Synchronization of spatiotemporal chaotic systems and application to secure communication of digital image*

Wang Xing-Yuan(王兴元)†, Zhang Na(张 娜), Ren Xiao-Li(任小丽), and Zhang Yong-Lei(张永雷)

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology, Dalian 116024, *China*

(Received 11 August 2010; revised manuscript received 3 October 2010)

Coupled map lattices (CMLs) are taken as examples to study the synchronization of spatiotemporal chaotic systems. In this paper, we use the nonlinear coupled method to implement the synchronization of two coupled map lattices. Through the appropriate separation of the linear term from the nonlinear term of the spatiotemporal chaotic system, we set the nonlinear term as the coupling function and then we can achieve the synchronization of two coupled map lattices. After that, we implement the secure communication of digital image using this synchronization method. Then, the discrete characteristics of the nonlinear coupling spatiotemporal chaos are applied to the discrete pixel of the digital image. After the synchronization of both the communication parties, the receiver can decrypt the original image. Numerical simulations show the effectiveness and the feasibility of the proposed program.

Keywords: coupled map lattice, projective synchronization, digital image, secure communication

PACS: 05.45.Jn, 05.45.Xt **DOI:** 10.1088/1674-1056/20/2/020507

1. Introduction

A lot of real systems in nature can be described by chaotic systems which show chaotic behaviours with spatiotemporal evolution. Coupled map lattice[1] is the description of spatiotemporal chaos as the most common form. The form not only can be used more easily in mathematics and computing than many other formulas but also can present an extremely rich chaotic dynamics, so it is widely used in the field of spatiotemporal chaos. At present, the method called variable coupling is a common way to do research on spatiotemporal chaos synchronization, which is evolved directly by the same method used in the time chaos synchronization. This method can inhibit the evolution of the chaotic systems through the coupling between state variables, so as to achieve chaotic synchronization. Now, there are many representative studies of spatiotemporal chaos. A one-way coupled map lattice of spatiotemporal chaos synchronization scheme was mentioned by Hu and Yang.[2] Nekorkin and Verlarde[3] implemented the synchronization of two coupled map lattices. Xun and Xiu[4] achieved the synchronization of discrete chaotic systems by using variable structure control. Yue and Shi[5] implemented the space–time chaos synchronization by using discrete fuzzy control. Wang and Hou[6] achieved the spatiotemporal chaos synchronization of complex networks under the linear coupling by numerical analysis. In addition, many other people have done a lot of research in this field.[7−13] However, in these studies one mostly used the linear coupling method concerning state variable in drive-response system to achieve the synchronization. The linear coupling method has many advantages such as simplicity and easiness in application and small cost in synchronization, but if the chaotic system has very strong nonlinear performance, this method can often give poor result of synchronization. Therefore the nonlinear coupling method is necessarily used in order to well achieve the synchronization of spatiotemporal chaos.

In the present paper, we study the projection synchronization of discrete spatiotemporal chaotic systems using the nonlinear coupled method. First of all, separate linear terms from nonlinear terms of chaotic systems appropriately, then we can obtain the proper nonlinear terms to be used as a coupling function and finally we can achieve the projective synchronization of two one-dimensional coupled map lattices. That is to say, the state variables of the target system and response system have evolved into a proportional rela-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 60573172 and 60973152), the Doctoral Program Foundation of Institution of Higher Education of China (Grant No. 20070141014), and the Natural Science Foundation of Liaoning Province, China (Grant No. 20082165).

†Corresponding author. E-mail: wangxy@dlut.edu.cn

© 2011 Chinese Physical Society and IOP Publishing Ltd

tionship when the two systems are synchronized. This nonlinear coupled synchronization method is extended to the case of digital image secure communication. We apply the discrete characteristic of the spatiotemporal chaos system to the pixel points of the digital image, then we can successfully achieve the secure communication of a digital image in a safe secure communication channel. Simulation shows the effectiveness and feasibility of the program proposed in this paper.

2. Algorithm description

Consider the following one-dimensional discrete chaotic systems:

$$\boldsymbol{x}_{n+1}(i) = \boldsymbol{F}(\boldsymbol{x}_n(i)), \tag{1}$$

where n is discrete time; i is the grid-point of space lattice, $i = 1, 2, \ldots, L$, L is the size of the system; $\boldsymbol{x}_n(i) \in R^N$ is state variable of system; $\boldsymbol{F} : R^N \to R^N$.

