International Journal of Pure and Applied Mathematics
Volume 80 No. 4 2012, 609-616
ISSN: 1311-8080 (printed version)
url: http://www.ijpam.eu

ijpam.eu

A NEW DIGITAL IMAGE ENCRYPTION ALGORITHM BASED ON 4D CHAOTIC SYSTEM

Xiaoling Huang

College of Science
Guangdong Ocean University
Zhanjiang, 524088, Guangdong, P.R. CHINA

Abstract: To overcome low security in the low-dimensional chaotic system, a new 4D chaotic system based image encryption is presented in this paper. Only the diffusion function is considered in the proposed algorithm. Besides of the parameters in 4D chaotic system, we also add three control parameters to enlarge the key space. Here, the designed control parameters are dependent on the plain-image. With three rounds of iteration, the experimental results show that the new algorithm can have fast performance, good efficiency and high security. It is suitable for us to make real-time communication and transformation over the internet.

AMS Subject Classification: 40C05, 68U10, 68P25, 94A60
Key Words: image encryption, 4D chaotic system, diffusion, security analysis, modular function

1. Introduction

With the fast development of computer technology and widely application of internet, we can enjoy the digital information with others more directly and conveniently. But, the security problem has being paid to our attention at the same time. Illegal person may attack the secret information by copy, revision and so on. So, it is important for us to search the encryption algorithm to protecting these information.

Received: September 19, 2012

© 2012 Academic Publications, Ltd.
url: www.acadpubl.eu

Recently, there are many encryption algorithms and schemes for the digital image information. For example, AES, DES, chaos and Arnold based method. However, among them, the chaos based image encryption algorithm has great interesting for the researchers. The reason is that the desirable cryptographic properties in chaotic system [1] such as control parameters, sensitivity to initial conditions, and random-like behavior. In [2], J. Fridrich adapted two-dimensional chaotic maps to create new symmetric block encryption schemes. D. Xiao [3] pointed out the cause of potential flaws in [4] with detail analysis, and then proposed the corresponding enhancement measures. To enlarge key space and enhance high security, T.G. Gao [5] used a hyper-chaotic system to confuse the relationship between the plain-image and the cipher-image. Some other methods of encryption for image are also presented [6, 7].

However, most of the image encryption adopted the classical structure of permutation plus diffusion, for example [5, 8], as a result, more time cost should be taken. In this paper, we suggest a new image encryption algorithm only considering the diffusion operation. The block way is processed with a 4D chaotic system. The rest of this paper is organized as follows. In Section 2, we mainly describe the proposed image encryption algorithm with the introduction of 4D chaotic system. Decryption process is also explained in this part. Then, some experimental results are given in Section 3 to show the efficiency. Security analyses are evaluated in Section 4. Finally, We make a summary for the whole paper in Section 5.

2. Proposed Image Encryption Algorithm

2.1. 4D Chaotic System

Compared with one-dimensional chaotic map, for example, logistic mp and skew tent map, 4D chaotic system defined as (1) has more control parameters and initial conditions. It can enlarge the key space when it is combined in the image encryption algorithm.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = -xz + dx + cy - w \\ \dot{z} = xy - bz \\ \dot{w} = x + k \end{cases} \tag{1}$$

where, when $a = 36, b = 3, c = 28, d = -16$, and $k \in [-0.7, 0.7]$, the system can be in chaos phenomena seeing Figure 1. More details can be seen and studied

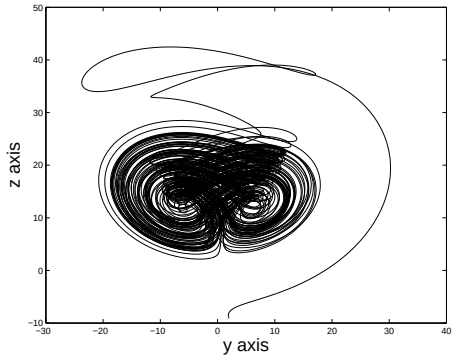


Figure 1: Chaotic behavior.

in [5] with some properties.

