Many statistical tests and security analysis indicate that this algorithm has an excellent security performance, and can be competitive with some other recently proposed image encryption algorithms.

Keywords Chaos · One-dimensional chaotic map · Bifurcation · Lyapunov exponent · Image encryption

1 Introduction

Chaos is a kind of nonlinear phenomenon in the physical world. The first chaotic system was proposed by Lorenz in [11]. After then, many different kinds of chaotic systems have been provided and constructed, eg, Logistic map [13], Tent map [6], Henon Map [7], Chen system [12], coupled map lattices [9], and very recently, Bulban map [1], Lorenz-like system [2], spatiotemporal chaotic system [19], et al.

In these studies, the high-dimensional chaotic system and hyper-chaotic systems have received much more attentions than one-dimension map. One of the main reasons is that the control parameter of the one-dimensional chaotic map is rather limited, which makes the chaotic map easier to be attacked. As we know, one-dimensional chaotic map is easy to implement and can also provide good chaotic characteristics,

✉ Lingfeng Liu
vatanoilcy@163.com

[1] School of Software, Nanchang University, Nanchang 330031, People's Republic of China

[2] Faculty of Science, Nanchang Institute of Technology, Nanchang 330029, People's Republic of China

which is also important for practical use. Therefore, in this paper, we propose a new simple one-dimensional chaotic map with two control parameters, where one of the parameter can be infinite, which greatly increase the parameter space. We theoretically analyze the linear stability of the fixed points of this new map, and use numerical simulations to reveal the bifurcation and Lyapunov exponent, the results show that the chaotic performance is only related to one of the system parameter, and has no correlation to the other.

With the rapid development in internet technology and multimedia technology, communications with images have become more and more popular. In order to ensure communication security, image encryption has become an increasingly serious issue and urgently needed [18]. However, traditional encryption algorithms, such as RSA, DES and IDEA, are not suitable for image encryption due to image's intrinsic properties such as bulky data capacity, strong redundancy and strong correlations among adjacent pixels [4, 5, 10].

Recently, chaotic systems have been widely used in image encryption for their significance nonlinear performance, such as sensitivity to both initial value and parameter, unpredictability, and pseudorandomness, et al. [8, 15–17, 20]. Wang and Guo [17] proposes an image alternate encryption algorithm based on Logistic map. In this algorithm, the shuffling and diffusion stages are combined in encryption process. However, Logistic map is proved to be not secure enough for its small key space and some other weaknesses [10]. Zhou and Liao [20] presents a digital image encryption algorithm with different precisions by three collision-based dynamical systems. This algorithm induces three chaotic systems, which increases its implementation cost. Sun et al. [15] proposes a new image encryption algorithm based on a new spatial chaos system. Tong et al. [16] proposes a new high-dimensional chaotic system, and presents a novel image encryption based on this map and Cat map. In order to enhance the security, a new separated Cat map with variable parameters is designed for the permutation process. These two algorithms are based on high-dimensional chaotic systems. Although the security performances are quite good, the encryption speed is not satisfactory. Hua et al. [8] proposes an image encryption algorithm based on new two-dimensional Sine Logistic modulation map. This map is derived from Logistic map and Sine map, while the use of original Logistic map makes this algorithm not that convincing.

In this paper, we propose a new image encryption algorithm based on our new one-dimensional chaotic map. Both shuffling and substitution algorithms are related to this new map. Many statistical tests and security analysis are carried out to evaluate the performances of our algorithm, including histogram analysis, information entropy analysis, key space analysis, key sensitivity analysis, correlation analysis, resistance to differential attack analysis, and randomness analysis. The results prove that our algorithm has a high security level, and can be competitive with other recently proposed image encryption algorithms.

The rest of this paper is organized as follows. The mathematically model of this new chaotic map is introduced in Section 2, and its dynamical performances are revealed in Section 3. In Section 4, we propose a new image encryption algorithm based on the new chaotic map. Statistical tests and security analysis of our algorithm are presented in Section 5. Finally, Section 6 concludes the whole paper.

2 A new one-dimensional chaotic map

The mathematical model of our new one-dimensional chaotic map is described as follow

$$x_{n+1} = f(x_n) = \sqrt{-ax_n^2 + bx_n} \tag{1}$$

here, n is the iteration number, a, $b > 0$ are the two control parameters of this equation, f: $I \to I$ is the nonlinear iterative function, $x_n = f^{(n)}(x_0)$ is the one-dimensional state variable after n times iteration by initial condition x_0.

A chaotic map must be bounded. By Eq. (1), obviously, we have $0 < x_n < b/a$, for every n. Thus, $I = [0, b/a]$. The nonlinear function f can be estimated as

$$f(x) = \sqrt{-a\left(x - \frac{b}{2a}\right)^2 + \frac{b^2}{4a}} \le \frac{b}{2\sqrt{a}} \tag{2}$$

the "=" holds if and only if $x = b/2a$. In order to make the state variable x bounded in the interval I, it should have

$$\frac{b}{2\sqrt{a}} \le \frac{b}{a} \tag{3}$$

Eq. (3) indicates that $a \le 4$. Set $a = 4$, $b = 3$, the trajectory diagram is shown in Fig. 1.

3 Dynamical performances

In this section, we will analyze the dynamical characteristics of our new chaotic map, including fix point, linear stability and bifurcation analysis.

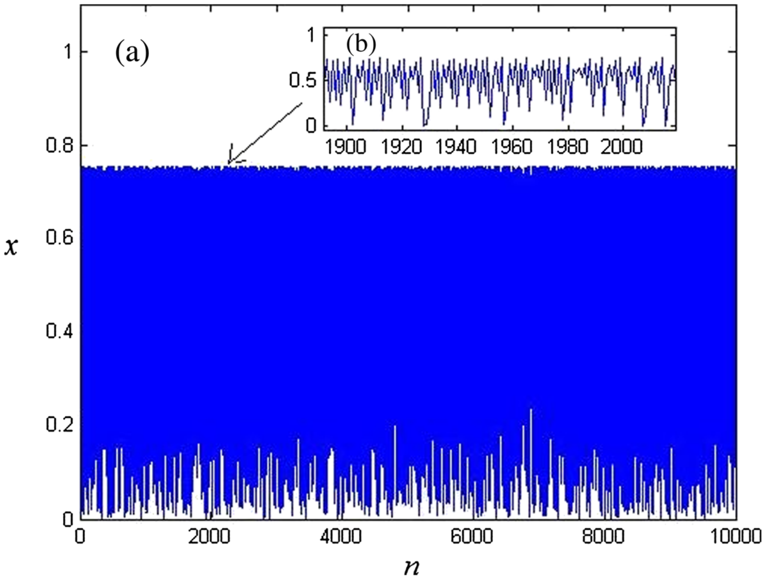

Fig. 1 (**a**) The trajectory diagram of Eq. (1); (**b**) Enlargement of (**a**)