Separate $F(\boldsymbol{x}_n(i))$ appropriately, then we will have

$$\boldsymbol{x}_{n+1}(i) = \boldsymbol{F}(\boldsymbol{x}_n(i)) = \boldsymbol{A}\boldsymbol{x}_n(i) + \boldsymbol{H}(\boldsymbol{x}_n(i)). \tag{2}$$

Here, $\boldsymbol{A}$ is the coefficient matrix for the linear term and each characteristic root can meet $|\lambda_i| < 1$ ($i = 1, 2, \ldots, L$), $\boldsymbol{H}(\boldsymbol{x}_n(i))$ is the remaining part which contains the nonlinear terms.

Theorem 1 Use the form of the discrete spatiotemporal chaotic system as system (2) serving as the drive system and assume the response system to be in the following form:

$$\boldsymbol{y}_{n+1}(i) = \boldsymbol{F}(\boldsymbol{y}_n(i)) + \boldsymbol{u}(\boldsymbol{x}_n(i), \boldsymbol{y}_n(i)), \tag{3}$$

where the coupling control term is $\boldsymbol{u}(\boldsymbol{x}_n(i)$ and $\boldsymbol{y}_n(i)) = \boldsymbol{A}\boldsymbol{y}_n(i) - \boldsymbol{F}(\boldsymbol{y}_n(i)) + \boldsymbol{H}(\boldsymbol{x}_n(i))/\boldsymbol{\beta}$, then systems (2) and (3) will realize the projection synchronization with the scale factor $\boldsymbol{\beta}$.

$$\lim_{n\to\infty} \boldsymbol{x}_n(i) = \boldsymbol{\beta}\boldsymbol{y}_n(i).$$

Here, $\boldsymbol{\beta} = \mathrm{diag}(\beta_1, \beta_2, \ldots, \beta_L)$.

Proof Suppose the error formula of the two systems is $\boldsymbol{e}_n(i) = \boldsymbol{x}_n(i) - \boldsymbol{\beta}y_n(i)$. Substitute Eqs. (2) and (3) into the error formula, then we will have

$$\begin{aligned}
&\boldsymbol{e}_{n+1}(i)\\
&= \boldsymbol{x}_{n+1}(i) - \boldsymbol{\beta}\boldsymbol{y}_{n+1}(i)\\
&= [\boldsymbol{A}\boldsymbol{x}_n(i) + \boldsymbol{H}(\boldsymbol{x}_n(i))] - \boldsymbol{\beta}[\boldsymbol{A}\boldsymbol{y}_n(i) + \boldsymbol{H}(\boldsymbol{x}_n(i))/\boldsymbol{\beta}]\\
&= \boldsymbol{A}\boldsymbol{x}_n(i) - \boldsymbol{\beta}\boldsymbol{A}\boldsymbol{y}_n(i)\\
&= \boldsymbol{A}[(\boldsymbol{x}_n(i)) - \boldsymbol{\beta}(\boldsymbol{y}_n(i))]\\
&= \boldsymbol{A}\boldsymbol{e}_n(i).
\end{aligned}$$

According to the stability criterion of discrete chaotic systems,[14,15] we have

$$\lim_{n\to\infty} \boldsymbol{e}_n(i) = 0.$$

That is to say, when $\boldsymbol{H}(\boldsymbol{x}_n(i))/\boldsymbol{\beta}$ is a coupled entry, systems (2) and (3) will achieve the projection synchronization with the scale factor $\boldsymbol{\beta}$.

3. Numerical simulation of synchronous

In this section, we use coupled map lattices as an example of simulation experiment, coupled map lattice model was proposed by Kaneko[1] initially, and its dynamics formula is expressed as

$$\begin{aligned}
x_{n+1}(i) = {} & (1-\varepsilon)f(x_n(i)) + \frac{\varepsilon}{2}(f(x_n(i-1))\\
& + f(x_n(i+1))),
\end{aligned} \tag{4}$$

where n is the time step; i ($i = 1, 2, \ldots, L$) is the grid coordinates, L being the grid point; ε is the coupling strength factor between the lattices; $x_n(i)$ is the state of the grid point i at time n. Take logistic map as local function $f(x_n(i))$

$$f(x_n(i)) = 1 - ax_n^2(i), \tag{5}$$

where a is the parameter, then system (1) will become

$$\begin{aligned}
x_{n+1}(i) = {} & (1-\varepsilon)(1-ax_n^2(i)) + \frac{\varepsilon}{2}((1-ax_n^2(i-1))\\
& + (1-ax_n^2(i+1))).
\end{aligned} \tag{6}$$

When $a = 1.8$ and $\varepsilon = 0.1$, system (6) will show spatiotemporal chaos phenomenon. Initial value of $x_n(i)$ is a random value between –1 and 1. Under the periodic boundary condition, we can observe the chaotic behaviours of 30 lattices in 200 time-steps iterative. Figure 1 shows chaotic attractors of system (6).

