A Color Image Encryption Scheme Based on Generalized Synchronization Theorem

Shuang-Shuang Han*[1, 3], Le-Quan Min[1, 2]
[1]Schools of Automation and Electrical Engineering, University of Science and Technology Beijing, China
[2]Schools of Mathematics and Physics, University of Science and Technology Beijing, China
[3]Beijing Command College of Chinese People's Armed Police Force, China
*Corresponding author, e-mail: shuangert1@126.com

Abstract

In order to enhance the security of image information, base on generalized synchronization theorem (GCS) for discrete chaotic system, this paper introduces a new 6-dimensional generalized chaos synchronization system based on 3D-Lorenz map. Numerical simulation showed that two pair variables of the synchronization system achieve generalized synchronization via a transform H. Combining with the 2-Dimension non equilateral Arnold transformation; a color image encryption scheme was designed. Analyzing the key sensitivity, key space, histogram, information entropy and correlation of adjacent pixels, it showed that the scheme have sound encryption and decryption effects. Numerical simulations reveal that the scheme is effective in commercial network communication for its strong anti-interference ability.

***Keywords**: generalized synchronization, color image encryption, non equilateral Arnold transformation, discrete chaotic system*

Copyright © 2014 Institute of Advanced Engineering and Science. All rights reserved.

1. Introduction

With the development of computer and network technology, image information becomes an important mean of information exchanges, and its security problem is outstanding increasingly. However, the algorithm for the text encryption is not suitable for image encryption, so there are some novel algorithms for the color image to be presented, such as single-channel channel algorithms [1] [2], algorithms based on nonlinear fractional Mellin transform [3], algorithm based on the wavelength multiplexing [4] and so on.

As a nonlinear dynamics phenomenon, chaos has many properties to be worthwhile use, such as pseudo-random characteristics, the extreme sensitivity of the initial state and so on [5] [6]. Since the earlier work of Pecora and Carroll [7], chaos synchronization (CS) based on cryptography communication research has attracted much attention [8]-[9]. Generalized chaotic synchronization (GCS) is one of the focal research topics in CS. It provides a new tool for constructing secure communication systems [10] [11], which can solve the security problem of the lower dimensional chaotic systems used in image encryption [12].

Based on the generalized synchronization for discrete chaotic systems [10] and 3-D Lorenz map, a GCS is constructed by a new invertible transformation. Combining with 2-Dimension non equilateral Arnold transformation, a color image encryption scheme is introduced. Numerical simulation and the security analysis reveal that the scheme can encrypt and decrypt color image accurately without any lost.

2. Algorithm

To design the new generalized chaos synchronization system, some basic concepts are introduced.

Definition 1: Consider two discrete systems

$$X(k+1)=F(X(k)) \quad (1)$$

$$Y(k+1)=G(Y(k),X_m(k)) \quad (2)$$

Received May 15, 2013; Revised July 8, 2013; Accepted August 15, 2013

where $X(k)=(x_1(k),...,x_n(k))^T \in R^n$, $Y(k)=(y_1(k),...,y_m(k))^T \in R^m$, .
$F_m(X(k))=(f_1(X(k)),...,f_m(X(k)))^T$, $G(Y(k),X(k))=(g_1(Y(k),X(k)),..,g_m(Y(k),X(k)))^T$.

If there exists a transformation $H: R^n \to R^m$ and a subset $B = B_X \times B_Y \subset R^n \times R^m$ such that all trajectories of (1), (2) with intial conditions $(X(0),Y(0)) \in B$ satisfies $\lim_{k\to+\infty} \| H(X(k)) - Y(k) \| = 0$, then the systems in (1) and (2) are said to be in GS with respect to the transformation H.

Theorem 1[10]**:** If two discret sysems (1) and (2) are in GS with respect to the transformation H given by Definition 1. Then the $G(Y(k),X(k))$ in (2) has form

$$G(Y,X) = H(F(X) - Q(Y,X)) \tag{3}$$

where $F(X)=(f_1(X),f_2(X),...,f_m(X))^T$ and $Q(X,Y)=(Q_1(X,Y),Q_2(X,Y),...,Q_m(X,Y))^T$ makes the zero solution of the error equation

$$e(k+1) = H(X(k+1)) - Y(k+1)) = Q(X,Y) \tag{4}$$

be asymptotically stable.