2.2. Image Encryption and Decryption Process

In first place, Suppose that the plain-image A with size $m \times n$ is divided into two parts A_1 and A_2 equally in vertically. Then, each sub-part is in size $m/2 \times n$. With randomly chosen initial conditions x_0, y_0, z_0 and w_0, we can get a chaotic sequence $S = \{x_0, y_0, z_0, w_0, x_1, y_1, z_1, w_1, \cdots\}$ if the system (1) is iterated after many rounds.

To make the keystream dependent on the plain-image, we compute the sum s of all elements in the second sub-part A_2 as following equation (2). In this case, the number s is a bigger integer. However, to reduce the computation, we do the process for s with number m and n, and get three control parameters r_1, r_2 and r_3 as equations (3).

$$s = \Sigma_{i,j} A_2(i,j), i = 1, 2, \cdots, m/2.\ j = 1, 2, \cdots, n. \tag{2}$$

$$\begin{cases} r_1 = mod(s, m/2) + 1 \\ r_2 = mod(s, n) + 1 \\ r_3 = mod(s, m/2 + n) + 1 \end{cases} \tag{3}$$

here, *mod* means the modular function after division.

For avoiding harmful effect in former iteration values from system (1), a new chaotic sequence $\overline{S} = \{x_r, y_r, z_r, w_r, x_{r+1}, y_{r+1}, z_{r+1}, w_{r+1}, \cdots\}$ of size $1 \times mn/2$ is selected from S with control parameter $r = r_1 + r_2$. Then, we arrange $\overline{S}$ into a matrix P of size $m/2 \times n$ from top to bottom and from left to right. But, here, the elements of P are still in format of decimal fraction, they can not used

directly for the plain-image matrix A. So, we should do processing for them and transfer they into integer numbers. Here, we design the following function (4) for P.

$$P(i,j) = mod(floor(P(i,j) \times 10^{14}), 256) \tag{4}$$

here, $i = 1, 2, \cdots, m/2$, $j = 1, 2, \cdots, n$. $floor(x)$ rounds x to the nearest integer towards minus infinity.

After the keystream P being generated, the encryption process can be carried out for the sub-parts A_1 and A_2 as equations (5).

$$\begin{cases} \overline{A}_1 = A_1 + r_3 P \\ \overline{A}_2 = A_2 + \overline{A}_1 \end{cases} \tag{5}$$

here, symbol + denotes the modular operation.

Of course, the decryption process is similarly to the encryption process but in reverse order, it can also be easily got from (5) seeing (6).

$$\begin{cases} A_2 = \overline{A}_2 - \overline{A}_1 \\ A_1 = \overline{A}_1 - r_3 P \end{cases} \tag{6}$$

here, symbol − denotes the modular operation.

2.3. The Steps of the Proposed Algorithm

Based the encryption process analysis above, the steps of the proposed image encryption algorithm are listed as follows. For achieving higher security from step 3 to step 6 should be repeated more than one rounds. Here, we take three rounds in our algorithm.

Step 1 Read the plain-image and express it with matrix A of size $m \times n$.

Step 2 Generate chaotic sequence S with initial conditions x_0, y_0, z_0, w_0 iterated in 4D system (1).

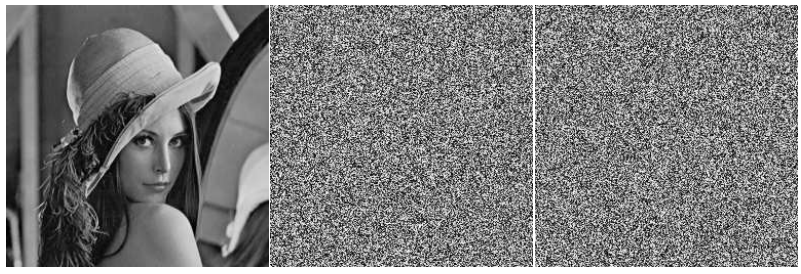
Step 3 Calculate the control parameters r_1, r_2 and r_3 from the sum of A_2 by equation (3).