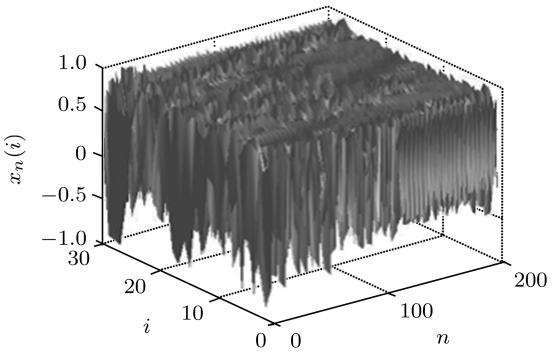


Fig. 1. Spatiotemporal evolution when $a = 1.8$ and $\varepsilon = 0.1$.

We assign system (4) to the drive system, and then the response system can be expressed as

$$y_{n+1}(i) = (1-\varepsilon)f(y_n(i)) + \frac{\varepsilon}{2}(f(y_n(i-1)) + f(y_n(i+1))) + u_n(i). \quad (7)$$

For simplicity, assign the coefficient matrix of linear term to $\boldsymbol{A} = \mathrm{diag}(0.5, 0.5, \ldots, 0.5)$, then we will have

$$u_n(i) = 0.5y_n(i) - (1-\varepsilon)f(y_n(i)) + \frac{\varepsilon}{2}(f(y_n(i-1)) + f(y_n(i+1))) + h(x_n(i))/\beta_i, \quad (8)$$

where $h(x_n(i))/\beta_i$ is the single lattice coupling term, and we will further have

$$h(x_n(i)) = (1-\varepsilon)f(x_n(i)) + \frac{\varepsilon}{2}(f(x_n(i-1)) + f(x_n(i+1))) - 0.5x_n(i). \quad (9)$$

We suppose that the error system is $e_n(i) = x_n(i) - \beta_i y_n(i)$ and assign the scale factor of the projective synchronization to $\boldsymbol{\beta} = \mathrm{diag}(2, 2, \ldots, 2)$. After step 100, add a control to the response system. Figure 2 shows the error system evolving with time. From Fig. 2 we can clearly see that drive system (4) and response system (7) achieve the projection synchronization.

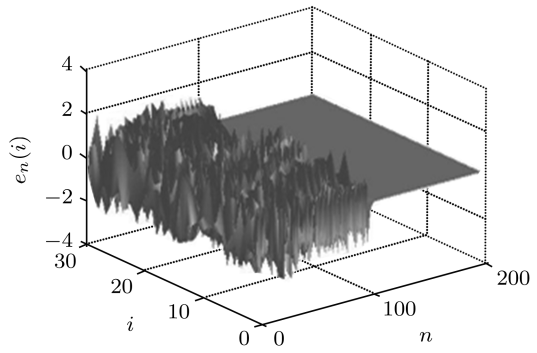


Fig. 2. Spatiotemporal evolution of projection synchronization.

4. Application of spatiotemporal chaotic synchronization in digital image secure communication

4.1. Secure communication

4.1.1. Program analysis

Spatiotemporal chaos can provide a large number of unrelated, pseudorandom and definite chaotic sequences, which can enhance the robustness and the anti-crack ability of the system. Because of these features the spatiotemporal chaos are used in secure communication field effectively.

In the present paper, we use the CML system model as a key generator of the transmitter and receiver. It is known from the above content, the chaotic systems of the sender and the receiver can achieve the synchronization through a synchronous transient process, which means that we can decrypt the plaintext (shown in Fig. 3) by the inverse operation of encryption function on cipher. Thanks to the infinite dimensionality and a high degree of complexity of the spatiotemporal chaotic system, the method mentioned above can reduce the burden of the channel transmissions and improve the transmission effectively. At the same time, this method can also improve the confidentiality performance of the system, the main reasons are as follows: i) users can customize the number of grids and the grid coupling coefficients, which determines the complexity of the system; ii) the image data and the spatiotemporal chaotic signals are the integrated complex, which are not easily cracked.