Definition 2: The 2-Dimension non equilateral Arnold transformation is defined as [13]:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \text{mod} \begin{pmatrix} M \\ N \end{pmatrix} \tag{5}$$

Where the adjoint matrix satisfies $a=1$, $c=rq$, $d=1+bc$, $q=N/\gcd(M,N)$. Besides, b and r are positive integers. The phase space of the transformation is $M \times N$.

Its inverse transformation can be defined as

$$\begin{cases} y_n = (y_{n+1} - cx_{n+1}) \text{mod} N \\ x_n = (x_{n+1} - by_{n+1}) \text{mod} M \end{cases} \tag{6}$$

3. Research Method

In this section, a novel discrete chaotic system could be constructed using the Theorem 1, and then a new color image scheme is designed based on the GCS and generalized cat map. The last procedure is to verify the anti-attack ablility of the scheme . All the simulations are implemented using Matlab 7.0.

3.1. A New GCS

Suppose 3-D Lorenz map has the form[14]:

$$\begin{cases} x_1(k+1) = x_1(k)x_2(k)\text{-}x_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \end{cases} \tag{7}$$

Its largest Lyapunov exponent is 0.07456, which shows the system is chaotic.

Now we define an invertible transformation $H: R^3 \to R^3$ as follows:

$$H(x_1,x_2,x_3) = (H_1(x_1,x_2,x_3), H_2(x_1,x_2,x_3), H_3(x_1,x_2,x_3)) = (y_1,y_2,y_3)^T, \tag{8}$$

where

$$\begin{cases} H_1(x_1,x_2,x_3)=\ln[(x_1+2x_2+x_3)+\sqrt{(x_1+2x_2+x_3)^2+1}] \\ H_2(x_1,x_2,x_3)=\ln[(2x_1+x_2+x_3)+\sqrt{(2x_1+x_2+x_3)^2+1}] \\ H_3(x_1,x_2,x_3)=\ln[(2x_1+x_2+2x_3)+\sqrt{(2x_1+x_2+2x_3)^2+1}] \end{cases}$$

Let $Q(X(k),Y(k))=0.2e(k)=0.2(X_m(k)-V(Y(k)))$. Here, $V(Y(k))=H^{-1}(y_1,y_2,y_3)=(x_1,x_2,x_3)^T$. Then $Q(X(k),Y(k))$ makes the error equation (4) be zero asymptotically stable.

Based on the Theorem 1, the driven system has the form:

$$Y(k+1)=G(Y(k),X_m(k))=H[F(X_m)-q(X_m,Y)] \tag{9}$$

3.2. Image Scheme

Suppose the size of a RGB image be $M\times N$, where M and N represent the numbers of rows and column of pixels. In this paper, we choose $M=N=256$ .The sender and the receiver share the systems (7) and (9). Before the remote transmission, they agree on basic initial conditions. The framework of the encryption scheme is shown in Figure 1.

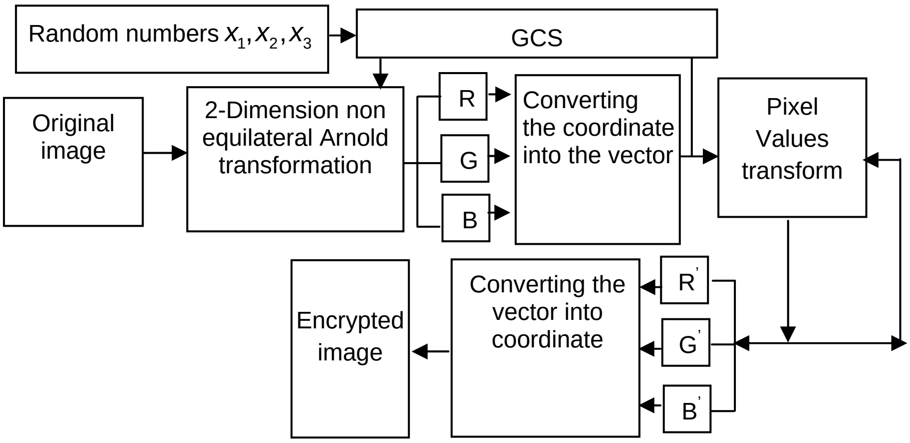

Random numbers x_1,x_2,x_3
GCS
Original image
2-Dimension non equilateral Arnold transformation
R
G
B
Converting the coordinate into the vector
Pixel Values transform
Encrypted image
Converting the vector into coordinate
R'
G'
B'

