A new parallel image cryptosystem based on 5D hyper-chaotic system

Hong-Mei Yuan, Ye Liu, Tao Lin, Ting Hu, Li-Hua Gong

www.elsevier.com/locate/image

PII: S0923-5965(17)30001-2
DOI: http://dx.doi.org/10.1016/j.image.2017.01.002
Reference: IMAGE15163

To appear in: *Signal Processing : Image Communication*

Received date: 30 August 2016
Revised date: 2 December 2016
Accepted date: 2 January 2017

Cite this article as: Hong-Mei Yuan, Ye Liu, Tao Lin, Ting Hu and Li-Hua Gong, A new parallel image cryptosystem based on 5D hyper-chaotic system *Signal Processing : Image Communicatio* http://dx.doi.org/10.1016/j.image.2017.01.002

A new parallel image cryptosystem based on 5D hyper-chaotic system

Hong-Mei Yuan, Ye Liu*, Tao Lin, Ting Hu, Li-Hua Gong

Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China

*Corresponding author. E-mail address: liuye@ncu.edu.cn

Abstract

A new parallel image cryptosystem is presented using 5D hyper-chaotic system. The 5D hyper-chaotic system is combined with the Logistic map for the generation of pseudo-random sequences of better properties. Different from the general image cryptosystems, plain image is divided into levels. Pixels within the same level are processed in a parallel way. Moreover, the encryption procedure of each pixel is directly decided by two encrypted pixels which are closest to it of its neighbor level. In this way, the provided 5D hyper-chaotic based parallel image cryptosystem could achieve excellent plaintext sensitivity and relatively satisfactory speed performance. Numerous simulations are conducted, and security analyses based on the simulation results are exhibited in support of the security and availability of the proposed 5D hyper-chaotic based parallel image cryptosystem.

Keywords

Parallel image cryptosystem; 5D hyper-chaotic system; Pseudo-random sequences

1. Introduction

Digital images are widespread over the public channels with the rapid improvement of multimedia and the security concerns about the digital images with vital information are increasing simultaneously. An increasing number of researchers are paying attention to image security. Many image cryptosystems were developed to enhance the security of these images. Due to the intrinsic features of digital images such as high redundancy, high correlation between two adjacent pixels and bulk date capacity [1], the traditional methods (such as DES, AES and IDEA) fail to satisfy the requirements of digital image encryption commendably. In contrast, the chaos-based approaches are demonstrated to be secure and efficient.

The properties of chaotic systems, e.g., pseudo-randomness, ergodicity, initial values sensitivity and unpredictability, can meet the demands of the confusion and

diffusion in cryptography. Therefore, much effort has been devoted to the research of chaotic image cryptosystems [2-7]. Nowadays, there are mainly two kinds of chaotic systems for generating chaotic sequences: the common chaotic systems that only possess one positive Lyapunov exponent and the hyper-chaotic systems that possess more than one positive Lyapunov exponents. Compared with the normal chaotic systems, the hyper-chaotic system has a larger quantity of parameters and more complex chaotic orbits generally, which is identified as an important guarantee of the security of image cryptosystems. Hence, the applications of hyper-chaotic systems have been extensively explored in image cryptosystems [8-11]. Gao proposed a chaotic image cryptosystem where a 4D (four-dimensional) hyper-chaotic system was introduced and the generated hyper-chaotic sequences were used in the modification of the pixel values of the shuffled image [12]. But Rhouma found that it was weak against chosen plaintext/ciphertext attacks due to the fact that the generation of the keystreams neither depended on the plaintext nor did it depend on the ciphertext. Moreover, the encryption operations of pixels were independent of each other. Then Rhouma proposed an improved image cryptosystem, in which the generated keystreams were ever-changing in the encryption process and the CBC (Cipher-Block changing) method was applied [13]. Recently, Jeng has pointed that the two image cryptosystems abovementioned were both less sensitive to the change of plain image, which drags them to suffer from the statistical attacks [14]. Moreover, the traditional CBC method would greatly limit the encryption speed. The reason was that pixels are encrypted sequentially i.e. a pixel could be encrypted only when the encryption operation of its previous pixel was finished. In order to enhance the encryption effect and efficiency of image cryptosystems, a large amount of image encryption schemes were described [7, 15-20]. Parallel image encryption is a valid manner to improve efficiency. But the conventional CBC-like mode must be eliminated to allow parallel image encryption [20], which will lead to the less plaintext sensitivity.

In order to accelerate operating speed while presuming the security of image cryptosystems, a new parallel image cryptosystem is designed by employing a 5D (five-dimensional) hyper-chaotic system. Firstly, plain image is classified into levels. The encryption operations of plain image are implemented hierarchically and pixels within the same level are encrypted concurrently. Levels are encrypted sequentially. Compared with the traditional CBC encryption method, it is time-saving. Moreover, each pixel in the current level is influenced by two encrypted pixels in the previous level. The processed pixels, in turn, will have effect on the pixels in the next level. Consequently, the cipher image is sensitive to the plain image. Furthermore, the rotation operations further the impacts of the changed pixels on cipher image. In this manner, we can trade off between the security and efficiency of the presented parallel

image cryptosystem. Moreover, the performances of both two respects are verified to be content by the security analyses in section 3.

The rest of this paper is organized as follows. In Section 2, we review the 5D hyper-chaotic system; give an introduction to the preprocessing method of the hyper-chaotic sequences and the proposed parallel image cryptosystem. Computer simulation results and detailed security analyses are provided in Section 3. Section 4 draws a conclusion.

2. Parallel image cryptosystem based on the 5D hyper-chaotic system

The 5D hyper-chaotic system based parallel image cryptosystem will be described in detail from the following aspects: the generation of the pseudo-random sequences; the insertion of the chaotic sequences; the classification of the plain image and the encryption operations. The total encryption flowchart is shown as Fig. 1. We assume that the plain image is an $M \times N$ 8-bit gray image.

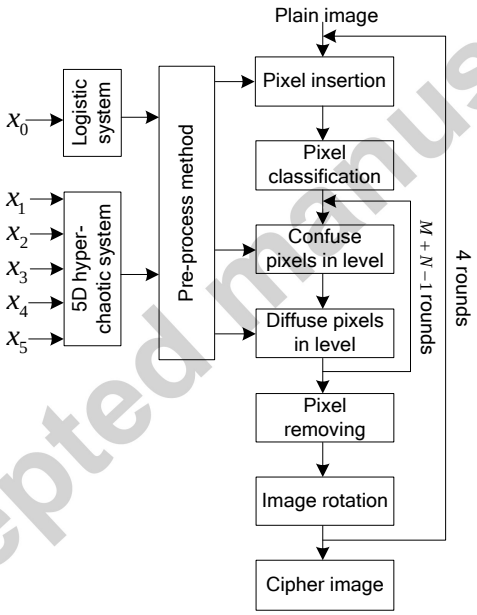


Fig. 1. Flow diagram of the encryption process.

2.1. Generation of the pseudo-random sequences

The generation of pseudo-random sequence is based on a 5D hyper-chaotic system. This section will introduce how to generate the pseudo-random sequence in detail and analysis the properties of the generated pseudo-random sequences.