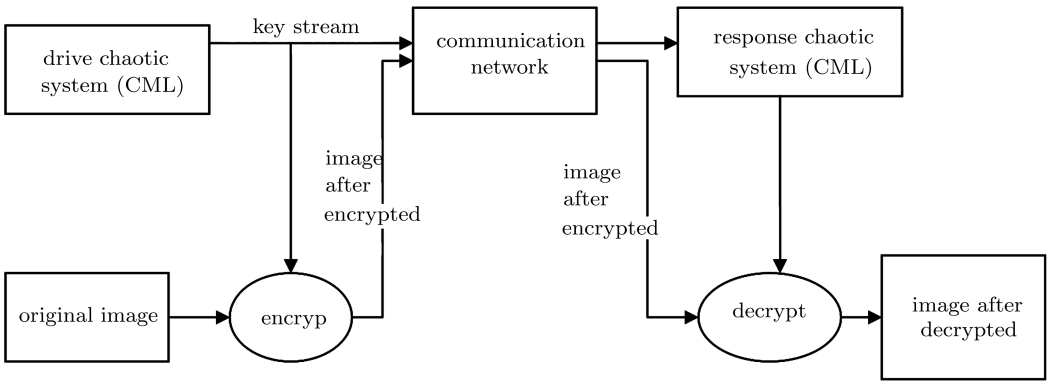


Fig. 3. Flow chart of secure communication system based on the spatiotemporal chaos synchronization.

Figure 4 shows the specific process of image secure communication scheme based on the spatiotemporal chaotic sequence. The process is as follows: read the image pixel data and then obtain the sequence numbers in CML systems according to the number of pixels. The method to obtain the sequence number is that in the sender part we use the system parameters (key) to drive the CML system. After that we can obtain the spatiotemporal chaos real sequence corresponding to the image pixel data generated by the system. But this numerical sequence is in the minority and it cannot encrypt the image pixel. We perform the fixed width binary treatment on the chaotic sequence mentioned in Ref. [16] and after that change the binary sequence into characteristic type. Finally the data signal of the original image can be encrypted. After the synchronization of sender and receiver, we sent the signals and system parameters to the receiver through the communication channel. So the CML response system in the receiver can reproduce the same synchronized chaotic sequence as the sender's, thus the receiver can decrypt the original image using the same binary chaotic sequence method mentioned above.

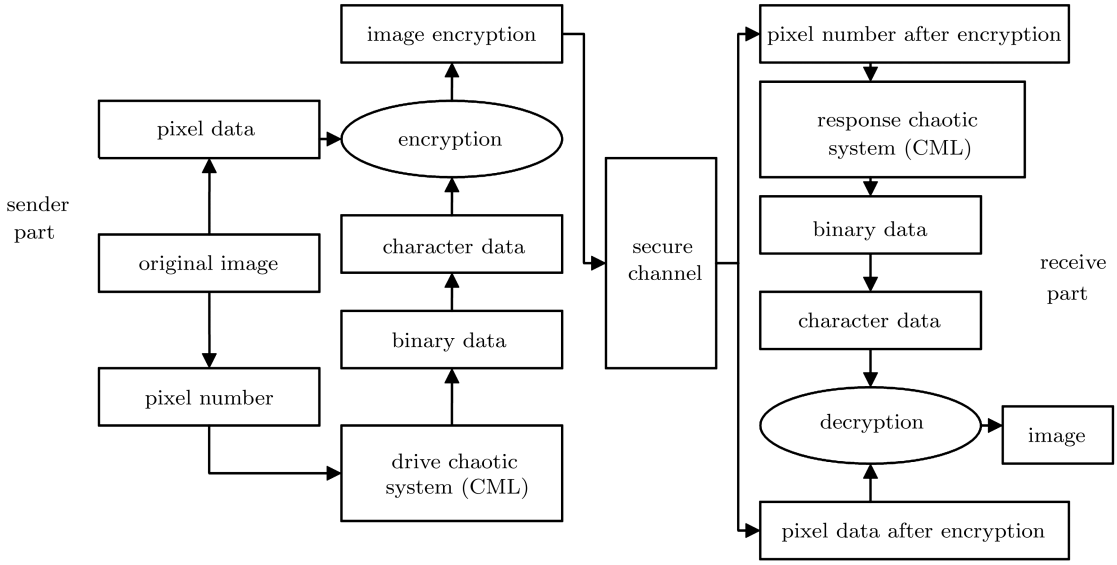


Fig. 4. Flow chart of secure communication system based on the spatiotemporal chaos synchronization.