3.1 Fixed points, linear stability and bifurcation analysis

We consider the fixed points and also the equilibrum points of our map, which can be calculated as $x^* = f(x^*)$. After calculation, there exist two fixed points, which are found as

$$x^* = 0 \text{ and } x^* = \frac{b}{1+a}, \tag{4}$$

respectively. In order to get bifurcation, the fixed points should be unstable. We consider a point x_n close to the fixed point x^* with a small difference Δx, we get

$$\Delta x_n = x_n - x^* \tag{5}$$

Afterward, we do the Taylor expansion of function f, and get

$$x^* + \Delta x_{n+1} = x_{n+1} = f(x_n) = f(x^*) + f'\left(x^*\right)\Delta x_n + \cdots \tag{6}$$

Here $f'(x)$ is the derivation of function f at point x, which can be calculated as

$$f'(x) = \frac{-2ax + b}{2\sqrt{-ax^2 + bx}} \tag{7}$$

Put $x^* = f(x^*)$ into Eq. (6), Eq. (6) can be simplified as

$$\Delta x_{n+1} = f'\left(x^*\right)\Delta x_n + \cdots \tag{8}$$

Therefore, if $|f'(x^*)|$ is larger than 1, we have that the difference $|\Delta x_{n+1}|$ is larger than $|\Delta x_n|$, which means that the fixed point is unstable.

Next, we consider the value of $|f'(x^*)|$. Substituting $x^* = 0$ into Eq. (7), we have $|f'(x^*)|$ approach to infinity. Thus, the fixed point 0 becoming unstable. When substituting $x^* = b/(1 + a)$ into Eq. (7), we get

$$f'\left(x^*\right) = \frac{-2a\cdot\frac{b}{1+a} + b}{2\sqrt{-a\cdot\frac{b^2}{(1+a)^2} + b\cdot\frac{b}{1+a}}} = \frac{1-a}{2} \tag{9}$$

In order to make the fixed point x^* unstable, it should have

$$f'\left(x^*\right) = \frac{1-a}{2} > 1 \tag{10}$$

or

$$f'\left(x^*\right) = \frac{1-a}{2} < -1 \tag{11}$$

From Eq. (10), we can get $a < -1$. This contradicts the requirement that $a > 0$, and thus, be neglected. From Eq. (11) we have that $a > 3$. This solution gives the first bifurcation point on

$a > 3$, and the fixed point becoming unstable, which means the chaotic behavior of Eq. (1). Furthermore, the second bifurcation point can be calculated using the period 2 points of $f^{(2)}(x_n)$.

$$f^{(2)}(x_n) = f(f(x_n)) = \sqrt{-a\left(-ax_n^2 + bx_n\right)^2 + b\left(-ax_n^2 + bx_n\right)} \tag{12}$$

By using the similar method of fixed points, the second bifurcation point can be approximately calculated as $a > 3.6451$. Moreover, by using simulations on Matlab, the bifurcation diagram of parameter a is shown in Fig. 2. From Fig. 2 we have that this map will be chaotic when $3.7835 < a \leq 4$. Another interesting result is that the bifurcation point has no relevance to the parameter b, the similar result can also be achieved in the Lyapunov exponent analysis. Parameter b only affects the interval I.

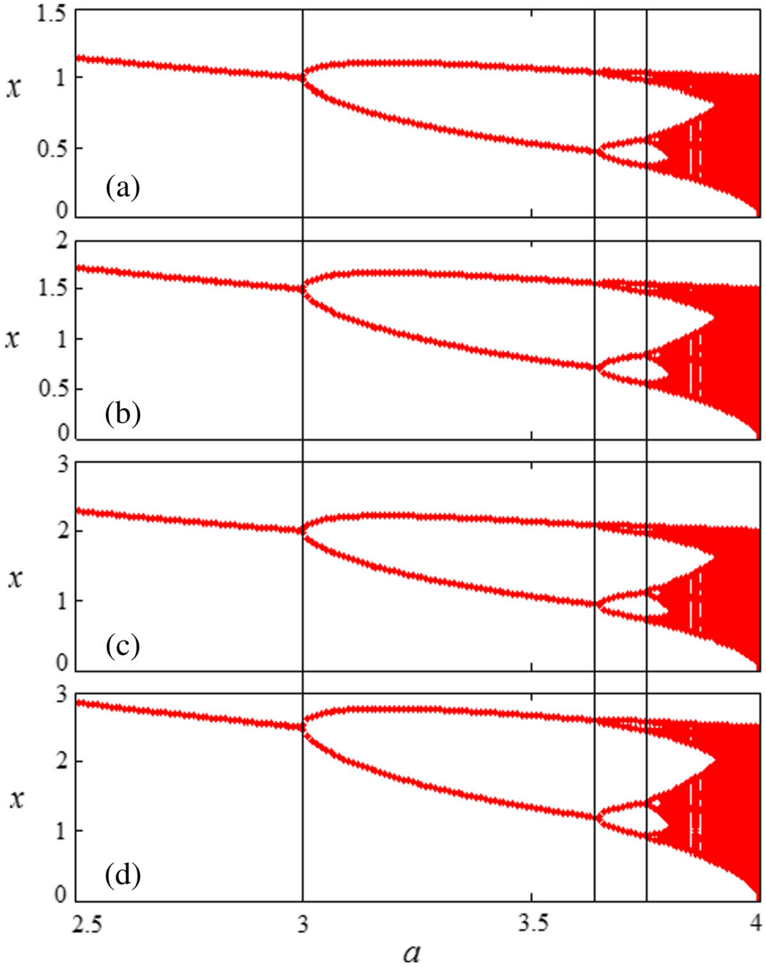

Fig. 2 Bifurcation diagram of parameter a (**a**) $b = 4$; (**b**) $b = 6$; (**c**) $b = 8$; (**d**) $b = 10$