Figure 1. The framework of the encryption scheme

The detailed process is given as follows:

Step1: generate the chaos streams of length $M\times N\times 3$ by using the initial conditions $X(0)=(x_1(0),x_2(0),x_3(0))^T$, $Y(0)=H(X(0))$. Note that $s(k)=k_1x_1(k)y_3(k)+k_2y_1(k)$, and then the key streams can be derived by a transform from a real number field to the integer domain, that is

$$T(s(k))=\text{mod}(round(\frac{\sqrt{2}\times 10^5\times 255(s(k)-\min(s))}{\max(s)-\min(s)}),256)$$

where $\min(s)=\min\{s(k)|k=1,2,\cdots M\times N\times 3\}$, $\max(s)=\max\{s(k)|k=1,\cdots M\times N\times 3\}$, $k_1=k_2=\sqrt{3}$.

Step 2: divide the image into 4 blocks, and denote them as P_1,P_2,P_3,P_4 in accordance with the row priority.

Step 3: choose the first one P_1 to be as an example, which size is $M_1\times N_1$ .Choose the $s(M_1)$ and $s(N_1)$ as the control key of the adjoint matrix. That is, $b_1=abs(round(s(M_1)\times a_1))$, $r_1=abs(round(s(N_1)\times a_2))$, where $a_1=2$, $a_2=1$. According to the expression (5), the block can be scrambled for k times. The scrambling processing of the remaining blocks is similar to the first one. Combining these sub-blocks, one can get the image P' .

Step 4: convert the RGB components of the image P' into the vectors, which length is $V_r = V_g = V_b = M \times N$. Suppose $V_r(i_1)$、$V_g(i_1)$ and $V_b(i_1)$ represent the RGB components of the spatial coordinates i_1 respectively, and $V_r'(i_1)$、$V_g'(i_1)$、$V_b'(i_1)$ represent the encrypted components. Then the RGB components of encrypted block can be derived by

$$V'_r(i) = (V_r(i) + T(s(1:M \times N)) + V'_r(i-1)) \bmod 256$$

$$V'_g(i) = (V_g(i) + T(s(M \times N + 1 : M \times N \times 2)) + V'_g(i-1)) \bmod 256$$

$$V'_b(i) = (V_b(i) + T(s(M \times N \times 2 + 1 : M \times N \times 3)) + V'_b(i-1)) \bmod 256$$

Step 5: convert the vectors into 2-dimensional coordinate, and complete the pixel value conversion.

The decryption process is the inverse operation of the encryption process.

4. Results and Discussion

The chaotic trajectories of the GCS and the anti-attack ablility of the scheme are simulated and analyzed in this section.

4.1. Chaotic Trajectories of the GCS

In the GCS, we select the following parameters and initial conditions $X(0) = (0.5, 0.5, -1)^T$, $Y(0) = H(X(0))$. It shows the GCS is chaotic. Then the trajectories of system (7) and (9) are shown in Figure 2. From (d), it can be seen that the two pair of variables are in GS with respect to H, so it is in line with expectations.

