A Novel Color Image Encryption Method Based on Sequence Cross Transformation and Chaotic Sequences

Chunming Xu, Yong Zhang, Zhenglan Gu

***Abstract*—Color image encryption attracts more attentions because it contains more information than gray image. A novel color image encryption technique based on sequence cross transformation and chaotic sequences is presented in this paper. The proposed encryption method can make full use of the R, G B components of the color image and fully integrate them by sequence cross transformation and xor operation. In addition, both the initial values of the chaotic system and the key streams are associated with the plain image so that the proposed image encryption method can effectively resist plaintext attack. The experiment results on the classical Baboon image demonstrate that the proposed algorithm is a security and effectiveness tool for image encryption.**

***Index Terms*—color image encryption; chaotic system; sequence cross transformation; bit permutation.**

I. Introduction

IMAGE is a very important information transmission carrier. In the process of information transmission, many images need to protect their contents. Therefore, image encryption technology plays an important role in information security and is highly concerned by researchers. Image encryption mainly changes the original data of image and changes the statistical information of image through scrambling and diffusion, so as to achieve the purpose of hiding information. Digital image has large amount and high redundancy. In addition, there is a strong correlation between adjacent pixels. The traditional encryption algorithm is difficult to effectively solve the problem of image encryption. However, many characteristics of chaotic system such as determinacy, sensitivity to initial values and long-term unpredictability are suitable to solve these problems. As a result, chaotic system has been widely used in image encryption, and a large number of chaos based image encryption algorithms have been proposed [1]–[6].

Compared with gray scale image, color image contains more effective information. Therefore, the research of color image encryption algorithm is more valuable. However, many color image encryption algorithms just encrypt each component of the colour image respectively and ignore the connections among them.

Manuscript received April 10, 2020; revised August 20, 2020. This work is partially supported by the National Natural Science Foundation of China (No.11871417).

Chunming Xu is with School of Mathematics and Statistical, Yancheng Teachers University, 224051,Yancheng, PR China. E-mail: (ycxcm@126.com).

Yong Zhang is with School of Mathematics and Statistical, Yancheng Teachers University, 224051,Yancheng, PR China.E-mail: (137676720@qq.com).

Zhenglan Gu is with School of Mathematics and Statistical, Yancheng Teachers University, 224051,Yancheng, PR China.E-mail: (14530639@qq.com).

Plaintext attack is a problem worthy of consideration in image encryption. Many researchers seeks to generate the key streams utilizing the plainimage information to resist plaintext attacks. For example, Wang utilized image pixel values to generate chaotic system parameters which were used for image encryption [7]. In [8], The SHA hash function of the plainimage was used to calculate the system parameters and initial values of chaotic system. Ye took advantage of the information entropy of the plainimage to generate the key streams in [9].

In view of the above discussion, this paper proposes a novel color image encryption method based on sequence cross transformation and chaotic sequences. The main advantages of the proposed algorithm are:

(1) Both the initial values of the chaotic system and the key streams adopted for encryption in this paper are plaintext-related so that it can effectively resist plain attacks;

(2) The R, G and B components of the color image are well confused by xor operation and bit-level permutation [10]–[14], and the R, G and B components are fully integrated in the cipher image;

(3) The encryption algorithm is simple and easy to implement.

The rest of the paper is organized as follows. A brief review of some fundamental knowledge is given in section 2. Section 3 introduces the proposed image encryption and decryption scheme. Section 4 presents the experimental results and the security of the algorithm. Finally, we conclude this paper in Section 5.

II. Fundamental Knowledge

A. The Chaotic System

In 2019, Atiyeh Bayani etc. [15] presented a four dimensional chaotic system which has a plane as the equilibrium points and is described by:

$$\begin{cases} \dot{x_1} = x_2 \\ \dot{x_2} = x_3 \\ \dot{x_3} = x_3 + ax_2x_4 - x_3x_4 \\ \dot{x_4} = x_1x_2 + bx_2x_3 \end{cases} \tag{1}$$

where x_1, x_2, x_3, x_4 are state variables, and a, b are system parameters. When the system parameters are $a = -1, b = 1$, the system (1) exhibits a chaotic attractor. The state space plots for system (1) are shown in Figure 1.