2.1.1. 5D hyper-chaotic system

Chaos is a ubiquitous phenomenon in nonlinear dynamic system. The Lyapunov exponent can show the feature of most nonlinear dynamic systems and its numerical number can reflect the radiation degree of adjacent locus. The hyper-chaotic systems with more than one positive Lyapunov exponents are usually with more complex structure and dynamic behaviors than those of the chaotic systems with only one positive Lyapunov exponent. But some hyper-chaotic systems can be cracked by some parametric identification technologies [21] due to the fact that their radiation degree is still simpler and the order of nonlinear product terms is low [22]. Hence, hyper-chaotic systems with greater complexity are needed to improve the security of cryptosystems.

In Ref. [22], a new 5D hyper-chaotic system is described as follows:

$$\begin{cases} \dot{x}_1 = a\left(x_2 - x_1\right) + x_2 x_3 x_4 \\ \dot{x}_2 = b\left(x_1 + x_2\right) + x_5 - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_2 - dx_3 - ex_4 + x_1 x_2 x_4 \\ \dot{x}_4 = -fx_4 + x_1 x_2 x_3 \\ \dot{x}_5 = -g\left(x_1 + x_2\right) \end{cases} \tag{1}$$

Where a, b, c, d, e, f, g are system parameters, when $a=30$, $b=10$, $c=15.7$, $d=5$, $e=2.5$, $f=4.45$, $g=38.5$, the corresponding Lyapunov exponents are 5.12, 0.9, 0, -10.41, -25.08.

Table 1 has shown some hyper-chaotic systems and summarized some characteristics. The characteristics shown in Table 1 support the following results:

1. The maximum Lyapunov exponent of the employed 5D hyper-chaotic system is bigger than that of most hyper-chaotic systems. Hence, it has more complex dynamic behaviors.

2. It has seven parameters, which indicates that a larger keys space of the corresponding cryptosystem is available for resistance to the brute-force attack.

3. It has cubic nonlinear product terms while the order of other systems is two generally. Accordingly, it has better resistance to some parametric identification technologies.

Therefore, the 5D hyper-chaotic system is more suitable for secure and reliable image cryptosystems.

Table 1 Hyper-chaotic nonlinear dynamic systems.

Name	Hyper-chaotic system	Order of nonlinear product terms	Parameters	Lyapunov exponents
Hyper-chaotic Lü system in Ref. [24]	$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=-xz+cy\\ \dot{z}=xy-bz\end{cases}$	TWO	$a=36,\ b=3,$ $c=20$	$\lambda_1=1.5046,$ $\lambda_2=0,$ $\lambda_3=-22.5044$
Hyper-chaotic Chen system in Ref. [12]	$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=-xz+dx+cy-q\\ \dot{z}=xy-bz\\ \dot{q}=x+k\end{cases}$	TWO	$a=36,\ b=3,$ $c=28, d=-16,$ $k=0.2$	$\lambda_1=1.552,$ $\lambda_2=0.023,$ $\lambda_3=0,$ $\lambda_4=-12.573$
Hyper-chaotic Rossler system in Ref. [23]	$\begin{cases}\dot{x}=-y-z\\ \dot{y}=x+ay+w\\ \dot{z}=b+xz\\ \dot{w}=-cz+dw\end{cases}$	TWO	$a=0.25,\ b=3,$ $c=0.5, d=0.05$	$\lambda_1=0.112,$ $\lambda_2=0.019,$ $\lambda_3=0,$ $\lambda_4=-25.188$
Hyper-chaotic Lorenz system in Ref. [25]	$\begin{cases}\dot{x}=-a(x-y)+u\\ \dot{y}=-xz+rx-y\\ \dot{z}=xy-bz\\ \dot{q}=-xz+du\end{cases}$	TWO	$a=10,\ r=28,$ $b=8/3, d=1.3$	$\lambda_1=0.39854,$ $\lambda_2=0.24805,$ $\lambda_3=0,$ $\lambda_4=-12.913$
Hyper-chaotic system in Ref. [26]	$\begin{cases}\dot{x}=a(y-x)\\ \dot{y}=bx-kxz+w\\ \dot{z}=-cz+hx^2\\ \dot{w}=-dx\end{cases}$	TWO	$a=10,\ b=40,$ $c=2.5, k=1,$ $h=4,\ d=10.6$	$\lambda_1=1.1491,$ $\lambda_2=0.12688,$ $\lambda_3=0,$ $\lambda_4=-13.767$
Hyper-chaotic system in Ref. [27]	$\begin{cases}\dot{x}_1=a(x_2-x_1)+x_4+x_5\\ \dot{x}_2=cx_1-x_1x_3-x_2\\ \dot{x}_3=x_1x_2-bx_3\\ \dot{x}_4=-x_1x_3+px_4\\ \dot{x}_5=qx_1\end{cases}$	TWO	$a=10,$ $b=8/3,$ $c=28,\ p=1.3$ $,\ q=2.5$	$\lambda_1=0.4195,$ $\lambda_2=0.2430,$ $\lambda_3=0.0145,$ $\lambda_4=0,$

				$\lambda_5 = -13.0405$
Ours	$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + x_2 x_3 x_4 \\ \dot{x}_2 = b(x_1 + x_2) + x_5 - x_1 x_3 x_4 \\ \dot{x}_3 = -cx_2 - dx_3 - ex_4 + x_1 x_2 x_4 \\ \dot{x}_4 = -fx_4 + x_1 x_2 x_3 \\ \dot{x}_5 = -g(x_1 + x_2) \end{cases}$	THREE	$a = 30$, $b = 10$, $c = 15.7$, $d = 5$, $e = 2.5$, $f = 4.45$, $g = 38.5$	$\lambda_1 = 5.12$, $\lambda_2 = 0.9$, $\lambda_3 = 0$, $\lambda_4 = -10.41$, $\lambda_5 = -25.08$

2.1.2. Preprocessing of chaotic sequences

Four-order Runge-Kutta method are implemented to iterate the 5D hyper-chaotic system. Preprocessing of each hyper-chaotic sequence is necessary to endow them better properties of distribution, randomness, auto-correlation and cross-correlation. The preprocessing function described in Ref. [28] is expressed as

$$x'_n = x_n 10^l - \text{round}\left(x_n 10^l\right) \tag{2}$$

where $\text{round}(x)$ returns the nearest integer to x.

Based on the above preprocessing function, a preprocessing method is designed to further enhance the security of our 5D hyper-chaotic based parallel image cryptosystem. The steps for generating pseudo-random sequences are as below

Step 1 The logistic map is iterated $h_0 + M \times N$ times. It is shown as

$$y_{n+1} = \mu y_n (1 - y_n) \tag{3}$$

where $\mu \in [0,4]$, $y_n \in (0,1)$ and h_0 is a constant. When $3.569945 \le \mu \le 4$, The system is in chaotic state. The first h_0 values are abandoned to reduce the harmful effect of transitional procedure and a new chaotic sequence $Y = \{y_1, y_2, \ldots, y_{M \times N}\}$ is obtained.

Step 2 The value domain of Y is changed by Eq. (4) and then a new sequence $m = \{m_1, m_2, \ldots, m_{M \times N}\}$ is obtained.

$$m_i = \text{floor}(Y_i 10^4 \bmod 3) + 1 \tag{4}$$

where $\text{floor}(x)$ returns x to the nearest integers less than or equal to x and $a \bmod b$ returns the remainder after division.