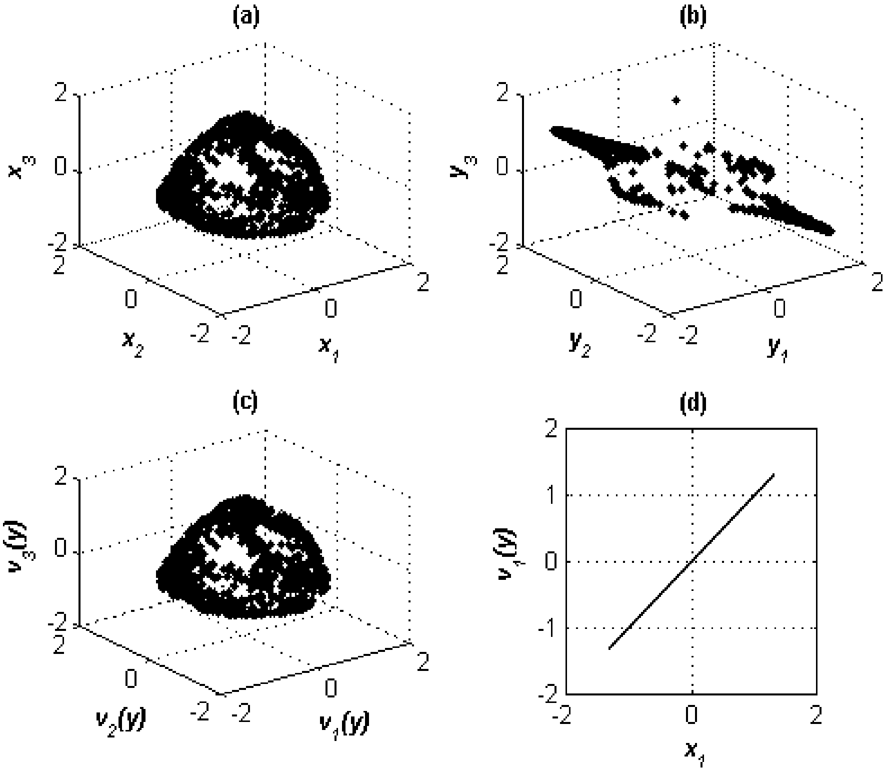


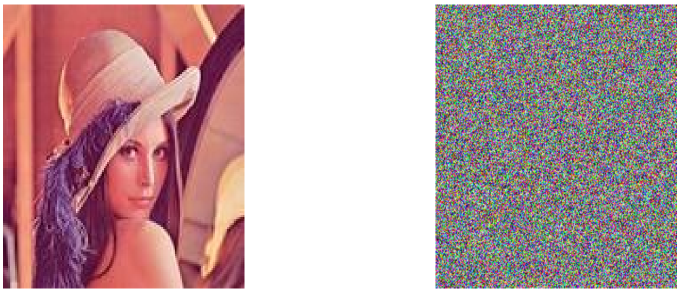
Figure 2. Chaotic trajectories: (a) $x_1 - x_2 - x_3$; (b) $y_1 - y_2 - y_3$; (c) $v_1(y) - v_2(y) - v_3(y)$; (d) $x_1 - v_1(x)$

4.2. Encryption Simulation

Now we use the above image encryption scheme to encrypt the color Lena image shown in Figure 3. (a). And then the encrypted image shown in Figure 3. (b) can be obtained.

4.3. Information Entropy

For the encrypted image, we calculate the information entropies of RGB components by the definition $-\sum_{i=1}^{n} p_i \log p_i$. There are 7.9976, 7.9974 and 7.9971. It is shown that each value of entropy is close to the ideal value 8. Moreover, they are better than the algorithm in [15], which are 7.9921, 7.9879 and 7.9852, respectively. So the algorithm can resist the entropy attack.



(a) (b)

Figure 3. (a) original image; (b) encrypted image

4.4. Key Sensitivity Analysis

To test the key sensitivity, we analyze the change rate of pixel values between the original image and encrypted image decrypted by perturbative keys. The results are shown in Table 1, which reveals that algorithm have a strong sensitivity on the keys.

Table 1. The change rate of pixel values between the original image and encrypted image decrypted by perturbative keys

perturbation	10^{-3}	10^{-7}	10^{-10}	10^{-15}
$x_1(0)$	0.9963	0.9955	0.9964	0.9957
$x_2(0)$	0.9958	0.9961	0.9962	0.9952
$x_3(0)$	0.9961	0.9959	0.9964	0.9965
a_1	0.9960	0.9958	0.9961	0.9963
a_2	0.9962	0.9959	0.9958	0.9964

4.5. Key Space Analysis

By the results of sensitivity, one can obtain that the key space can be $10^{15\times 5} > 2^{249}$ for the five keys in the scheme. If the controlling parameters are set to be the keys, the space would be further expanded. It is shown that the key space in this paper is larger than algorithm proposed in [15], which key space is 2^{192} . So the algorithm can resist the brute-force attack.

4.6. Histogram

The histograms of RGB components for the original image are shown in Figure 4. (a)-(c), while the histograms of RGB colors for the encrypted image are shown in Figure 4. (d)-(f).