3.2 Lyapunov exponent

The one-dimensional chaotic map has only one largest Lyapunov exponent. The largest Lyapunov exponent is used to measure whether the map is chaotic or not. For an exponent larger than zero, the map is chaotic, and vice versa. The larger the Lyapunov exponent is, the more complex (less predictable) the map is. The largest Lyapunov exponent can be calculated as [14]:

$$LE = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \lambda_i \tag{13}$$

where

$$\lambda_n = \ln\left|f^{'}(x_n)\right| \tag{14}$$

$f'(x_n)$ is given by Eq. (7). For different parameter b, Fig. 3 show the Lyapunov exponents with the variation of parameter a. From Fig. 3 we have that the Lyapunov exponent diagram is the same with different parameter b, which means that the chaotic characteristics has no relevance to parameter b. This gets the same conclusion as bifurcation analysis. The Lyapunov exponent of Eq. (1) reaches its maximum value when $a = 4$, which is about $LE = 0.5547$. The convergence process is shown in Fig. 4.

Based on the above analysis, the significant advantages of this map can be described as

1) This map is one-dimensional, which is much easier to implement than high dimensional maps. For most of 1D chaotic maps, such as Logistic map, Chebyshev map, Tent map, et al., they have only one control parameter, which leads to a relatively small key space. While in our map, there are two control parameters, and the key space is larger, which is more suitable for image encryption.
2) Generally, the dynamics of chaotic map will be influenced by its control parameters. All the parameters will affect the dynamics of chaotic map, such as [1], which makes the dynamical behavior of map hard to control. For our map, the chaotic performance is only related to one of the system parameter, and has no correlation to the other, which indicates that our map is easier to control in this sense.

4 A new image encryption algorithm

In this section, we propose a new image encryption algorithm based on this new one-dimensional chaotic map. Our new algorithm is combined with two steps, shuffling algorithm and substitution algorithm.

4.1 Shuffling algorithm

The shuffling algorithm is used to disturb the positions of each pixel of a plain image A, which can reduce the correlationship between adjacent pixels. In our algorithm, we use the proposed chaotic map Eq. (1) to shuffle the pixels.

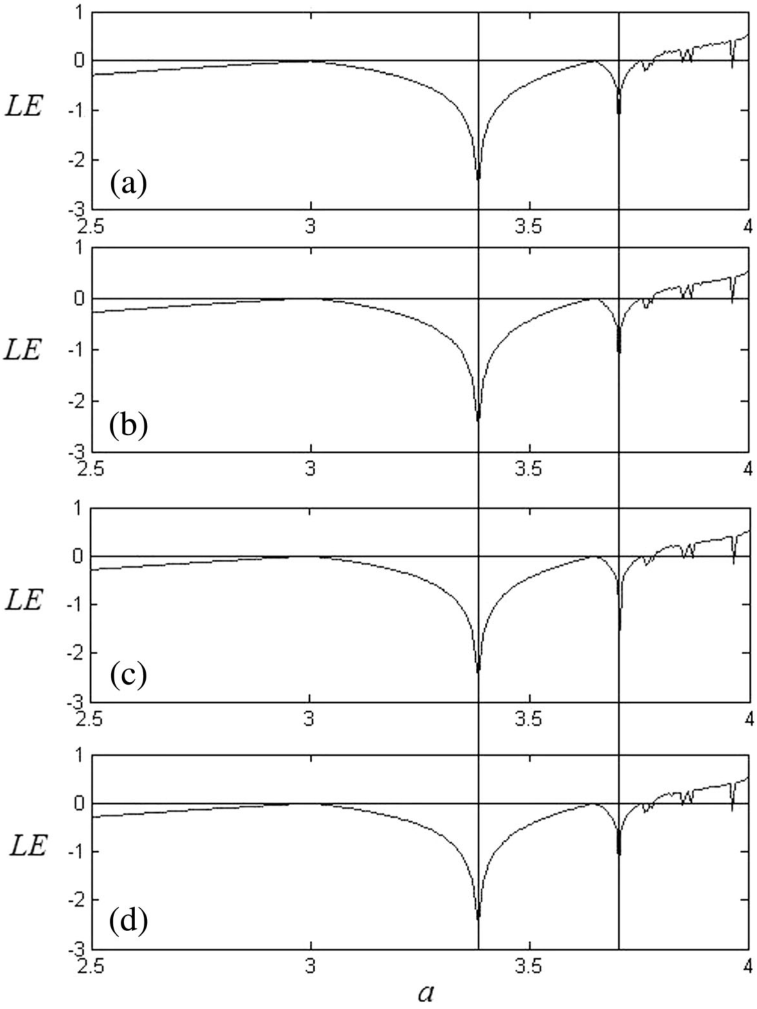

Fig. 3 Lyapunov exponent with the variation of parameter a (**a**) $b = 10$; (**b**) $b = 8$; (**c**) $b = 6$; (**d**) $b = 4$

Assume $\{A_{ij}\}$ be the pixel matrix of $M \times N$ plain image A, and a real-valued sequence $\{x_k\}$ is generated by the Eq. (1) with a given initial value with length MN. Rearrange the sequence $\{x_k\}$ according to the ascending order, and get the rearranged sequence

$$x_{k_1}, x_{k_2}, \ldots, x_{k_{MN}} \tag{15}$$

where

$$x_{k_1} < x_{k_2} < \cdots < x_{k_{MN}} \tag{16}$$

and $k_l \in \{1, 2, ..., MN\}$, $1 < l < MN$, is different from each other. Now, the integer sequence $\{k_l\}$ is used as the shuffling sequence. Scanning the matrix A into a sequence $\{b_s\}$ as