Step 3 The 5D hyper-chaotic system is iterated 1000 times in advance to eliminate the transient response. Then the 5D hyper-chaotic system is iterated $(M \times N)/4$ times to generate five chaotic sequences $x_1 = \{x_{11}, x_{12}, \ldots, x_{1M\times N/4}\}$, $x_2 = \{x_{21}, x_{22}, \ldots, x_{2M\times N/4}\}$, $x_3 = \{x_{31}, x_{32}, \ldots, x_{3M\times N/4}\}$, $x_4 = \{x_{41}, x_{42}, \ldots, x_{4M\times N/4}\}$ and $x_5 = \{x_{51}, x_{52}, \ldots, x_{5M\times N/4}\}$.

Step 4 Four sequences are selected from the five chaotic sequences. Then the selected sequences are combined to form a new mixed-chaotic sequence with the length MN. There are 120 kinds of arrangement methods for each sequence according to the Combination Theorem in mathematics. Then the arrangement methods are chosen to get mixed-chaotic sequences K_1, K_2, K_3 and K_4. Therefore, there are totally $A(120,4) > 10^8$ possible combinations. In the example presented in this paper, $K_1 = \{x_4, x_1, x_3, x_2\}$, $K_2 = \{x_5, x_4, x_2, x_3\}$, $K_3 = \{x_1, x_3, x_2, x_5\}$ and $K_4 = \{x_2, x_5, x_3, x_1\}$.

Step 5 Four sequences K_1', K_2', K_3' and K_4' are obtained by rearranging the mixed-chaotic sequences K_1, K_2, K_3 and K_4, respectively. And the processes of the rearrangement are as

$$[f_y, l_y] = \text{sort}(Y) \tag{5}$$

$$K_j'(i) = K_j(l_y(i)) \tag{6}$$

where $i = 1, 2, \ldots, M \times N$, $j = 1, 2, 3, 4$, f_y is the new series of sequence Y and l_y is the index value of f_y.

Step 6 Four improved mixed-chaotic sequences k_1', k_2', k_3' and k_4' are acquired by Eq. (2) in which the exponent l is replaced with the sequence m and x_n represents the sequences K_1', K_2', K_3' and K_4', respectively.

Step 7 The improved mixed-chaotic sequences k_1', k_2', k_3' and k_4' are mapped into interval $[0, 255]$ by Eq. (7). Finally, four processed pseudo-random sequences k_1, k_2, k_3 and k_4 are formed.

$$k_i = \text{floor}\left(\left(\text{abs}(k_i') \times 10^{12}\right) \bmod 256\right) \tag{7}$$

where $i=1,2,3,4$, $\mathrm{abs}(x)$ returns the absolute value of x.

Fig. 2(a) is the auto-correlation of sequences x_1 and Fig. 2(c) of k_1'; Fig. 2(b) is the cross-correlation between x_1 and x_2; Fig. 2(d) between k_1' and k_2'. It can be seen that the auto-correlation of the improved mixed-chaotic sequence k_1' closely resembles the delta function and the cross-correlation between k_1' and k_2' fluctuates around zero. Both of the two properties of the improved sequences are better than that of the original chaotic sequences. The characteristics of other improved mixed-chaotic sequences are proved to be similar to that of the sequence k_1'.

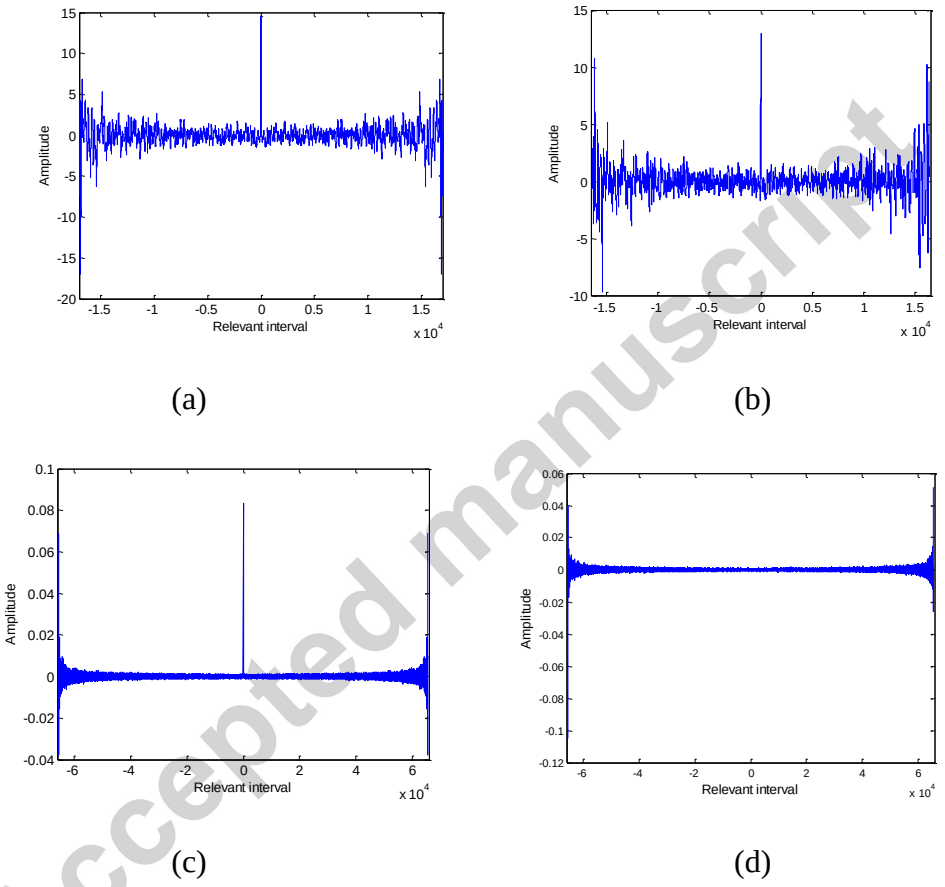


Fig. 2. The characteristics of sequences: (a) autocorrelation of sequence x_1, (b) cross-correlation between sequence x_1 and x_2, (c) autocorrelation of sequence k_1', (d) cross-correlation between sequence k_1' and k_2'.

2.2. The proposed parallel image cryptosystem

2.2.1. Insertion of the pseudo-random sequence

Because the encryption operation for each pixel is influenced by its neighbor pixels (namely the upper one and the left one) as described in the following sections, some extra pixels are required for encrypting the pixels in the first row and column.

Hence, an insertion method is designed in the parallel image cryptosystem. The inserted pixels are creamed off to encrypt the pixels in the first row and column. The sequence k_4 is used to perform the insertion operation. k_4 is divided into two sequences k_r and k_c whose size is $N\times 4$ and $M\times 4$, respectively. And the division equation is defined as

$$\begin{cases} k_r(n,r)=k_4(1+2k), & n=1,2,\ldots,N, \\ k_c(m,r)=k_4(2(k+1)), & m=1,2,\ldots,M, \end{cases} \quad r=1,2,3,4 \tag{8}$$

where $k=1,2,\ldots,(M+N)\times 2$, r is the rotation times. Then k_r and k_c are inserted into the plain image as the first row and the first column by the following equations.

$$P'(1,\ 2:N+1)=k_r(:,\ r) \tag{9}$$

$$P'(2:M+1,\ 1)=k_c(:,\ r) \tag{10}$$

$$P'(2:M+1,\ 2:N+1)=P \tag{11}$$

P is the plain image and P' is the processed image whose first row as well as column is a random chaotic sequence, as shown in Fig. 3. In Fig. 3, the dark triangles represent the inserted pseudo-random sequences and the filled circles represent pixels.