B. Sequence cross transformation

For a given ordered sequence, divide it into two equal parts from the middle and use the one by one cross method to

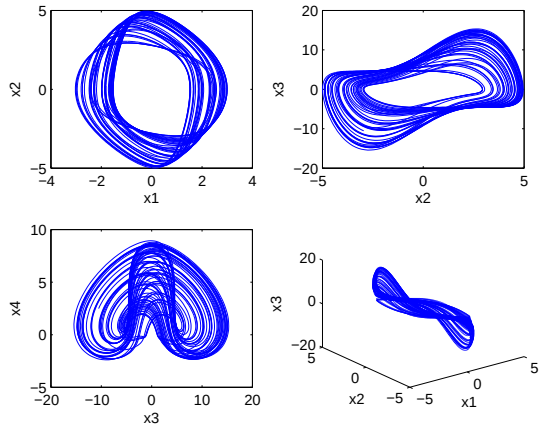

Fig. 1: Typical dynamical behaviors of the 3D autonomous analytic chaotic system.

rearrange it, then we can get the resulting transformation sequence [16]. Take the ordered sequence $1, 2, 3, 4, 5, 6, 7, 8$ as an example, we can get another sequence $1, 5, 6, 2, 3, 7, 4, 8$ using sequence cross transformation. The flowchart of the sequence cross transformation process is shown in Figure 2.

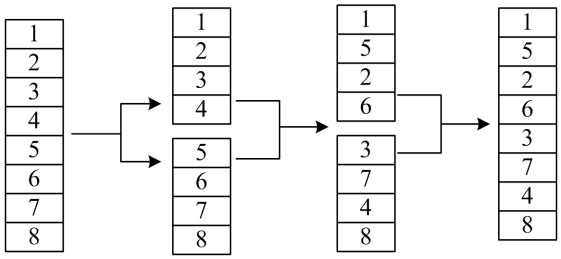

Fig. 2: The flowchart of the sequence cross transformation process.

III. Scheme Description

A. The Encryption Method

Suppose the size of the color plain image P_0 is $M \times N \times 3$, where M and N represent the height and width of the image respectively. Denote the color components of red, green and blue of P_0 as P_R, P_G and P_B, respectively. The specific steps of the encryption algorithm can be described as follows:

Step(1) : Calculate the initial values x_0, y_0, z_0, w_0 of chaotic system (1) by the following equations:

$$\begin{cases} x_0 = \frac{\sum_{ij} P_{Rij}}{255MN} + 0.01 \\ y_0 = \frac{\sum_{ij} P_{Gij}}{255MN} + 0.02 \\ z_0 = \frac{\sum_{ij} P_{Bij}}{255MN} + 0.03 \\ w_0 = \frac{x_0+y_0+z_0}{3} \end{cases} \tag{2}$$

Step(2) : Choose the system control parameters a, b of chaotic system (1).

Step(3) : Iterate the chaotic system (1) for $N + 2000$ times with the parameters x_0, y_0, z_0, remove the former 2000 values and three chaotic sequences x_s, y_s, z_s, w_s of length L can be gotten, where $L = M \times N$. Calculate four sequences S_V, S_R, S_G, S_B with x_s, y_s, z_s, w_s by:

$$\begin{cases} S_V = |x_s| \times 10^{15} \mod 256 \\ S_R = |y_s| \times 10^{15} \mod 256 \\ S_G = |z_s| \times 10^{15} \mod 256 \\ S_B = |w_s| \times 10^{15} \mod 256 \end{cases} \tag{3}$$

Step(4) : Transform the three matrixes P_R, P_G and P_B into three 1D pixel arrays P_{VR}, P_{VG} and P_{VB}, respectively.

Step(5) : Integrate the three pixel arrays P_{VR}, P_{VG} and P_{VB} together to form a $3 \times L$ matrix P_1.

Step(6) : Perform the xor operation on each column of P_1 using the random sequences S_V:

$$\begin{cases} P_1(1,i) = P_1(1,i) \oplus S_V(i) \\ P_1(2,i) = P_1(2,i) \oplus P_1(1,i) \\ P_1(3,i) = P_1(3,i) \oplus P_1(2,i) \end{cases} \tag{4}$$

where $i = 1, 2, \cdots, L$ and symbol " $\oplus$ " is the bitwise exclusive or operator.

Step(7) : For each i, transform $P_1(1,i)$, $P_1(2,i)$ and $P_1(3,i)$ into an 8-bit binary value and connect them, then we can get a bit vector S with the length 24. Scrambling S using the sequence cross transformation method introduced in the second section, we will get a new bit vector T, then

$$\begin{cases} P_1(1,i) = bin2dec(T(1:8)) \\ P_1(2,i) = bin2dec(T(9:16)) \\ P_1(3,i) = bin2dec(T(17:24)) \end{cases} \tag{5}$$

Step(8) : Suppose the cipher vectors of red, green and blue are C_{VR}, C_{VG} and C_{VB}, respectively. Calculate $C_{VR}(1)$, $C_{VG}(1)$ and $C_{VB}(1)$ using the following equation

$$\begin{cases} C_{VR}(1) = P_1(1,i) \oplus S_1(i) \\ C_{VG}(1) = P_1(2,i) \oplus S_2(i) \\ C_{VB}(1) = P_1(3,i) \oplus S_3(i) \end{cases} \tag{6}$$