$$b_{(i-1)N+j} = A_{ij}, \quad 1 \le i \le M, 1 \le j \le N \tag{17}$$

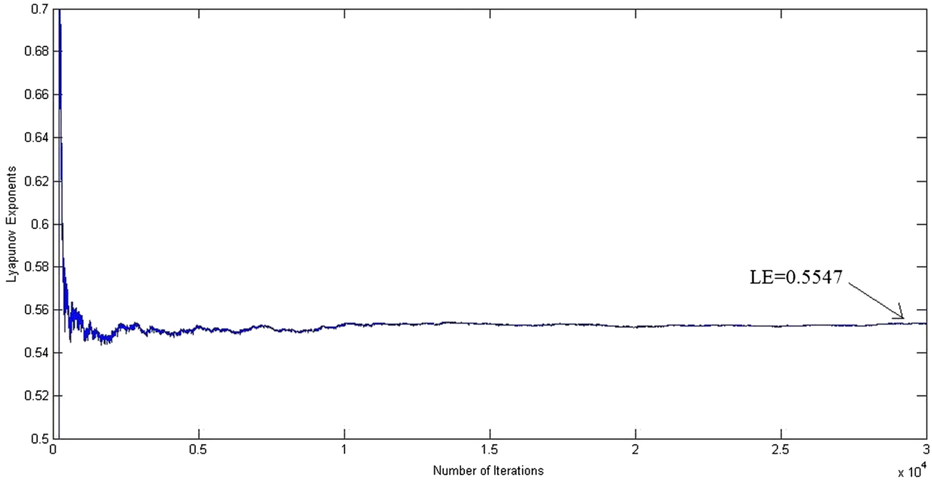

Fig. 4 Convergence of the Lyapunov exponent for $a = 4$

Then, the shuffled sequence $\{c_t\}$ can be calculated as

$$c_{k_i} = b_i, \quad 1 \le i \le MN \tag{18}$$

Finally, reconstruct the sequence $\{c_t\}$ to a matrix as

$$C_{ij} = c_t \tag{19}$$

where

$$i = floor\lfloor (t-1)/N \rfloor + 1 \tag{20}$$

and

$$j = t-(i-1)N \tag{21}$$

Thus, the matrix C is the shuffled matrix of plain A by using our shuffling algorithm. This shuffled matrix is based on the chaotic sequence $\{x_k\}$, which can be regarded as unpredictable and randomness.

4.2 Substitution algorithm

The Substitution algorithm is used to change the pixel value of plain image A. Based on the chaotic characteristics of our proposed map, here, we also use this map in our substitution algorithm.

Also, assume a real-valued sequence $\{x_k\}$ is generated by the Eq. (1) with a given initial value with length MN. In order to get good statistical properties, we first change the sequence $\{x_k\}$ into a uniformly distributed integer sequence $\{d_k\}$. In this paper, we propose the following coding algorithm to generate uniformly distributed integer sequence

$$d_k = 600000(x_k + 2350) \quad \mathrm{mod}256 \tag{22}$$

The distribution of sequence $\{x_k\}$ and $\{d_k\}$ are shown in Fig. 5, which indicate that our uniformly distributed algorithm is quite effective.

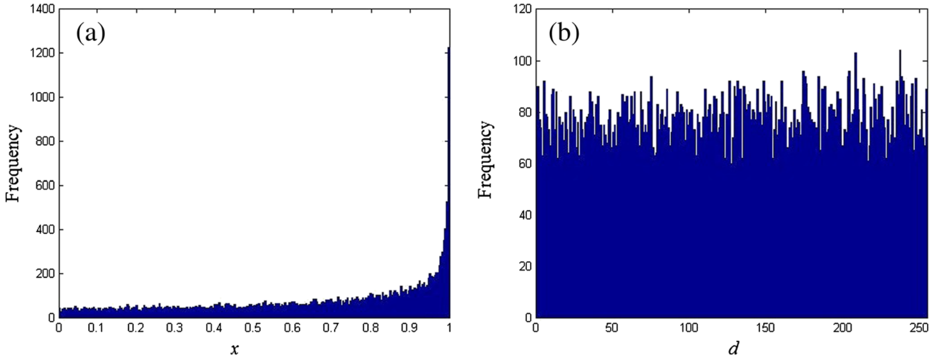

Fig. 5 Distribution of (**a**) chaotic sequence $\{x_k\}$; (**b**) coding sequence $\{d_k\}$

Change the sequence $\{d_k\}$ into a substitution matrix D by using the same method as Eq. (19), (20) and (21). The substituted image matrix E can be written as

$$E_{ij} = D_{ij} + C_{ij} \quad \mathrm{mod}256 \tag{23}$$

Remark 1 In our algorithm, the newly proposed chaotic map is the key factor to ensure the security of encrypted images. Eq. (22) is used to improve the statistical characteristics of chaotic sequences. The randomness tests are provided in Section 5.8. Certainly, we can replace this generator by another one. If other generators can make the sequence $\{d_k\}$ with good randomness, there will have no much differences in the security of encrypted images.

4.3 The new image encryption algorithm

In order to have a high chaotic characteristics of Eq. (1), we always set $a = 4$ in our algorithm. The detailed steps of our algorithm are described as follows.

Step 1: Read the plain image A. Assume the size of plain image A be $M \times N$, and set $R = 1$.

Step 2: Set secret values $x_{0,1}$, $x_{0,2}$, ..., $x_{0,T}$, $y_{0,1}$, $y_{0,2}$, ..., $y_{0,T}$ and b_1, b_2, ..., b_T for T round encryption. Secret values $x_{0,1}$, $x_{0,2}$, ..., $x_{0,T}$ are used in the shuffling phase, and $y_{0,1}$, $y_{0,2}$, ..., $y_{0,T}$ are used in the substitution phase. b_1, b_2, ..., b_T are the parameters of our chaotic map which are used in both shuffling and substitution phases.

Step 3: Generate the real-valued chaotic sequences $\{x_k\}$ and $\{y_k\}$ with length MN based on Eq. (1) by the initial values $x^*_i = x_{0,i} + \mathrm{mean}\{A\}/256 \bmod (b_i/4)$, and $y^*_i = y_{0,i} + \mathrm{mean}\{A\}/256 \bmod (b_i/4)$, $i = 1, 2, ..., T$, and denote as $\{X_1\}$, $\{X_2\}$, …, $\{X_T\}$ and $\{Y_1\}$, $\{Y_2\}$, …, $\{Y_T\}$ respectively. Here, $x_{0,i}$ and $y_{0,i}$ can be selected arbitrarily in the interval I. In generating the chaotic sequences, the average pixel value of plain image A is used, which makes our algorithm to resist the chosen-plaintext attack. The item mod $(b_i/4)$ is used to ensure the initial values locates in the interval I.

Step 4: Change the real-valued sequences $\{X_R\}$ into shuffling matrix according to Eq. (15), (16) and (17), and then generate the shuffled matrix $\{C_R\}$ by Eq. (18), (19), (20) and (21).

Step 5: Change the sequence $\{Y_R\}$ into uniformly distributed sequence by Eq. (22), and construct this sequence into matrix according to Eq. (19), (20) and (21).