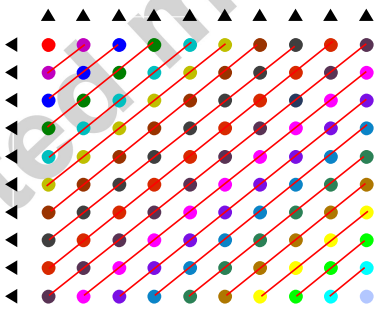


Fig. 3. The classification of a 10×10 plain image.

2.2.2. Classification of plain image

Different from the CBC-like encryption mode, parallel encryption mode can reduce the encryption time. But it cannot fulfill the diffusion requirement as the CBC-like encryption mode, which makes the cryptosystem more vulnerable to plaintext attack for lacking of plaintext sensitivity. Although some researchers exchange the information between different processing elements as compensation [20], the diffusion result cannot commendably satisfy the requirement of cryptosystem.

In order to enhance the diffusion effect and improve efficiency, a new parallel image cryptosystem is described. And we have provided a classification of plain image. Fig. 3 gives an illustration to the classification of a 10×10 plain image. It can be seen that pixels in the same counter-diagonal, which are marked with same color, are set into the same level. The classification is conducted from top to bottom and left to right. Firstly, the pixel both in the first row and column is deemed as $L(1)$, pixels on the counter-diagonal after $L(1)$ is $L(2)$, and so on, until it gets to $L(10)$ which is in the middle of the image. And the counter-diagonal after $L(10)$ is recorded as $L(-9)$, that after $L(-9)$ is $L(-8)$, and so on until the $L(-1)$. The classification for an image of size $M\times N$ can be deduced from this.

By this manner, the plain image is divided into levels. Pixels in the same level are independent of one another and levels are encrypted sequentially. For pixels in each level, its neighbor pixels (the upper one and the left one) are both in the previous encrypted level. Hence, the encrypted pixels within the previous encrypted level are introduced into the current level for furthering the diffusion effect like the CBC mode, which is detailed described in the next section. As a result, the corresponding image cryptosystem increases the plaintext sensitivity while encrypting the image in parallel.

2.2.3. Confusion and diffusion method

P' is the source image in the confusion and diffusion stages. Pixels in the same level are encrypted simultaneously. Moreover, the encryption operation starts from the point $P'(2,2)$ as exhibited in Fig. 3 and the pixels on the first row and column in P' are copied into the matrixes C'' by Eqs. (12)-(13).

$$C''(1,2:N+1)=P'(1,2:N+1) \tag{12}$$

$$C''(2:M+1,1)=P'(2:M+1,1) \tag{13}$$

The confusion and diffusion approaches are given as

$$j'=j+\left(k_3''(i-1,j-1)+C''(i,j-1)\right)\bmod(M+1-j) \tag{14}$$

$$C'(i-1,j-1)=P'(i,j') \tag{15}$$

$$P'(i,j')=P'(i,j) \tag{16}$$

$$\begin{aligned} C''(i,j) = &\left(k_1''(i-1,j-1) + C'(i-1,j-1)\right) \bmod 256 \\ &\oplus \left(C''(i-1,j) + C''(i,j-1)\right) \bmod 256 \\ &\oplus k_2''(i-1,j-1) \end{aligned} \tag{17}$$

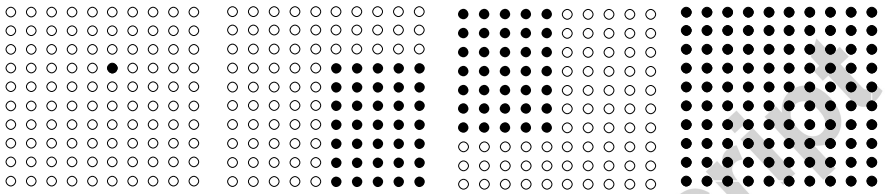
where $i \in [2,\ M+1]$ and $j \in [2, N+1]$ are the indexes of the processed image; k_1'', k_2'' and k_3'' are obtained by reshaping the four sequences k_1', k_2' and k_3' into $M \times N$ matrixes, respectively; C' is an $M \times N$ matrix for storing the confused pixels; C'' is a new $(M+1)\times(N+1)$ matrix to store the encrypted pixels; $\oplus$ is the exclusive OR operation bit-by-bit.

The confusion and diffusion operations are conducted in level. Pixels in the same level would be encrypted in parallel. In each level, Eqs. (14)-(16) are carried out for the confusion purpose, which indicates that each pixel is only scrambling in its original row i.e. pixels in the same level have no interference on each other. Then Eq. (17) is employed in the diffusion of the pixel values, which is only infected by the encrypted pixels in the previous encrypted level and the pseudo-random sequences. Thus, there come to a conclusion that pixels in the same level could be encrypted in parallel. Moreover, the encrypted pixels will make a difference on the confusion stage of the pixels in the next level. The final $M \times N$ cipher image C can be obtained by removing the pre-configured pseudo-random sequences in C''.

For the consideration of improving the security of the proposed parallel image cryptosystem, other encryption rounds are essential. Before a new encryption round, the latest cipher image needs to be rotated. And the rotated image is regarded as a new plain image P in the next encryption round. Then the above encryption operations are performed to obtain a new cipher image C. After four-fold encryption, the final cipher image C could be achieved. It is worth remanding that the rotation angle is different in different rounds in order to achieve better encryption performance. When it reaches to the third round $r = 3$, the image is suggested to be rotated $90(r-1)$ degrees counterclockwise. While in the other three rounds $r = 1, 2, 4$, the rotation angle is $90(r+1)$ degrees. By revising the rotation angle, the described parallel image cryptosystem behaves well in the plaintext sensitivity.

Fig. 4 gives an illustration, where the hollow circles are pixels of plain image and the black solid circles are pixels influenced by the slightly changed pixel. Firstly, we set a little change to any pixel within the plain image (Fig. 4(a)). Then the difference will be spread to its neighbor pixels (the right one and the lower one in the next level) after performing the abovementioned image encryption operations. Similarly, the two influenced pixels will make differences on their right and lower pixels separately by taking the presented image encryption operations. Finally, all pixels, which located on

the bottom right of the slightly changed one, will be different from the encrypted image without any change in plain image, as displayed in Fig. 4(b). It can be seen from Fig. 4(b) that the difference has not been diffused to the whole image. In order to spread the difference to the whole image, the image is rotated by 180 degrees in the first round and the rotated image is shown in Fig. 4(c). It is obvious that all hollow circles are located on right or lower of the solid circles. Therefore, the differences will be spread to the whole image after performing the provided encryption operations, as depicted in Fig. 4(d). The following two rounds of the encryption operations will strengthen the influence. Hence, excellent plaintext sensitivity can be achieved and the capability of plaintext sensitivity is free from the restriction of the coordinates of the changed pixels.



(a) (b) (c) (d)

Fig. 4. The spread of the difference in plain image.

As the provided 5D hyper-chaotic based parallel image cryptosystem is a symmetric cryptosystem, the corresponding decryption algorithm is a converse process of the encryption process. Fig. 5 gives the flow diagram of the decryption process.