Step 4 Get random matrix P in size $m/2 \times n$ from $\overline{S}$ by control parameters r_1 and r_2.

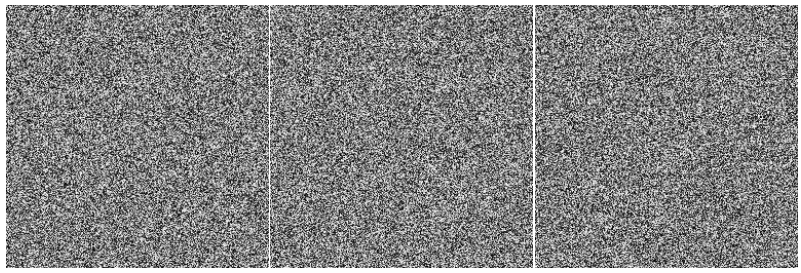
Step 5 Do modular function for matrixes A_1 and P together with r_3, and get new sub-part $\overline{A}_1$.

Step 6 Do modular function again for matrixes $\overline{A}_1$ and A_2 to obtain another new sub-part $\overline{A}_2$.

Step 7 Cipher-image is formed with $\overline{A} = [\overline{A}_1; \overline{A}_2]$.



(a) (b) (c)



(d) (e) (f)

Figure 2: (a) plain-image, (b) cipher-image, (c) wrong cipher-image with 10^{-14} shift in x_0, (d) wrong cipher-image with 10^{-14} shift in y_0, (e) wrong cipher-image with 10^{-14} shift in z_0, (f) wrong cipher-image with 10^{-14} shift in w_0.

3. Experimental Results

In this section, Some experimental tests are done for the proposed algorithm. We use the software Matlab 7.0 on platform Windows 7. Lena image in size 256×256 is randomly chosen in simulations. Figure 2(a) shows the plain-image while the cipher-image is obtained in figure 2(b) with initial conditions $x_0 = 13.73$, $y_0 = -4.66$, $z_0 = 2.72$ and $w_0 = -10.01$. Only 0.0390 seconds are taken for the whole encryption algorithm which shows a fast way.

4. Security Analyses

(1) Key space used analysis. In the proposed algorithm, the 4D chaotic system is adopted with four system parameters and four secret keys, i.e., x_0, y_0, z_0 and w_0. As we know that the high-dimensional chaotic system can efficiently the brute-force attack. So, the key space is big enough because it can reach 10^{56} if

Lena image	(1,1)	(20,203)	(234,61)	(256,256)
UACI	0.3363	0.3342	0.3353	0.3353
NPCR	0.9964	0.9961	0.9958	0.9958

Table 1: UACI and NPCR test for different positions

the precise is set to be 10^{-14}.

(2) Sensitivity analysis. A good encryption algorithm should be sensitive to every initial conditions. In our test, figures 2(c), (d), (e) and (f) are wrong decryption image just with 10^{-14} difference in keys x_0, y_0, z_0 and w_0 respectively. Further, UACI and NPCR [9] are usually taken to measure the chosen-plaintext and known-plaintext attacks. The calculation equations are following (7) and (8). Table 1 lists the results for different positions just one-bit shift in gray values in Lena image of size 256×256. Therefore, it is obvious that the algorithm is very sensitive to initial conditions and plain-image.

$$NPCR = \frac{\sum_{ij} D(i,j)}{M \times N} \times 100\% \tag{7}$$

$$UACI = \frac{1}{M \times N}[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}] \times 100\% \tag{8}$$

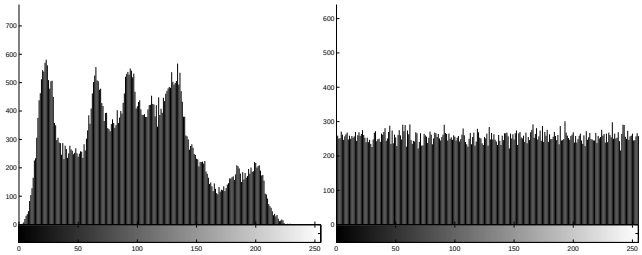
where $D(i,j) = 0$ if $C_1(i,j) = C_2(i,j)$; otherwise, $D(i,j) = 1$.