Step 6: Encrypt the shuffled matrix $\{C_R\}$ by Eq. (23).
Step 7: Set $R = R + 1$.
Step 8: If $R \leq T$, go to step 4. Else, break out.
Step 9: Save as encrypted image A^*.

The flowchart of our algorithm is shown in Fig. 6. The values $x_{0,1}$, $x_{0,2}$, ..., $x_{0,T}$, $y_{0,1}$, $y_{0,2}$, ..., $y_{0,T}$ and b_1, b_2, ..., b_T can be used as the security keys. The decryption algorithm is the inverse process of our encrypt algorithm which is neglected here.

Our encryption algorithm is based on our newly proposed 1D chaotic map. In order to enhance the security, we use Eq. (22) to generate a uniformly distributed sequence. Our encryption scheme is quite different from other chaotic image encryption algorithms since the chaotic source used here is completely different from others.

As we know, the security of the encrypted image is mainly depended on the chaotic sequences generated by chaotic sources. In our algorithm, the parameter is selected in the chaotic region, and Eq. (22) is used to improve its statistical characteristics. Therefore, the output chaotic sequence is with good randomness (We use NIST test suite to confirm the randomness of the output chaotic sequence in Section 5.8), and thus the encrypted images have relatively high security (uniformly distribution, weak correlation between pixels, large entropy, et al.). Furthermore, the average pixel value of plain image A is used in generating the chaotic sequences to resist the chosen-plaintext attack.

5 Statistical tests and security analysis

In this section, we make some experiments to evaluate the security and statistical properties of our image encryption algorithm, and compare the results with some other algorithms in [8, 15–17, 20]. The experiment image is 256 × 256 plain image, and the encryption round is one.

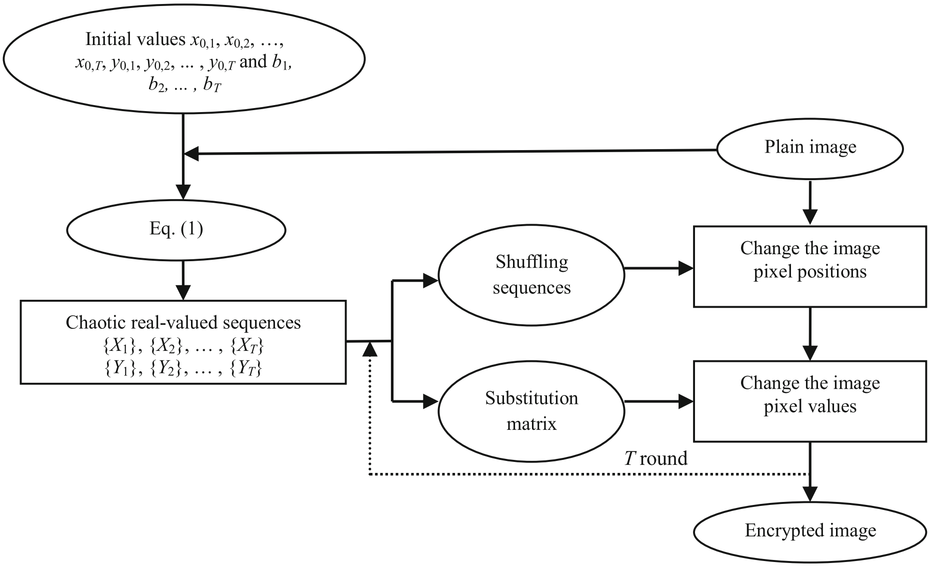
Initial values $x_{0,1}$, $x_{0,2}$, …, $x_{0,T}$, $y_{0,1}$, $y_{0,2}$, … , $y_{0,T}$ and b_1, b_2, … , b_T
Plain image
Eq. (1)
Shuffling sequences
Change the image pixel positions
Chaotic real-valued sequences $\{X_1\}$, $\{X_2\}$, … , $\{X_T\}$ $\{Y_1\}$, $\{Y_2\}$, … , $\{Y_T\}$
Substitution matrix
Change the image pixel values
T round
Encrypted image

Fig. 6 The flowchart of our image encryption algorithm

All the tests are processed by Matlab 7.0 on computer with 1.99 GHz CPU and 1.92 GB memory. The security keys are selected as $x_{0,1} = 0.1236$, $y_{0,1} = 0.3278$ and $b_1 = 4$.

5.1 Encryption and decryption experiment tests

The encryption and decryption results are shown in Fig. 7. Four plain images are used in the encryption phase, including "Lena", "Horse", "Cameraman" and "Cameo", where "Cameo" is a computer generated image. From Fig. 7 we know that all the encrypted images are completely unrecognized. In the decryption phase, as the results are quite similar, so we only present the decryption results of Lena image here. By using the correct keys, the decrypted image is the same as the plain image, while with a wrong key, the decrypted image is also unrecognized.

5.2 Histogram analysis

The histogram is use to evaluate the distribution of ciphered image. In order to withstand the statistical attack and cipher-only attack, the histogram should be uniform. The histogram of