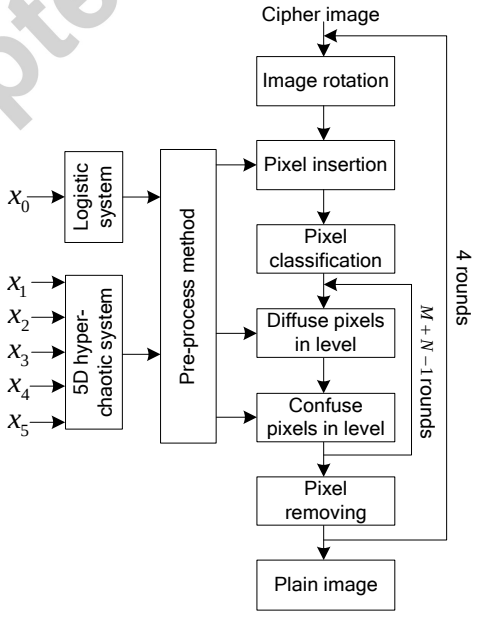


Fig. 5. Flow diagram of the decryption process.

3. Security analyses

Experimental simulations of the presented 5D hyper-chaotic based parallel image cryptosystem are carried out by the MATLAB R2012b on a personal computer with an Intel Core i5, 2GHz CPU and a Windows 7 operation system.

3.1. Keys space

The security of an image cryptosystem depends heavily on its key space size. A large enough key space is essential for resisting the exhaustive attack efficiently. The key space of the 5D hyper-chaotic based parallel image cryptosystem consists two parts: (a) the initial value of the logistic map x_0 that is set to 0.45; (b) the initial values of the 5D hyper-chaotic system $x_1(0)$, $x_2(0)$, $x_3(0)$, $x_4(0)$ and $x_5(0)$, which are set to 0.8, 4.9, 7.6, 3.7 and 6.5 respectively. As the precision is about 10^{-15}, the totally key space of the suggested 5D hyper-chaotic based parallel image cryptosystem is about $10^{90} > 2^{100}$.

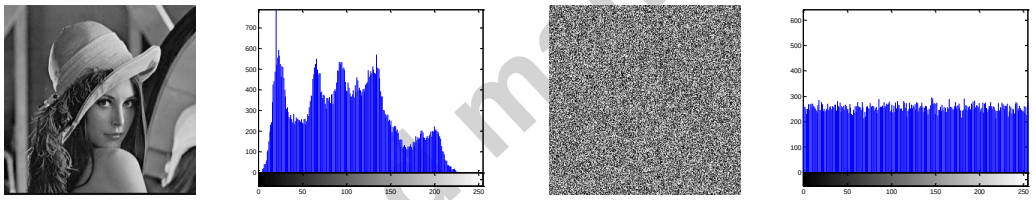
The key spaces of some hyper-chaotic system based image cryptosystem are exhibited in Table 2. It can be seen that the keys space of our cryptosystem is larger than that of Ref. [19] and Ref. [20], which benefits from the good properties (such as more parameters and sufficient key sensitivity) of the pseudo-random sequences generated by the 5D hyper-chaotic system. Hence, the presented parallel image cryptosystem has a good performance in resisting the exhaustive attack.

Table 2 Keys space of different hyper-chaotic based cryptosystems.

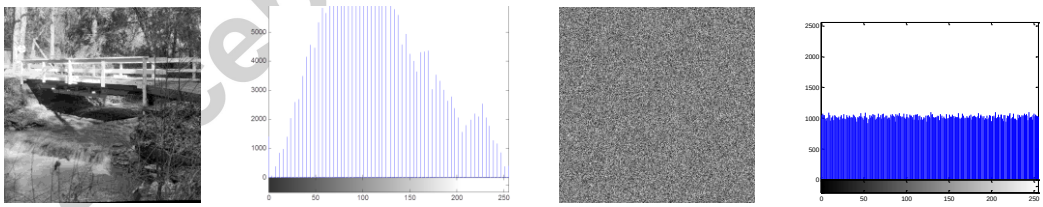
Cryptosystem	Ref. [19]	Ref. [20]	Ref. [31]	Ours
Keys space	2^{296}	2^{112}	10^{112}	10^{90}

3.2. Histogram

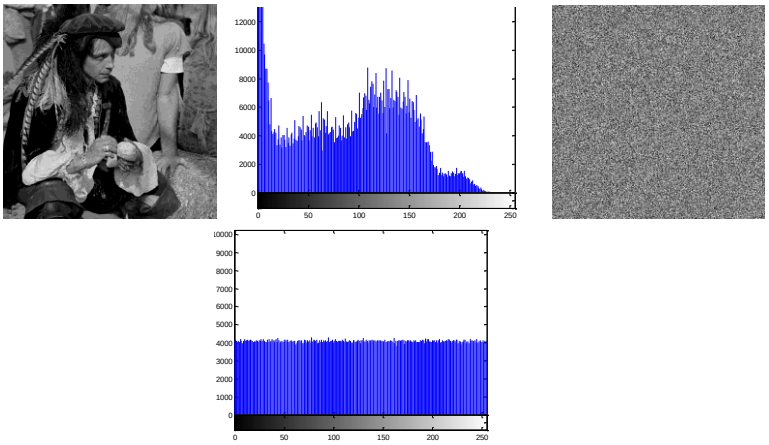
Histograms can graphically exhibit the distribution of pixel values. Usually, the histograms of plain images are unevenly distributed and different plain images show different patterns. For a satisfactorily secure image cryptosystem, the characteristic histograms of the plain images can be altered into even ones. Several plain images and their histograms are shown in Fig. 6(a)-(f), respectively. It indicates that the histograms of the plain images are distributed non-uniformly and different from each other. The corresponding encrypted images and their histograms are depicted in Fig. 6(g)-(l), respectively. It can be observed that the frequency at each gray level is pretty darn close. Thus, the frequency analysis is unworkable for the proposed 5D hyper-chaotic based parallel image cryptosystem.



(a) (d) (g) (j)



(b) (e) (h) (k)



(c) (f) (i) (l)

Fig. 6. The histograms of the plain and encrypted images: (a) “Lena” image, (d) the histogram of (a), (g) the encrypted image of (a), (j) the histogram of (g); (b) “bridge” image, (e) the histogram of (b), (h) the encrypted image of (b), (k) the histogram of (h); (c) “Men” image, (f) the histogram of (c), (i) the encrypted image of (c), (l) the histogram of (i).

3.3. Information entropy

The information quantity of an image can be quantified by its entropy. The randomness of image is positively correlated with its entropy. Hence the entropy is often used as a reference of randomness. The information entropy of a source s is defined as

$$H(s) = -\sum_{i=0}^{2^N-1} p(s_i)\log_2 p(s_i) \tag{14}$$

where 2^N denotes the number of possible symbols s_i. $p(s_i)$ represents the frequency at the symbol s_i. The entropy of an ideally random image is 8 bits. Information entropies of several plain and their cipher images are calculated, and the results are tabulated in Table 3. As can be seen from the results, the information entropies of the cipher images are close to 8 bits. It implies that the presented 5D hyper-chaotic based parallel image cryptosystem has the capability of resistance to entropy attack.

Table 3 Information entropies of images (bit).