Step(9) : Calculate all the other vector values of C_{VR}, C_{VG}, C_{VB} except $C_{VR}(1)$, $C_{VG}(1)$ and $C_{VB}(1)$ by the following equation

$$\begin{cases} C_{VR}(i) = P_1(1,i) \oplus (Ks(i) + w_4 S_R(i)) \mod 256 \\ C_{VG}(i) = P_1(2,i) \oplus (Ks(i) + w_4 S_G(i)) \mod 256 \\ C_{VB}(i) = P_1(3,i) \oplus (Ks(i) + w_4 S_B(i)) \mod 256 \end{cases} \tag{7}$$

where $Ks(i) = w_1 P_1(1, i-1) + w_2 P_1(2, i-1) + w_3 P_1(3, i-1)$ and $i = 2, 3, \cdots, L$.

Step(10) : Convert C_{VR}, C_{VG}, C_{VB} into R, G and B channels gray images C_R, C_G, C_B.

Step(11) : Combine these three image matrices C_R, C_G, C_B to get the ciphered color image C.

B. The Decryption Method

The decryption process is similar to the encryption process which mainly contains the following steps:

Step(1) : Suppose the color components of red, green and blue of cipher image C are C_R, C_G and C_B. Transform the three matrixes C_R, C_G and C_B into three 1D pixel arrays C_{VR}, C_{VG} and C_{VB}, respectively.

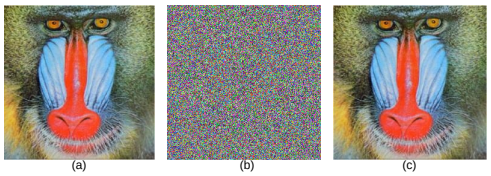

Fig. 3: The experimental results of the encrypted image. (a) The plain image. (b) The ciphered image. (c) The recovered image.

Step(2) : Suppose P_1 is a matrix with the size $3 \times L$. Calculate P_1 except the first column by the following equation:

$$\begin{cases} P_1(1,i) = C_{VR}(i) \oplus (Ks(i) + w_4 S_R(i)) \mod 256 \\ P_1(2,i) = C_{VG}(i) \oplus (Ks(i) + w_4 S_G(i)) \mod 256 \\ P_1(3,i) = C_{VB}(i) \oplus (Ks(i) + w_4 S_B(i)) \mod 256 \end{cases} \tag{8}$$

where $Ks(i) = w_1 P_1(1, i-1) + w_2 P_1(2, i-1) + w_3 P_1(3, i-1)$, $i = 2, 3, \cdots, L$.

Step(3) : Calculate the first column of P_1 using the following equation:

$$\begin{cases} P_1(1,i) = C_{VR}(1) \oplus S_1(i) \\ P_1(2,i) = C_{VG}(1) \oplus S_2(i) \\ P_1(3,i) = C_{VB}(1) \oplus S_3(i) \end{cases} \tag{9}$$

Step(4) : For each i, transform $P_1(1,i)$, $P_1(2,i)$ and $P_1(3,i)$ into an 8-bit binary value and connect them, then we can get a bit vector T with the length 24. Constuct S by $S(1:1:12) = T(1:2:24), S(13:1:24) = T(2:2:24)$, then

$$\begin{cases} P_1(1,i) = bin2dec(S(1:8)) \\ P_1(1,i) = bin2dec(S(9:16)) \\ P_1(1,i) = bin2dec(S(17:24)) \end{cases} \tag{10}$$

Step(5) : Perform the xor operation on each column of P_1 using the random sequences S_V:

$$\begin{cases} P_1(3,i) = P_1(3,i) \oplus P_1(2,i) \\ P_1(2,i) = P_1(2,i) \oplus P_1(1,i) \\ P_1(1,i) = P_1(1,i) \oplus S_V(i) \end{cases} \tag{11}$$

where $i = 1, 2, \cdots, L$.

Step(6) : Convert $P_1(1,:), P_1(2,:)$ and $P_1(3,:)$ into R, G and B channels gray images P_R, P_G, P_B.

Step(7) : Combine three image matrices P_R, P_G, P_B to get the plain color image P_0.

IV. Test and Analysis of the Proposed Scheme

The Matlab software is used as an experimental platform for experiments. The color image Baboon $(216 \times 216 \times 3)$ is used for testing. The system parameters of the chaotic system are $a = 1, b = -1$. The plain image and its corresponding encrypted image and recovered image are shown in Figure 3. It can be found that the encrypted image is quite different from the plain image.