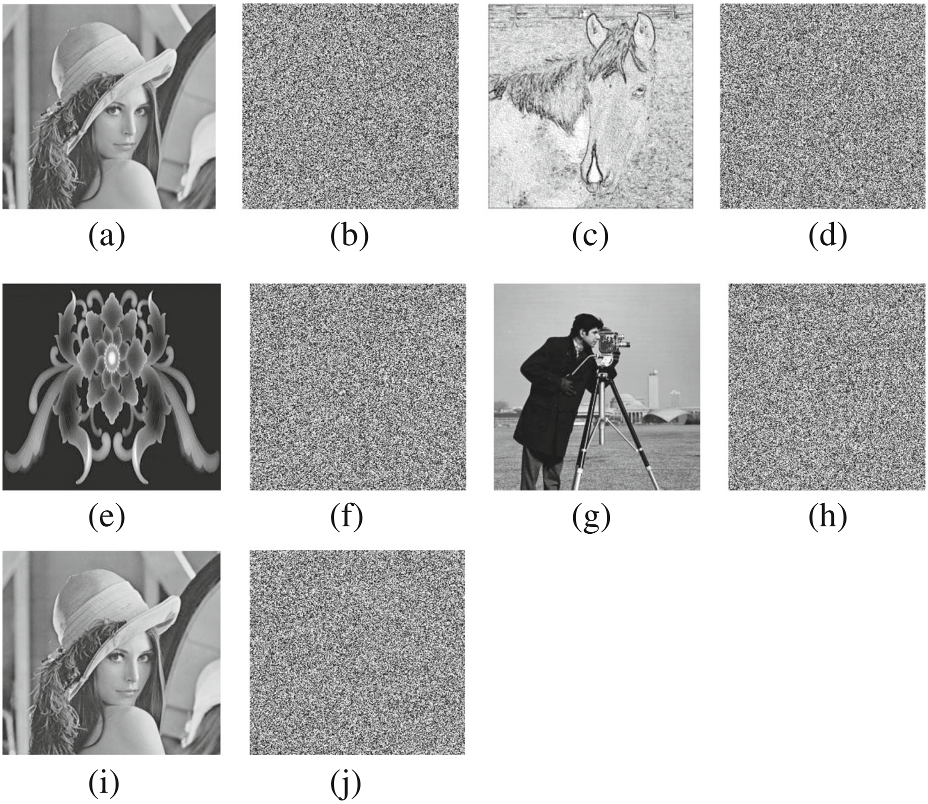

Fig. 7 Encryption and decryption results (**a**) Lena plain image; (**b**) Lena encrypted image; (**c**) Horse plain image; (**d**) Horse encrypted image; (**e**) Cameo plain image; (**f**) Cameo encrypted image; (**g**) Cameraman plain image; (**h**) Cameraman encrypted image; (**i**) Decryption of Lena image with correct key; (**j**) Decryption of Lena image with wrong key

plain Lena image and the encrypted Lena image are shown in Fig. 8, which indicates that the distribution of our encrypted image is rather uniform comparing to the plain image.

5.3 Information entropy analysis

Information entropy, proposed by Shannon, is widely used to evaluate the uncertainty or unpredictability, and can be calculated as

$$H(m) = -\sum_{i=1}^{M} p(m_i)\log_2 p(m_i) \tag{24}$$

here, M is the total number if symbols, and $p(m_i)$ is the probability of symbol m_i. For a random image with 256 Gy levels, the entropy should ideally be 8. In this test, the entropies of plain image and encrypted image are calculated in Table 1, which indicates that the entropies of the encrypted images by our encryption algorithm are all close to 8, and is better than the results in [15, 17, 20], but a little less than the entropy in [16].

5.4 Key space analysis

The key space should be large enough to resist brute-force attacks. In our proposed encryption algorithm, values $x_{0,1}$, $x_{0,2}$, ..., $x_{0,T}$; $y_{0,1}$, $y_{0,2}$, ..., $y_{0,T}$ and b_1, b_2, ..., b_T are always be selected as security keys. If the precision of a real number is 10^{-14}, the key space of our algorithm can be approximately written as.

$$\left(\frac{1}{4}\cdot 10^{14}\cdot 10^{14}\cdot 10^{14}\right)^{T} \tag{25}$$

Set the round $T = 2$. the key space is about $0.25 \times 10^{84} \approx 2^{277}$, which is large enough to resist all kinds of brute-force attacks and is much larger than some recently proposed algorithms, such as 2^{160} in [17], 2^{140} in [16], and 2^{256} in [8], under the same precision.

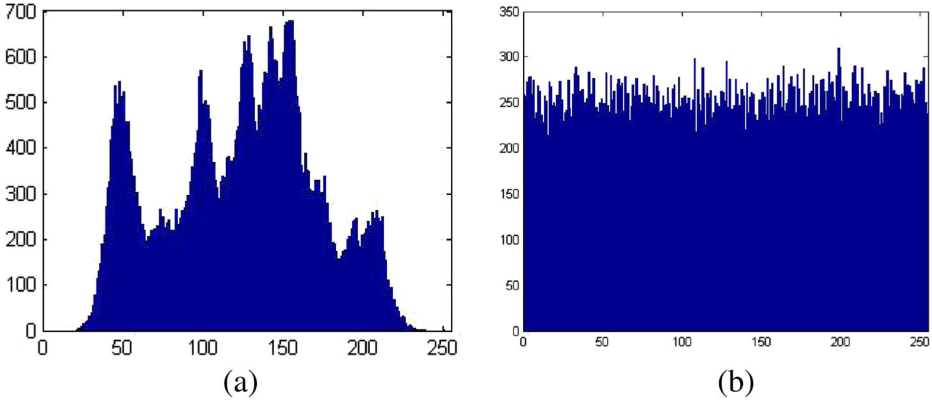

Fig. 8 Statistical histogram of (**a**) Lena plain image; (**b**) Lena encrypted image

Table 1 Information entropy analysis of plain image and encrypted image

Images	Information entropy
Plain image (Lena)	7.4532
Encrypted image (Lena)	7.9979
Ref. [17] (Lena)	7.9977
Ref. [20] (Lena)	7.9966
Ref. [15] (Lena)	7.9965
Ref. [16] (Lena)	7.9989
Encrypted image (Horse)	7.9973
Encrypted image (Cameo)	7.9977
Encrypted image (Cameraman)	7.9974

5.5 Key sensitivity analysis

A good encryption scheme should be extremely sensitive to its security key. Key sensitivity means that for the same plain image, if there is a small change (only 1 bit) of the secret keys, the encrypted image should be totally different. In this test, we test the key sensitivity of $x_{0,1}$ and b_1, the sensitivity of $y_{0,1}$ is similar which we omitted here. Change each secret key by only 10^{-14}, the test results are shown in Fig. 9.

Figure 9a is the encrypted image by changing the key $x_{0,1}$ to $0.1236 + 10^{-14}$. Figure 9b shows the difference between Fig. 9a and Fig. 7b, which is vastly different from each other. Figure 9c is the encrypted image by changing the key b_1 to $4 + 10^{-14}$. Figure 9d shows the difference between Fig. 9c and Fig. 7b, which is totally different from each other as well. These results show that the security keys have good sensitivity.

5.6 Correlation analysis

The pixels of a plain image always have a high correlation with their neighboring pixels, either in horizontal, vertical or diagonal directions. Therefore, a good image encryption algorithm should remove this strong correlation between adjacent pixels.

In this test, we first randomly select 2040 pairs of adjacent pixels along with the horizontal, vertical and diagonal directions. The distributions of these pixel sequence pairs are plot in Fig. 10. From Fig. 10, we have that the points of plain Lena image are located nearby the diagonal line, while the points of encrypted Lena image are uniformly located in the whole space. These results show that we can remove the correlation between adjacent pixels.