Image name	Image size	Plain image	Cipher image

Lena	256×256	7.5534	7.9973
Finger	256×256	7.1075	7.9975
Bridge	512×512	5.7056	7.9993
Dollar	512×512	6.9785	7.9993
Man	1024×1024	7.5237	7.9998
Testpat	1024×1024	4.4077	7.9998

3.4. Correlation coefficient

A sufficiently secure image cryptosystem can get rid of the high correlation between adjacent pixels of plain image. The correlation coefficient is calculated as

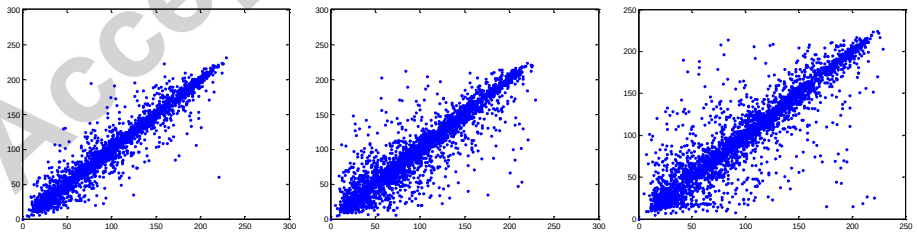
$$r_{xy}=\frac{\left|\operatorname{cov}(x,y)\right|}{\sqrt{D(x)}\sqrt{D(y)}} \tag{15}$$

where $\operatorname{cov}(x,y)=\frac{1}{N}\sum_{i=1}^{N}\prod_{z=x,y}\left(z_i-E(z)\right)$, $E(x)=\frac{1}{N}\sum_{i=1}^{N}x_i$, $D(x)=\frac{1}{N}\sum_{i=1}^{N}\left(x_i-E(x)\right)^2$; x_{i} and y_{i} are gray-scale values of two adjacent pixels within an image.

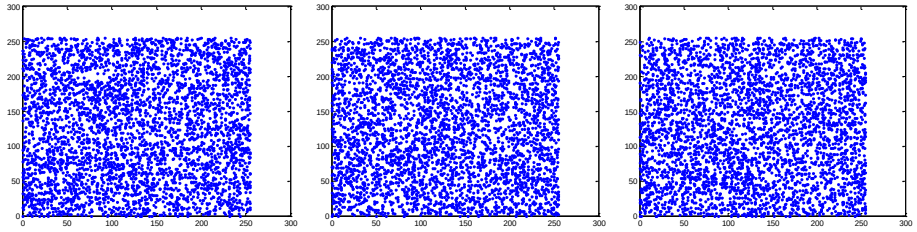
By randomly selecting 10000 pairs of adjacent pixels (horizontally, vertically and diagonally) within an image, the correlation coefficients are calculated to signify the strength of linear relationship. Table 4 reports the correlation coefficients of several plain images and those of their cipher images. Moreover, Fig. 7 depicts the correlations of the adjacent pixels in different directions of "Lena" and the corresponding cipher image, respectively. It is clear from Table 4 and Fig. 7 that the correlation coefficients of the plain images are close to one and the correlation coefficient of the cipher images are near to zero. Therefore, we conclude that adjacent pixels of the plain image are highly correlated while the correlations between adjacent pixels are negligible within the corresponding cipher image. Thus, the described 5D hyper-chaotic based parallel image cryptosystem has achieved an efficient encryption effect.

Table 4 Correlation coefficients of two adjacent pixels in different images.

Name	Size	Plain image			Cipher image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Lena	256×256	0.9705	0.9414	0.9136	−0.0052	0.0031	−0.0003
Finger	256×256	0.6229	0.5653	0.5156	0.0001	0.0018	−0.0070
Bridge	512×512	0.9390	0.9396	0.9100	−0.0004	−0.0050	−0.0055
Dollar	512×512	0.7541	0.8444	0.6726	−0.0034	0.0037	−0.0007
Man	1024×1024	0.9736	0.9797	0.9564	0.0009	−0.0015	−0.0007
Testpat	1024×1024	0.9785	0.9753	0.9605	−0.0028	−0.0016	−0.0001



(a) (b) (c)



(d) (e) (f)

Fig. 7. Correlations of two adjacent pixels of the "Lena" image in (a) horizontal direction, (b) vertical direction, (c) diagonal direction; correlations of two adjacent pixels of the encrypted "Lena" image in (d) horizontal direction, (e) vertical direction, (f) diagonal direction.

3.5. Plaintext sensitivity

Differential attack is a common way of the existing image cryptosystem attacks. The image cryptosystems are expected to be sensitive to the tiny variation of plain images with respect to the differential attack. NPCR (Number of Pixel Changing Rate) and UACI (Unified Average Changing Intensity) [29] are two of the most common parameters to estimate the disparity between two images. And the definitions of the two parameters are defined as

$$D(i,j)=\begin{cases}1 & \text{if } C_1(i,j)=C_2(i,j)\\ 0 & \text{otherwise}\end{cases} \tag{16}$$

$$\text{NPCR}=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100\% \tag{17}$$

$$\text{UACI}=\frac{1}{M\times N}\left(\sum_{i=1}^{M}\sum_{j=1}^{N}\frac{\left|C_1(i,j)-C_2(i,j)\right|}{255}\right)\times 100\% \tag{18}$$

where C_1 and C_2 are two images.

The following steps are taken to test the influence of one changed pixel on the whole cipher image. Firstly, the value of an arbitrary pixel is changed within the plain image. Then, the plain and modified images are encrypted by the 5D hyper-chaotic based parallel image cryptosystem with the same keys. Then two cipher images are obtained. Finally, the scores of NPCR and UACI are calculated to quantitatively describe the differences between the two cipher images. Several plain images are selected as the text images and each image is examined 100 times in the same circumstance. The experimental results are summarized in Table 5. It shows that

every value fluctuates nearby the expected values 99.6094% and 33.4636% [30], respectively. Moreover, the average NPCR and UACI of "Lena" for different algorithms are calculated and reported in Table 7. It indicates that our algorithm has a better performance than the other algorithms. Table 6 depicts the performances of some given points within "Lena". From the results, we found that the degree of plaintext sensitivity of the provided 5D hyper-chaotic based parallel image cryptosystem is close for different indexes, which means that the plaintext sensitivity is irrelevant to the position of the changed pixel. Thus, the capability of plaintext sensitivity is free from the restriction of the coordinates of the changed pixels. All of the results verify that any swiftly change in the plain image can lead to a significantly different cipher image even other conditions stay the same. Therefore, the designed image cryptosystem has reached an excellent sensitivity to the plaintext, which plays an important role in the resistance to differential attack.

Table 5 NPCR and UACI scores between two cipher images.

Name	Size	NPCR (%)			UACI (%)		
		Max	Min	Average	Max	Min	Average
Lena	256×256	99.66	99.57	99.6122	33.65	33.24	33.4573
Finger	256×256	99.68	99.55	99.6118	33.68	33.19	33.4557
Bridge	512×512	99.64	99.57	99.6102	33.60	33.34	33.4691
Dollar	512×512	99.65	99.59	99.6108	33.61	33.35	33.4653
Man	1024×1024	99.62	99.59	99.6092	33.51	33.40	33.4682
Testpat	1024×1024	99.62	99.59	99.6084	33.53	33.41	33.4622

Table 6 Fixed points test for plaintext sensitivity.

Index	[1,1]	[1,256]	[84,42]	[101,69]	[198,133]	[256,1]	[256,256]
NPCR (%)	99.6048	99.6140	99.6262	99.6216	99.5956	99.6170	99.6444
UACI (%)	33.5938	33.52	33.5040	33.4350	33.5180	33.4564	33.4907

Table 7 Performance of different algorithms.