The horizontal axis represents 256 gray-levels, while the vertical axis represents the frequency distribution. It can be seen that the histograms between original image and encrypted image are of obviously difference.

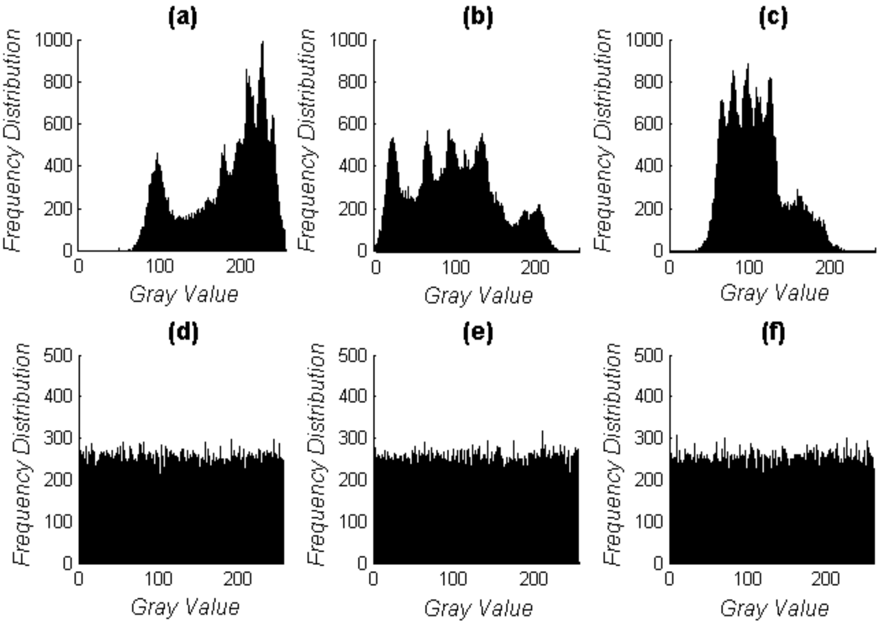


Figure 4. Histograms of RGB components for the original image and the encrypted image

4.7. Correlation of Adjacent Pixels

In order to verify the correlation of adjacent pixels between the original image and encrypted image, we randomly select 2000 pairs of two adjacent pixels from the original image and the encrypted image. Then, calculate the correlation coefficient of each pair by using the following formula:

$$R_{AB} = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A})^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2)}} \qquad (10)$$

Here, A and B are the original image and the encrypted image, while $\bar{A}$ and $\bar{B}$ are the mean.

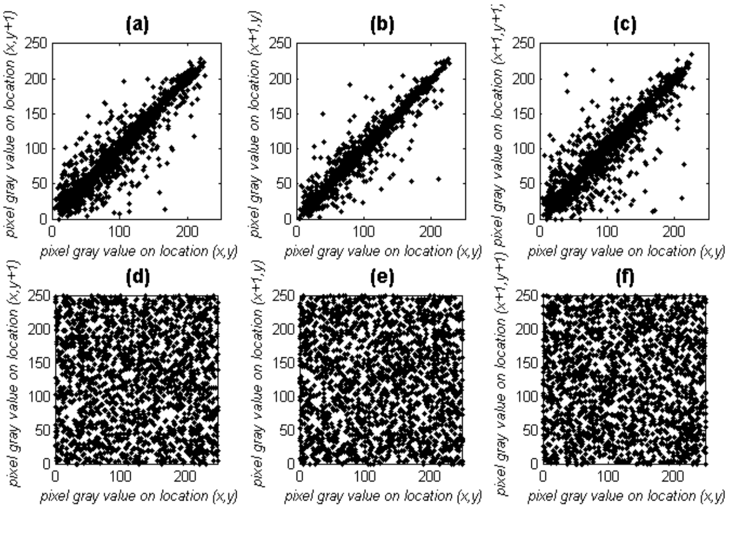


Figure 5. Correlation distribution of the R component

Figure 5 shows the correlation distribution of the R component for the original image and encrypted image. That is, (a)-(c) show the distribution for the original image, and (d)-(e) show the distribution for the encrypted image. From the results, it can be seen that the correlation of the adjacent pixels for the original image is linear, while the correlation for the encrypted is random. One can obtain similar results for B and G components.