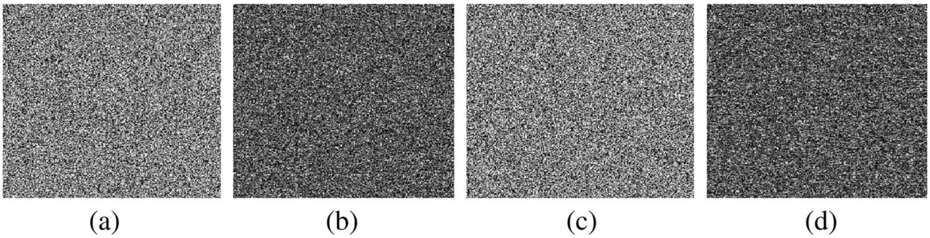

Fig. 9 Key sensitivity analysis in the encryption process

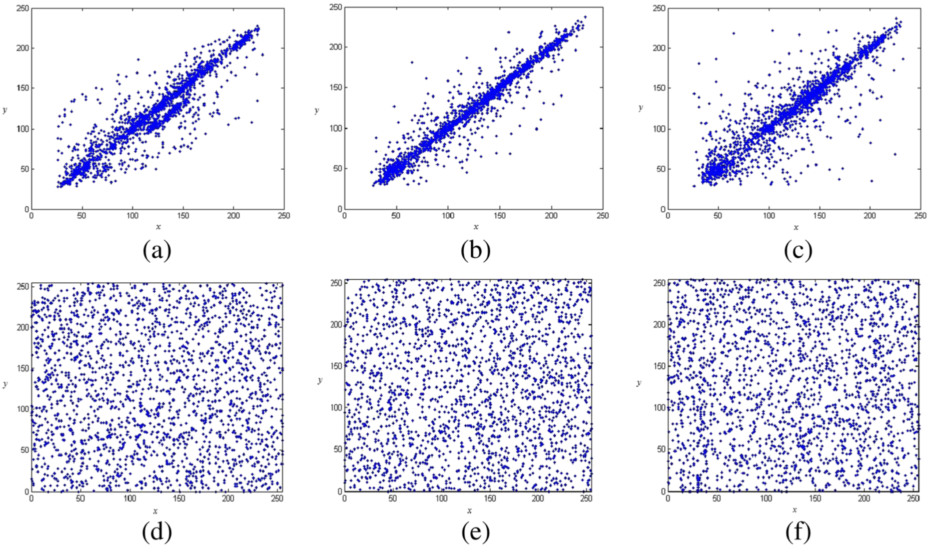

Fig. 10 Distributions of adjacent pixel sequence pairs of Lena image (**a**) horizontal of plain image; (**b**) vertical of plain image; (**c**) diagonal of plain image; (**d**) horizontal of encrypted image; (**e**) vertical of encrypted image; (**f**) diagonal of encrypted image

Furthermore, we test the correlation coefficient of pixel sequence pairs by using the following equation

$$Corr = \frac{N\sum_{i=1}^{N}(x_i \times y_i) - \sum_{i=1}^{N}x_i \times \sum_{i=1}^{N}y_i}{\sqrt{\left(N\sum_{i=1}^{N}x_i^2 - \left(\sum_{i=1}^{N}x_i\right)^2\right) \times \left(N\sum_{i=1}^{N}y_i^2 - \left(\sum_{i=1}^{N}y_i\right)^2\right)}} \tag{26}$$

where x_i and y_i be the two pixel sequences, N is the length. If the correlation value is close to 1, then these two sequences have a high correlation. If the correlation value is close to 0, then these two sequences have little correlation with each other. The value of *Corr* for each pair is shown in Table 2. From Table 2 we have that the correlation coefficients of our encrypted

Table 2 Correlation analysis

Images	Horizontal	Vertical	Diagonal
Plain image (Lena)	0.9686	0.9677	0.9172
Encrypted image (Lena)	– 0.0026	– 0.0054	0.0082
Ref. [17] (Lena)	0.0063	0.0063	0.0069
Ref. [20] (Lena)	0.0139	– 0.0231	– 0.004
Ref. [15] (Lena)	0.0013	– 0.0026	– 0.0013
Ref. [16] (Lena)	0.0038	0.0058	0.0133
Ref. [8] (Lena)	0.0024	– 0.0086	0.0402
Encrypted image (Horse)	0.0036	0.0018	– 0.0068
Encrypted image (Cameo)	– 0.0039	– 0.0044	– 0.0076
Encrypted image (Cameraman)	– 0.0068	– 0.0046	0.0020

images are all close to 0, which also means that our algorithm has successfully disrupted the correlation between adjacent pixels. Some comparisons to other proposed methods show that our algorithm is quite competitive.

5.7 Resistance to differential attack analysis

The differential attack, also called the chosen-plaintext attack, is a well-known and effective image analysis method. To resist the differential attack, the algorithm should have good sensitivity to plaintext. Two measures are often used to evaluate this property, which are the number of pixels change rate (NPCR) and unified average changing intensity (UACI), and can be calculated as Eq. (27) and (29), respectively [3].

$$\mathrm{NPCR} = \frac{\sum_{i,j} D(i,j)}{L} \times 100\% \tag{27}$$

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & C_1(i,j) \neq C_2(i,j) \end{cases} \tag{28}$$

$$\mathrm{UACI} = \frac{1}{L}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{H}\right] \times 100\% \tag{29}$$

Where C_1 and C_2 are two images with the same size, L is the number of pixels and H is the largest allowed pixel value in the images. In our test, $L = 65{,}536$, $H = 255$. For the random gray image, the ideal value of NPCR and UACI are 0.9961 and 0.3346, respectively.

We randomly change 1 bit of the plain image. The values of NPCR and UACI of two encrypted images with the same keys are shown in Table 3. Table 3 indicates that both NPCR

Table 3 Sensitivity to plaintext test

Test name	Result
NPCR (Lena)	0.9955
UACI (Lena)	0.3327
NPCR (Horse)	0.9961
UACI (Horse)	0.3347
NPCR (Cameo)	0.9959
UACI (Cameo)	0.3344
NPCR (Cameraman)	0.9952
UACI (Cameraman)	0.3360

and UACI values of all images are close to the ideal value, which means that our encryption algorithm has good performance to resist the differential attack.