Algorithm	NPCR (%)	UACI (%)
Ours	99.6122	33.4573
Ref. [19]	51.9018	1.05922
Ref. [31]	99.59106	33.4949

3.6. Key sensitivity

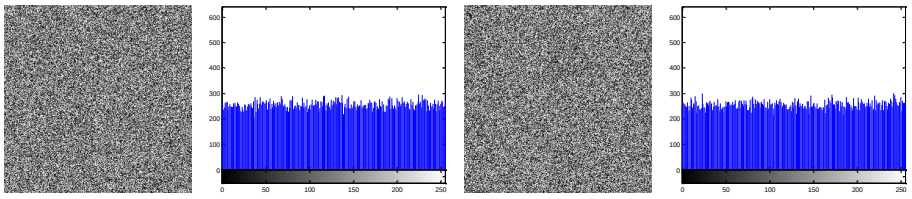
Image cryptosystems are suggested to be sensitive to the keys. In order to test key sensitivity, two experiments are conducted:

(1) Sensitivity tests for encryption keys. Firstly, set a minor change 10^{-14} to $x_1(0)$ and leave the other four keys unchanged. Secondly, encrypt “Lena” by the changed keys and the correct keys, respectively. Finally, compare the differences between the two cipher images. Fig. 8 shows the corresponding encrypted images and their histograms. It is hard to visually distinguish the difference between the two cipher images. By comparing their histograms, we found that their pixel distributions are different which means that they are two different

images. The NPCR values between the cipher images are calculated to quantitatively compare their differences and Table 8 displays the results. It can be seen that 99.66% pixels are found to be different. Furthermore, when other keys exist in the same situation, almost 99.60% pixels between the correctly encrypted image and incorrectly encrypted image are different. As observed from these results, minor change of the encryption keys can cause great changes of cipher images. Therefore, the described image cryptosystem is confirmed to be sensitive to the encryption keys.

Table 8 NPCR scores between the image encrypted by the correct keys and the image encrypted by the changed keys.

Encryption keys						NPCR (%)
x_0	$x_1(0)$	$x_2(0)$	$x_3(0)$	$x_4(0)$	$x_5(0)$	
0.45	$0.8+10^{-14}$	4.9	7.6	3.7	6.5	99.66
0.45	0.8	$4.9+10^{-14}$	7.6	3.7	6.5	99.59
0.45	0.8	4.9	$7.6+10^{-14}$	3.7	6.5	99.61
0.45	0.8	4.9	7.6	$3.7+10^{-14}$	6.5	99.59
0.45	0.8	4.9	7.6	3.7	$6.5+10^{-14}$	99.60
$0.45+10^{-14}$	0.8	4.9	7.6	3.7	6.5	99.63



(a) (b) (c) (d)

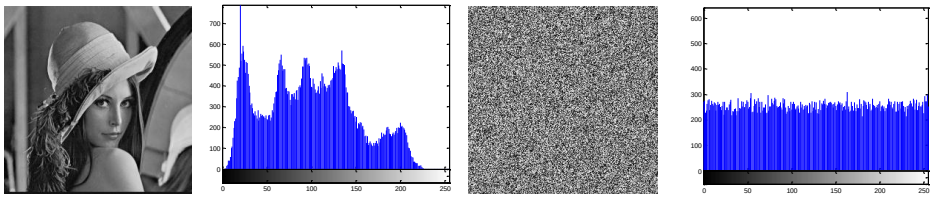
Fig. 8. Encryption key sensitivity test: (a) the image encrypted by the correct keys, (b) the histogram of (a), (c) the image encrypted by $x_1(0)+10^{-14}$, (d) the histogram of (c).

(2) Sensitivity tests for decryption keys. A satisfactory image cryptosystem is suggested to be sensitive to the mutation of the decryption keys. Experiments as above described are performed to explore the decryption key sensitivity of the 5D hyper-chaotic based parallel image cryptosystem. Fig. 9(a) and (c) show the correctly and incorrectly decrypted images, respectively. Fig. 9(b) and (d) are their histograms, respectively. It illustrates that the incorrectly decrypted image is still noise-like and its histogram is uniform, which are apparently different from that of the correctly decrypted image. Similar results could be observed when the same change happens in other keys. Moreover, NPCR between the decrypted image and the plain image are computed for the purpose of analyzing their differences. The corresponding results presented in Table 9 shows that NPCR between the plain image and the correctly decrypted image is zero, in other words, the image can be thoroughly decrypted only if the decrypted keys are precisely correct. And over 99.60% pixels between the plain image and the incorrectly decrypted images are different. It draws a conclusion that the proposed parallel image cryptosystem possesses high key sensitivity. Hence, it has the capability of resisting exhaustive attack.

Table 9 NPCR scores between the decrypted image and the plain image.

Decryption keys						NPCR
x_0	$x_1(0)$	$x_2(0)$	$x_3(0)$	$x_4(0)$	$x_5(0)$	(%)
0.45	0.8	4.9	7.6	3.7	6.5	0
$0.45+10^{-14}$	0.8	4.9	7.6	3.7	6.5	99.63
0.45	$0.8+10^{-14}$	4.9	7.6	3.7	6.5	99.61
0.45	0.8	$4.9+10^{-14}$	7.6	3.7	6.5	99.63
0.45	0.8	4.9	$7.6+10^{-14}$	3.7	6.5	99.64

0.45	0.8	4.9	7.6	$3.7+10^{-14}$	6.5	99.63
0.45	0.8	4.9	7.6	3.7	$6.5+10^{-14}$	99.65



(a) (b) (c) (d)

Fig. 9. Decryption key sensitivity test: (a) the correctly decrypted image, (b) the histogram of (a), (c) the image decrypted by $x_1(0)+10^{-14}$, (d) the histogram of (c).

3.7. Encryption speed

Given that the encryption speed is also a significant consideration for an excellent image cryptosystem, we have performed the encryption operations of several image cryptosystems in one personal computer and the encryption time of these image cryptosystems are listed in Table 10. The encryption time of two 1024×1024 images for Ref. [31] is not observed. In Ref. [31], the initial values of hyper-chaotic system are related to the size of plain image. Hence the initial value may beyond the scope when the plain image is too large. As can be seen from Table 10 that the encryption speed of our image cryptosystem is relatively faster than that of the other two hyper-chaotic based image cryptosystems.

Table 10 Encryption speed analyses.

Name	Size	Encryption time (seconds)		
		Ref. [19]	Ref. [31]	Ours
Lena	256×256	3.325199	3.995265	1.217300
Finger	256×256	3.350715	4.033281	1.225779

Bridge	512×512	12.077586	23.59560	4.901081
Dollar	512×512	12.082043	23.378967	4.893116
Man	1024×1024	47.302717	\	19.956056
Testpat	1024×1024	47.564316	\	19.891103

4. Conclusions and discussions

In this paper, we proposed a new parallel image cryptosystem with a 5D hyper-chaotic system. The 5D hyper-chaotic system is employed in the generation of hyper-chaotic sequences. Then, the described preprocessing method is applied to enhance the features of the hyper-chaotic sequences. As described in section 2.1, the generated pseudo-random sequences are proved to mainly have two advantages. Firstly, compared with other hyper-chaotic systems, the 5D hyper-chaotic system has more complex dynamic behaviors. Secondly, the generated pseudo-random sequences obtain better properties (distribution, randomness, auto-correlation and cross-correlation) than the original hyper-chaotic sequences. Hence we can come to a conclusion that the generated pseudo-random sequences can meet the demand for high security in cryptosystem better.