4.8. Differential Analysis

In order to avoid the known-plaintext attack, the changes in the cipher image should be significant even with a small change in the original. To quantify this requirement, number of pixel change rate (NPCR) and unified average changing intensity (UACI) are used.

The expected value of NPCR and UACI are 99.609375% and 33.46354% respectively. For the proposed algorithm in this paper, the values of NPCR and UACI are shown in Table 2, where the results are very close to the random case. The results are also compared with the encrypted image generated by reference [15]. It can be found that our output acts similar to the reference [15].

Table 2. The NPCR of the encrypted images

	Encrypted image			Encrypted image in [15]		
	R	G	B	R	G	B
NPCR (%)	99.6045	99.6277	99.5834	99.6162	99.5896	99.6189
UACI (%)	33.4561	33.4564	33.5021	33.4371	33.3542	33.3208

5. Conclusion

This paper constructs a novel GS system on a generalized synchronization theorem. Combining with 2-Dimension non equilateral Arnold transformation, an image encryption scheme is introduced. Simulation results show that the scheme can encrypt and decrypt RGB images accurately. From the security analysis, it can be seen the scheme have large key space and strong key sensitivity. And it has good statistical character which can be resist brute-force attack and entropy attack efficiently. In order to achieve better results, the focus of the future work is to optimize the encryption scheme in theory.

Acknowledgments

This project is supported by the National Nature Science Foundations of China (Grant No. 61074192 and No. 61170037).

References

[1] Deng XP, Zhao DM. Single-channel color image encryption based on asymmetric cryptosystem. *Optics& Laser Technology*. 2012; 44(1): 136-140.

[2] Sui LS, Gao B. Single-channel color image encryption based on iterative fractional Fourier transform and chaos. *Optics& Laser Technology*. 2013; 48: 117-127.

[3] Zhou NR, Wang YX, Gong LH, Chen XB, Yang YX. Novel color image encryption algorithm based on the reality preserving fractional Mellin transforms. *Optics& Laser Technology*. 2012; 44(7): 2270-2281.

[4] Hwang HE. Optical color image encryption based on wavelength multiplexing using cascaded phase only masks in Fresnel transform domain. *Optics Communication*. 2012; 285(5): 567-573.

[5] Behnia S, Akhavan A, Akhshani A, Samsudin A. A novel dynamic model of pseudorandom number generator. *Journal of Computational and Applied Mathematics*. 2011; 235(12): 3455-3463.

[6] Zhang Y, Xia JL, Cai P, Chen B. Plaintext related two-level secret key image encryption scheme. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1254-1262.

[7] Pecora LM, Carroll TL. Synchronization in chaotic systems. *Physical Review Letters*. 1990; 64(8): 821-824.

[8] Grzybowski JMV, Rafikov M, Balthazar JM. Synchronization of the unified chaotic system and application in secure communication. *Communications in Nonlinear Science and Numerical Simulation*. 2009; 14(6): 2793-2806.

[9] Du YL, Zhang JX. The performance of synchronization algorithm in real-time OFDM-PON system. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(7): 1784-1794.

[10] Min LQ, Chen GR. Generalized synchronization in an array of nonlinear dynamic systems with applications to chaotic CNN. *International Journal of Bifurcation and Chaos*. 2013; 23(1): 1350016.

[11] Khan MA, Poria S. Generalized synchronization of nuclear spin generator system and the application in secure communication. *Journal of Dynamical Systems and Geometric Theories*. 2012; 10(1): 53-59.

[12] Zhang YP, Zuo F, Zhai ZJ. Survey on image encryption based on chaos.*Computer Engineering and Design*. 2011; 32(2): 463-466.

[13] Sprott JC. Chaos and time-series analysis, Oxford: Oxford University Press. 2003: 513.

[14] Wu CM, Tian XP. 3-Dimensional non-equilateral Arnold transformation and its application in image scrambling. *Journal of Computer-Aided Design& Computer Graphics*. 2010; 22(10): 1832-1840.

[15] Luo SJ, Qiu SS. Color image encryption algorithm based on spatiotemporal chaos and S-box. *Journal of Circuits and Systems*. 2010; 15(3): 117-122.