4.1.2. Binarization process of chaotic sequence

The output of CML is a continuous real-valued sequence between –1 and 1. We should perform the binarization processing before using the sequence for image encryption. The methods are as follows: we use x_n^i as a binary sequence, in which i is the number of lattices in CML and n is the iteration number. The grid point value after a given number of iterations is a decimal, after binarization it is also a number of decimal sequences, $x_n^i = (0.a_{n+1}^i a_{n+2}^i a_{n+3}^i, \ldots, a_{n+m}^i)$, m is the binary precision. Therefore, $\{a_{n+1}^i a_{n+2}^i a_{n+3}^i, \ldots, a_{n+m}^i\}$ constitutes a pseudorandom binary sequence (PRBS). Because of the randomness of the chaotic orbit, the PRBS is distributed uniformly after using this method. The data of the grid i after n steps are: $x_1^i, x_2^i, \ldots, x_n^i$. Convert the value of each grid into binary one, then we will obtain the following binary matrix:

$$\begin{bmatrix} a_{1,1}^i & a_{2,1}^i & \cdots & a_{n,1}^i \\ a_{1,2}^i & a_{2,2}^i & \cdots & a_{n,1}^i \\ \cdots & \cdots & \cdots & \cdots \\ a_{1,m}^i & a_{2,m}^i & \cdots & a_{n,m}^i \end{bmatrix}.$$

4.1.3. Secure communication process

To speed up the rate of image encryption, the encryption process of this program just perform the XOR operation between the chaotic sequence after binarization and the original image in the sender part. in the decryption process we use the local chaotic sequence generated in the receiving party. Due to the same initial sequence of drive chaotic, we have the same chaotic sequence in the two parts, after performing the XOR operation with the received image we can have the original image. Encryption process is given below through VC6.0 simulation, and the decryption

process is similar.

(i) Read the pixel values and records. Read the height of the image named Height and width named Width. Read the image pixels in BMP format and put them in the array num[ ]. The image used has 65, 536 pixels, which means we will read 65536 characters and put them in num[ ].

(ii) Obtain the numbers from CML and convert them into binary numbers. After compiling CML formula using VC + + we can obtain the value of a grid after many iterations. Here, parameters (a, ε) of CML system and the initial value z_0 of the system are the keys and these digits are transmitted through the secure channel. In this paper, the number of image pixels is 65536 and we give $i = 10$ (the value of i is a key value, which is determined by the sender), which means that we read the values of the tenth grid of the 65536 iterations after 10000 iterations into the array $X[\ ]$ (take sequence numbers after CML stable iterative). The number of the decimal places is 65536 and change these decimals into binary numbers. The precision of binary decimal is 8 and store them into the two-dimensional array $N[c]\ [n]$, where $c = 65536$ is the number of rows and $n = 8$ is the number of columns. Change the eight numbers in each column into a character and store them into an array called byte[65536].

(iii) Encrypt the character array which has been obtained after the above steps (i) and (ii): do the XOR operation between the image pixel array num[ ] and the character array byte[ ] obtained from the CML formula. Write the result into the array num[ ] and write back to the encrypted image using the statement fwrite (& num[i], 1,1, cipher) . Finally the image can be encrypted.

(iv) Put the encrypted image into the secure channel for data transmission. We can see from the above steps that there are many keys in this encryption process, which indicate that the periodic phenomenon will not happen. This method has a good encryption performance such that the image cannot be decrypted easily.