After preprocessing the hyper-chaotic sequences, the encryption procedures are taken in a parallel way. Experimental results have shown that our parallel image cryptosystem has some remarkable performances:

(1) High plaintext sensitivity. The encryption process is influenced by its neighbor pixels, namely the upper one and the left one, which strengthen the relationships between ciphertext and plaintext. Moreover, the rotation operations enhance the influence of the changed pixels. In result, the cipher image is sensitive to the change of any pixel within the plain image.

(2) Sufficient encryption speed. For our image cryptosystem, the plain image is divided into levels. Pixels within the same level are encrypted simultaneously to improve the encryption efficiency. As listed in Table 10, the encryption speed of our cryptosystem is relatively sufficient.

(3) High key sensitivity. Thanks to the initial values sensitivity of 5D hyper-chaotic system, the finally generated chaotic sequences will be totally different when a minor change is set into the initial value. Then a totally different cipher image is obtained after using the changed sequences.

(4) Large key space. Benefit from the large amount of parameters and high key sensitivity, the proposed image cryptosystem has an excellent performance in resisting brute-force attack.

Furthermore, our image cryptosystem has other characteristics, such as uniform pixel distribution and weak correlation between adjacent pixels. In conclusion, the presented parallel image cryptosystem can resist existing attacks and accelerate operating speed.

Acknowledgements This work is supported by the National Natural Science Foundation of China (grant nos. 61462061 and 61262084), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star) (grant no. 20122BCB23002), the Natural Science Foundation of Jiangxi Province, China (grant no. 20151BAB207002) and the Innovation Fund for graduates of Nanchang University (grant no. cx2015139).

References

1. Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos 1998; 8(06): 1259-1284.

2. Zhang LY, Hu XB, Liu YS, et al. A chaotic image encryption scheme owning temp-value feedback [J]. Communications in Nonlinear Science and Numerical Simulation 2014; 19(10): 3653-3659.

3. Zhang XP, Mao YB, Zhao ZM. An efficient chaotic image encryption based on alternate circular S-boxes [J]. Nonlinear Dynamics 2014; 78(1): 359-369.

4. Nanrun Zhou, Aidi Zhang, Fen Zheng, Lihua Gong. Image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing [J]. Optics and Laser Technology 2014; 62: 152-160.

5. Liu Ye, Wang Jun, Fan JingHui, Gong LiHua. Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences [J]. Multimedia Tools and Applications 2015; 1-20.

6. Nanrun Zhou, Haolin Li, Di Wang, Shumin Pan, Zhihong Zhou. Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform [J]. Optics Communications 2015; 343, 10-21.

7. Zhang YS, Xiao D. An image encryption scheme based on rotation matrix bit-level permutation and block diffusion [J]. Communications in Nonlinear Science and Numerical Simulation 2014; 19(1): 74-82.

8. Zhu HG, Zhao C, Zhang XD. A novel image encryption–compression scheme using hyper-chaos and Chinese remainder theorem. Signal Processing: Image Communication 2013; 28(6): 670-680.

9. Hermassi H, Rhouma R, Belghith S. Improvement of an image encryption algorithm based on hyper-chaos. Telecommunication Systems 2013; 52(2): 539-549.

10. Ye GD, Wong KW. An image encryption scheme based on time-delay and hyper-chaotic system. Nonlinear Dynamics 2013; 71(1-2): 259-267.

11. Norouzi B, Mirzakuchaki S. A fast color image encryption algorithm based on hyper-chaotic systems. Nonlinear Dynamics 2014; 78(2): 995-1015.

12. Gao TG, Chen ZQ. A new image encryption algorithm based on hyper-chaos [J]. Physics Letters A 2008; 372(4): 394-400.

13. Rhouma R, Belghith S. Cryptanalysis of a new image encryption algorithm based on hyper-chaos [J]. Physics Letters A 2008; 372(38): 5973-5978.

14. Jeng FG, Huang WL, Chen TH. Cryptanalysis and improvement of two hyper-chaos-based image encryption schemes [J]. Signal Processing: Image Communication 2015; 34: 45-51.

15. Wang XY, Liu LT, Zhang YQ. A novel chaotic block image encryption algorithm based on dynamic random growth technique [J]. Optics and Lasers in Engineering 2015; 66: 10-18.

16. Zhou G, Zhang D, Liu Y, et al. A novel image encryption algorithm based on chaos and Line map [J]. Neurocomputing 2015; 169: 150-157.

17. Huang XL, Ye GD. An efficient self-adaptive model for chaotic image encryption algorithm [J]. Communications in Nonlinear Science and Numerical Simulation 2014; 19(12): 4094-4104.

18. Chen JX, Zhu ZL, Fu C, et al. A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism [J]. Communications in Nonlinear Science and Numerical Simulation 2015; 20(3): 846-860.

19. Mirzaei Omid, Yaghoobi Mahdi, Irani Hassan. A new image encryption method: parallel sub-image encryption with hyper chaos [J]. Nonlinear Dynamics 2012; 67(1): 557-566.

20. Zhou Q, Wong K, Liao XF, Xiang T, Hu Y. Parallel image encryption algorithm based on discretized chaotic map [J]. Chaos, Solitons & Fractals 2008; 38(4): 1081-1092.

21. Dang H G. Parameter Identification of a New Hyper-chaotic System[C]. 2013 Fifth International Conference on Measuring Technology and Mechatronics Automation. IEEE 2013; 785-787.

22. Fan B, Tang LR. A new five-dimensional hyper-chaotic system and its application in DS-CDMA [C]//Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference on. IEEE 2012; 2069-2073.

23. Rossler O E. An equation for hyperchaos [J]. Physics Letters A 1979; 71(2): 155-157.

24. Lü JH, Chen GR. A new chaotic attractor coined [J]. International Journal of Bifurcation and chaos 2002; 12(03): 659-661.

25. Jia Q. Hyperchaos generated from the Lorenz chaotic system and its control [J]. Physics Letters A 2007; 366(3): 217-222.

26. Wang Fa-Qiang, Liu Chong-Xin. Hyperchaos evolved from the Liu chaotic system [J]. Chinese Physics 2006; 15(5): 963.

27. Vaidyanathan S, Volos C, Pham V T. Hyperchaos, adaptive control and synchronization of a novel 5-D hyperchaotic system with three positive Lyapunov exponents and its SPICE implementation [J]. Archives of Control Sciences 2014; 24(4): 409-446.

28. Cao YY, Fu C. An image encryption scheme based on high dimension chaos system[C]//Intelligent Computation Technology and Automation (ICICTA), 2008 International Conference on. IEEE 2008; 2: 104-108.

29. Mao YB, Chen GR, Lian SG. A novel fast image encryption scheme based on 3D chaotic baker maps [J]. International Journal of Bifurcation and Chaos 2004; 14(10): 3613-3624.

30. Zhao JF, Wang SY, Chang YX, Li XY. A novel image encryption scheme based on an improper fractional-order chaotic system [J]. Nonlinear Dynamics 2015; 80(4): 1721-1729.

31. Huang XL, Ye GD. An image encryption algorithm based on hyper-chaos and DNA sequence [J]. Multimedia Tools and Applications 2014; 72(1): 57-70.

Highlights

- A parallel image cryptosystem is proposed.
- The 5D hyper-chaotic system and Logistic map are combined in the generation of chaotic sequences with better properties.
- Plain image is divided into levels, and pixels within the same level can be encrypted in parallel.
- Each pixel is directly influenced by its neighbor pixels, namely the upper one and the left one, which makes the cipher-text to be more sensitive to the plaintext.