5.8 Randomness analysis

In our substitution algorithm, we use Eq. (22) to generate the sequence $\{d_k\}$ with uniformly distributed. Here, we further evaluate the randomness of these sequences by using NIST sp-800-22 test suites.

The significance level of each test in NIST is set to 0.01, which means that 99% of test samples pass the tests if the random numbers are truly random. The P-value $\geq$ 0.01 would mean that the sequence would be considered to be random with a confidence of 0.99. In this test, we have generated 500 different sequences randomly by using different initial values and parameter, each sequence having a length of 125,000. Use Eq. (22) to change these sequences into integer sequences. By coding d_k into binary sequence with 8 b, (as: 0 is encoded into "00000000" and 255 is encoded into "11,111,111"), we can totally get 500 pseudorandom binary sequences with length 1,000,000. We test the passing ratio of each test from the NIST test suite and the uniformity of the p-values of each test. The results are shown in Table 4. From Table 4 we know that the sequences have passed all tests suite, which can be regarded as random.

6 Conclusions

In this paper, we propose a new simple one-dimensional chaotic map. The bifurcation of this system is analyzed by both theoretical and experimental methods.

Table 4 The passing ratio and the uniformity of the p-values of each test from the NIST suite

Test index	Passing ratio	P_value	Results
Approximate entropy	0.996	0.577562	SUCCESS
Block frequency	0.994	0.481245	SUCCESS
Cumulative sums	0.998	0.427677	SUCCESS
FFT	0.994	0.247963	SUCCESS
Frequency	1.000	0.845457	SUCCESS
Linear complexity	0.994	0.457133	SUCCESS
Random excursions	0.996	0.135379	SUCCESS
Random excursions variant	1.000	0.237967	SUCCESS
Longest runs of ones	0.998	0.453458	SUCCESS
Overlapping template of all ones	0.998	0.213579	SUCCESS
Rank	0.994	0.237794	SUCCESS
Runs	0.996	0.874754	SUCCESS
Serial	0.996	0.232765	SUCCESS
Universal statistical	0.996	0.575694	SUCCESS
Lempe-Ziv Compression Test	0.998	0.612345	SUCCESS

The Lyapunov exponent is also calculated by numerical simulation. The results show that the chaotic characteristics of this new map have no correlation to the parameter *b*. Furthermore, we propose a new image encryption algorithm based on this new chaotic map. Many statistical tests and security analysis are carried out to evaluate our algorithm, including histogram analysis, information entropy analysis, key space analysis, key sensitivity analysis, correlation analysis, resistance to differential attack analysis, and randomness analysis. The results show that our algorithm has an excellent security performance, and can be competitive with some other recently proposed image encryption algorithms. Four different plain images are test here, including natural image and computer generated image. The results also show that our algorithm is effective to different images, and has no content dependency.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61601215).

References

1. Alpar O (2014) Analysis of a new simple one dimensional chaotic map. Nonlinear Dyn 78:771–778
2. Cang SJ, Wang ZH, Chen ZQ, Jia HY (2014) Analytical and numerical investigation of a new Lorenz-like chaotic attractor with compound structures. Nonlinear Dyn 75:745–760
3. Chen G, Mao Y, Chui CK (2004) A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons Fractals 21:749–761
4. Chen CS, Wang T, Kou YZ, Chen XC, Li X (2013) Improvement of trace-driven I-Cache timing attack on the RSA algorithm. J Syst Softw 86(1):100–107
5. Coppersmith D (1994) The data encryption standard (DES) and its strength against attacks. IBM J Res Dev 38(3):243–250
6. Devaney R (1984) A piecewise linear model for zones of instability of an area-preserving map. Phys D 10(3):387–393
7. Henon M (1976) A two-dimensional mapping with a strange attractor. Math Phys 50:69–77
8. Hua ZY, Zhou YC, Pun CM, Philip Chen CL (2015) 2D Sine Logistic modulation map for image encryption. Inf Sci 297:80–94
9. Kaneko K (1993) Theory and application of coupled map lattices. John Wiley and Sons, Nwe York
10. Li CQ, Xie T, Liu Q, Cheng G (2014) Cryptanalyzing image encryption using chaotic logistic map. Nonlinear Dyn 78:1545–1551
11. Lorenz EN (1963) Deterministic nonperiodic flow. J Atmos Sci 20:130–141
12. Lu JH, Chen GR (2002) A new chaotic attractor coined. Int J Bifurcat Chaos 12:659–661
13. May RM (1976) Simple mathematical models with very complicated dynamics. Nature 261:459–465
14. Sprott J (2003) Chaos and time series analysis. Oxford University Press, Oxford
15. Sun F, Lu Z, Liu S (2010) A new cryptosystem based on spatial chaotic system. Opt Commun 283: 2066–2073
16. Tong XJ, Wang Z, Zhang M, Liu Y, Xu H, Ma J (2015) An image encryption algorithm based on the perturbed high-dimensional chaotic map. Nonlinear Dyn 80:1493–1508
17. Wang XY, Guo K (2014) A new image alternate encryption algorithm based on chaotic map. Nonlinear Dyn 76:1943–1950
18. Ye G, Wong KW (2013) An image encryption scheme based on time-delay and hyperchaotic system. Nonlinear Dyn 71(1–2):259–267
19. Zhang YQ, Wang XY (2014) Spatiotemporal chaos in mixed linear-nonlinear coupled logisitic map lattice. Physica A 402:104–118
20. Zhou Q, Liao X (2012) Collision-based flexible image encryption algorithm. J Syst Softw 85:400–407

LingFeng Liu was born in Nanchang, China, in 1986. He received the B. S. Degree in mathematics, the M. Sc degree in Information Science, Ph. D. Degree in Information Science from Huazhong University of Science and Technology, China, in 2007, 2009, and 2014, respectively. He is now work in the School of Software, Nanchang University of China. His research interests cover the area of chaos, secure communication and information theory, as well as cryptography.

SuoXia Miao was born in Heze, China, in 1986. She received the B. S. Degree in mathematics, the M. Sc degree in applied mathematics from Fuyang Teachers College and Huazhong University of Science and Technology, respectively in 2008 and 2010. She is now work in the Faculty of Science, Nanchang Institute of Technology. Her research interests cover the area of chaos, differential equation, as well as cryptography.