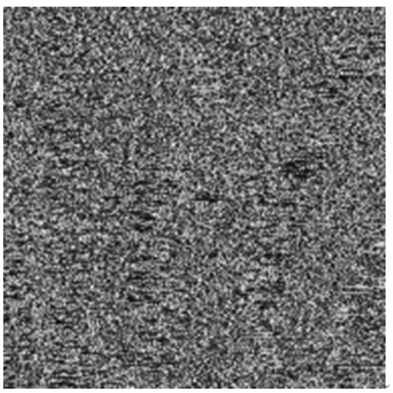
4.2. Numerical simulation

This part of the paper is devoted to the numerical simulation using VC++ 6.0. We choose $f(x) = 1 - ax_n^2(n)$, where $a = 1.8$. We also choose lattice parameters including grid points $i = 30$, iteration number $n = 80000$, and coupling parameter $\varepsilon = 0.1$. The initial value z_0 of the system is 0.5 when the number of points is even or the value is –0.5 when the number of grid points is odd. We perform the simulation following the steps mentioned above using the lattice iteration data of grid $m = 10$.

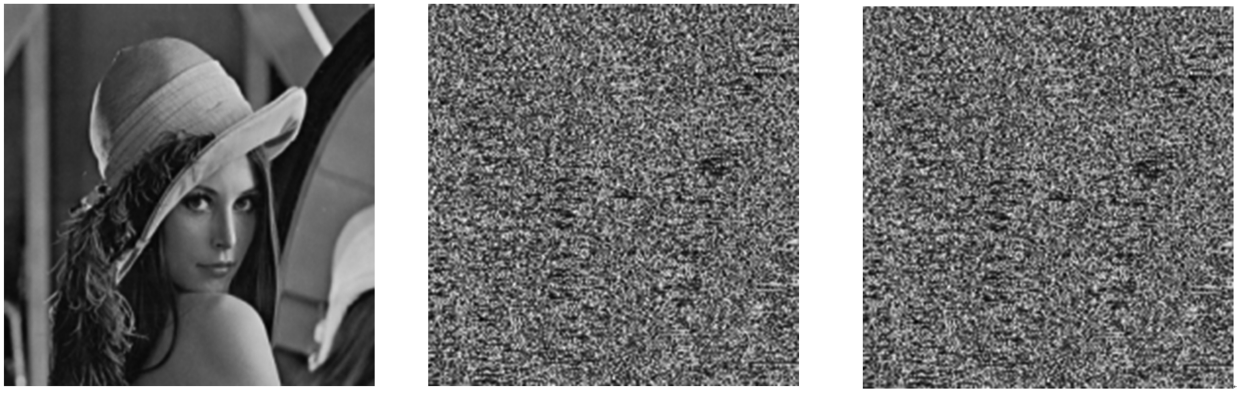
Results for the encryption and the decryption are shown in Fig. 5. Figure 5(a) shows the 256 × 256 dot matrix grayscale Lena image which is chosen to send. Figure 5(b) exhibits the transmission image after being modulated by spatiotemporal chaotic signal, from which we can see that the image signal has been completely covered by the chaotic signal. The image after being encrypted is completely different from the original image which is similar to a random image. That is to say, we obtain the encryption result. In order to obtain the original image, one should know the dynamic equation of chaotic system and use the same system parameters as the sender part: if not, it is almost impossible to unveil the original image. Experimental results verify the feasibility and correct of the program.