(3) Histogram analysis. Histogram shows gray distribution of an image, it is easily attacked by statical analysis. If the gray distribution of cipher-image is great different from that of plain-image, then, it can let histogram analysis be infeasible. By applying the proposed algorithm, figure 3(b) shows the histogram of cipher-image compared with that of plain-image in figure 3(a). Thus the algorithm can resist the histogram analysis.

(4) Correlation coefficient analysis. There are strong correlation coefficients [10] between two adjacent pixels in plain-image. An ideal should have the ability to deduce them to near zeros. By calculating the following equation (9), we get the results in table 2. So, we can see that the values are near to zeros in cipher-image using the proposed algorithm.

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \tag{9}$$

where $cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))$, $D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2$,



(a) (b)

Figure 3: Histogram: (a) plain-image, (b) cipher-image.

Model	Plain-image	Cipher-image
Horizontally	0.9514	-0.0092
Diagonally	0.9833	0.0733
Vertically	0.9457	-0.0376

Table 2: Correlation coefficients

$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$. where x_i and y_i represent the gray values of two adjacent pixels.

5. Summary

In this paper, a new image encryption algorithm based on a 4D chaotic system is suggested. It is designed in an efficient and fast block way. We only use the diffusion function, i.e., one of the traditional methods. Control parameters are dependent on the plain-image, of which can resist the chosen-plaintext and known-plaintext attacks. Furthermore, the algorithm is processed in blocks that can save us greatly much more time. The security analyses are evaluated such as key space, sensitivity, histogram and correlation, all results illustrate that the proposed algorithm is a suitable scheme to be applied in digital image encryption.

Acknowledgments

This work is part of the research project funded by the Science & Technology Program Foundation of Zhanjiang City of P.R. China (No. 2011C3109002).

References

[1] M. Amin, O.S. Faragallah, A.A. Abd El-Latif, A chaotic block cipher algorithm for image cryptosystems, *Commun. Nonlinear Sci.*, **15** (2010), 3484-3497.

[2] J. Fridrich, Symmetric cihpers based on two-dimensional chaotic maps, *Int. J. Bifurcat. Chaos*, **8** (1998), 1259-1284.

[3] D. Xiao, X.F. Liao, P.C. Wei, Analysis and improvement of a chaos-based image encryption algorithm, *Chaos Soliton. Fract.*, **40** (2009), 2191-2199.

[4] Z.H. Guan, F.J. Huang, W.J. Guan, Chaos based image encryption algorithm, *Phys. Lett. A*, **346** (2005), 153-157.

[5] T.G. Gao, Z.Q. Chen, A new image encryption algorithm based on hyperchaos, *Phys. Lett. A*, **373** (2008), 394-400.

[6] O.S. Faragallah, An enhanced chaotic key-based RC5 block cipher adapted to image encryption, *Int. J. Electron.*, **99** (2012), 925-943.

[7] I.S. Sam, P. Devaraj, R.S. Bhuvaneswaran, A novel image cipher based on mixed transformed logistic maps, *Multimed. Tools Appl.*, **56** (2012), 315-330.

[8] V. Patidar, N.K. Pareek, G. Purohit, K.K. Sud, Modified substitution-diffusion image cipher using chaotic standard and logistic maps, *Commun. Nonlinear Sci.*, **15** (2010), 2755-2765.

[9] F.Y. Sun, Z.W. L*ü*, S.T. Liu, A new cryptosystem based on spatial chaotic system, *Opt. Commun.*, **283** (2010), 2066-2073.

[10] Z. Wang, X. Huang, N. Li, X.N. Song, Image encryption based on a delayed fractional-order chaotic logistic system, *Chinese Phys. B*, **21** (2012), Article ID 050506.