(a) original image



(b) ciphered image

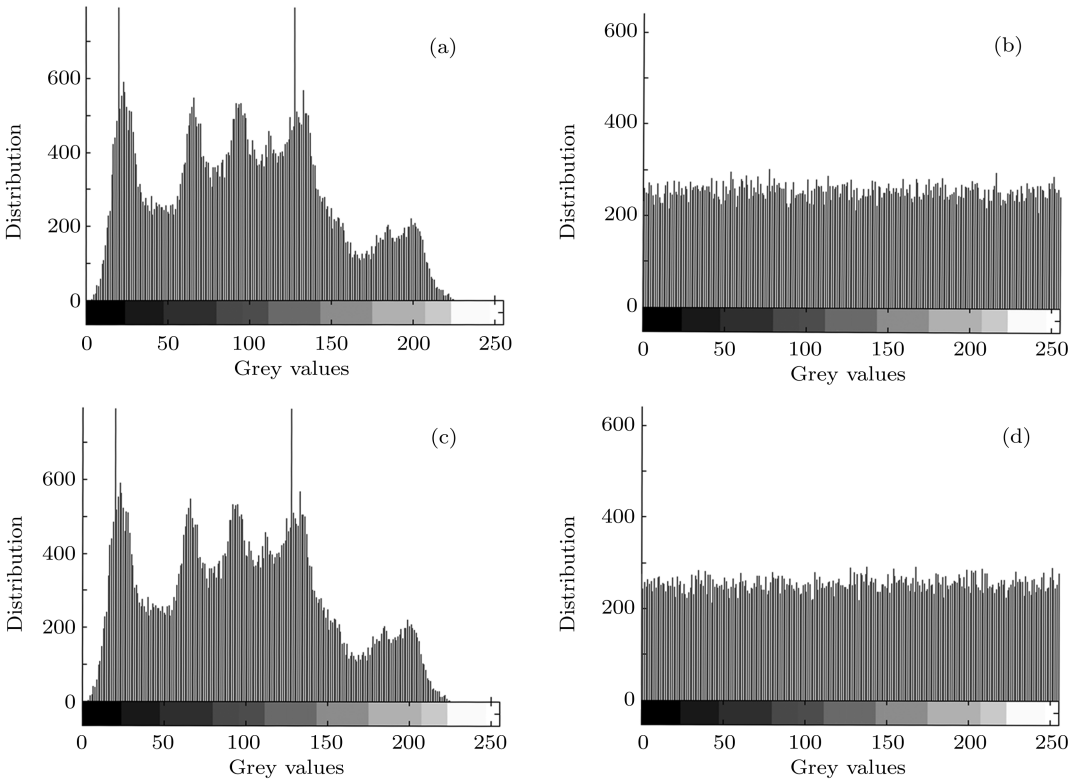


(c) correct keys decrypted image. (d) correct keys decrypted image ($a = 1.800001$) (e) correct keys decrypted image ($z_0 = 0.499999$)

Fig. 5. Results for the encryption and decryption.

When we use the correct system parameters (key) in the response system, we can decrypt the right results as shown in Fig. 5(c), from which it follows that encrypted image is correctly solved. Figures 5(d) and 5(e) show the experimental results of the system ability of anti-crack. Figure 5(d) indicates the decryption result when $a = 1.800001$ in logistic map, from which we can know that the transmitted image cannot be solved properly even if the system parameters have a very small error. This algorithm has a strong anti-crack ability. Figure 5(e) shows the decryption results when the initial value $z_0 = 0.499999$, from which we can see that the transmitted image cannot be solved even if the initial value of system has a very small error. Features mentioned above indicate the sensitivity to initial value of chaotic systems and also show that the algorithm has a robust breaking capacity.

Figure 6 shows the distributions of the pixel gray values of Fig. 5. It can be seen from Fig. 6 that the statistical feature of distribution of pixel gray levels is very obvious. But this distribution has disappeared after encryption. In the cipher text, pixel gray value distribution is uniform and after using the wrong key to decrypt, it is difficult to find a rule from the distribution of pixel gray values.



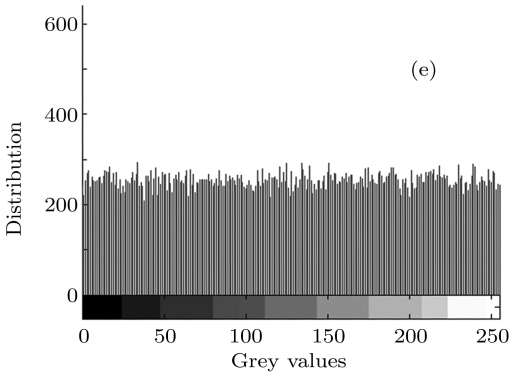


Fig. 6. The distribution of the pixel gray value for (a) original image, (b) ciphered image, (c) correct keys decrypted image, (d) correct keys decrypted image ($a = 1.800001$), (e) correct keys decrypted image ($z_0 = 0.499999$).

4.3. Security analysis

4.3.1. Key space

From the program, we can see that the security of system depends on the security of system parameters of both sending and receiving parts. System parameters are equivalent to the keys of traditional cryptography. Here we analyse only the numerical parameters. In the program, there are six real parameters (a, z_0, ε, i, n, m) and an assumption that the double-precision (2^{-32}) is used. Then the system parameter space size is $2^{32\times 6} = 2^{192}$, which means that the key space number is nearly 192. As to the current condition of view, this programme can stand a brute-force attack.

4.3.2. Key sensitivity

From the experimental results of perturbation in the parameter a and the initial value, we can see that the system has a strong sensitivity if the key does not match. Figures 5(d) and 5(e) show the image decryption result under the perturbation to parameters a and z_0 respectively. One cannot obtain a clear signal without using a precise key value so this programme provides users with a large key space.

4.3.3. Entropy

Entropy is a very important parameter to measure the randomness. Assume that the information source is m, then the information entropy will be

$$H(m) = \sum_{i=0}^{2^n-1} p(m_i) \log_2 \frac{1}{p(m_i)}. \tag{10}$$

Here, the value of $p(m_i)$ is the probability of m_i. Suppose that total state value of m is 2^8 and the probability values of state information are the same. According to Eq. (10) it is available that

$$H(m) = 8.$$

The formula indicates that the information is completely random. When the information is encrypted, the closer to 8 the information entropy of cipher text, the smaller will the information leakage be, that is to say, the more secure will the password system be. Use Eq. (10) on the encrypted Lena map and perform the calculation, then we will have

$$H(m) = 7.997.$$

The result is close to 8, which means that the result is almost an ideal value. So the possibility of the information leakage of code system designed in this passage is small.

4.3.4. Correlation of adjacent pixels

Correlation of adjacent pixels is

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{11}$$

where

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)),$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i,$$

and

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2.$$

We select 1000 pairs of adjacent pixels in plain text and cipher text randomly respectively (from horizontal, vertical, main diagonal, and subsidiary diagonal directions). By calculation from Eq. (11), we know that the relevance of adjacent pixels of original

image Lena is 0.935832 and the correlation of adjacent pixels in ciphered text is –0.033331, which shows that the correlation between adjacent pixels is large but the correlation between adjacent pixels is reduced greatly after being encrypted. The encryption works well.

The results of entropy and correlation of adjacent pixels show that the ciphered text can stand a statistical attack well.

5. Conclusion

Coupled map lattices (CMLs) are taken as examples to study the synchronization of spatiotemporal chaotic systems. In this paper, we use the nonlinear coupled method to implement the synchronization of two coupled map lattice systems. Through the appropriate separation of the linear term from the nonlinear term of the spatiotemporal chaotic system, we set the nonlinear term as the coupling function and then we can achieve the synchronization of two coupled map lattices. After that, we implement the secure communication of digital image using this synchronization method. Then, the discrete characteristics of the nonlinear coupling spatiotemporal chaos are applied to the discrete pixel of the digital image. After the synchronization of both communication parties, the receiver can decrypt the original image. Numerical simulations show the effectiveness and the feasibility of the proposed program.

The study of spatiotemporal chaos is still in its infancy. The applications to secure communication are not many. As to initial value and the boundary condition, the spatiotemporal chaos has a high degree of sensibility, which means that spatiotemporal chaos model has greater volume keys and key space than the time chaos model. Thanks to the key capacity, it is possible to resist to a brute-force attack. Through the analyses of correlation, entropy and the key sensitivity between neighbouring pixels of coupled map lattice system in driven model, it can be shown that the secure communication scheme presented in this paper has a strong anti-crack ability and a great future.

References

[1] Kaneko K 1985 *Prog. Theor. Phys.* **74** 1033

[2] Hu G and Yang J Z 1997 *Phys. Rev.* E **56** 2738

[3] Nekorkin V I and Verlarde M G 1997 *Phys. Lett.* A **236** 505

[4] Xun H Y and Xiu M S 2002 *Chaos, Solitons and Fractals* **14** 1077

[5] Yue J and Shi Y Y 2003 *Chaos, Solitons and Fractals* **17** 967

[6] Wang M S and Hou Z H 2006 *Chin. Phys.* **15** 2553

[7] Emura T 2006 *Phys. Lett.* A **349** 306

[8] Zhang H G 2007 *Acta Phys. Sin.* **56** 3796 (in Chinese)

[9] Yue L J and Shen K 2005 *Acta Phys. Sin.* **54** 5671 (in Chinese)

[10] Zhang H G, Ma D Z and Wang Z S 2010 *Acta Phys. Sin.* **59** 147 (in Chinese)

[11] Alexander A and Uzrich P 2008 *Phys. Rev.* E **77** 016201

[12] Zhang H G 2006 *Acta Phys. Sin.* **55** 2687 (in Chinese)

[13] Lü L and Li G 2008 *Acta Phys. Sin.* **57** 7517 (in Chinese)

[14] Chen G and Lai D 1998 *Int. J. Bifurc. Chaos* **8** 1585

[15] Fuh C C and Tsai H H 2002 *Chaos, Solitons and Fractals* **13** 285

[16] Li P and Li Z 2006 *Phys. Lett.* A **349** 467