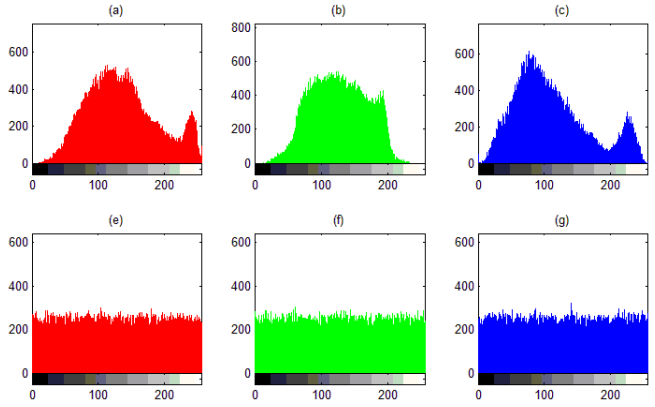

Fig. 4: Histograms of Baboon in red, green, and blue. Histograms of plain and cipher image are shown in row 1 and 2, respectively.

A. Key Space Analysis

Key space is the range of the size of the key. A good encryption algorithm should have sufficient key space to resist violent attacks. The key of image encryption method in this paper is comprised of chaotic system parameters a, b and initial values x_0, y_0, z_0, w_0. Assuming that the computational accuracy is 10^{15}, the key space of the proposed algorithm is 10^{90}, which is large enough to resist violent attacks.

B. Histogram Analysis

The gray histogram indicates the distribution of the image pixel directly, which is an important statistical feature of image. When the gray histogram is uniform and flat, it is difficult for the attacker to obtain the information of the original plain image from the cipher image. Figure 4(a)-(c) gives the histogram of R, G, B components of the Baboon image. The histogram of R, G, B components of the cipher image is shown in Figure 4(d)-(f). As can be seen from Figure 4, the distribution of the pixel values of the cipher image is very uniform so that it has a good resistance to statistical analysis.

C. Correlation Analysis

If the correlation of adjacent pixels in the image is large, the attacker will use this feature to attack. Therefore, a reliable image encryption algorithm needs to be able to reduce the correlation between adjacent pixels. The formula for calculating the correlation of adjacent pixels is as follows [17]:

$$r_{xy} = \frac{\sum_{i=1}^{N}((x_i - E(x))(y_i - E(y)))}{\sqrt{(\sum_{i=1}^{N}(x_i - E(x))^2)(\sum_{i=1}^{N}(y_i - E(y))^2)}} \tag{12}$$

$$E(x) = \sum_{i=1}^{N} x_i \tag{13}$$

$$E(y) = \sum_{i=1}^{N} y_i \tag{14}$$

where x_i and y_i are gray-level values of the selected adjacent pixels, and N is the number of sample pixels.

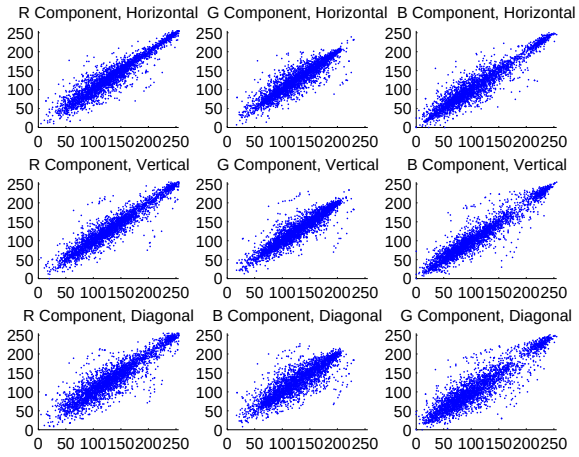

Fig. 5: Correlation distributions of plain image in each direction.

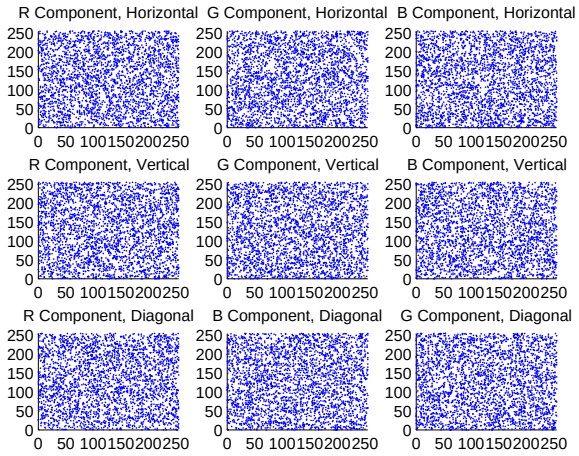

Fig. 6: Correlation distributions of cipher image in each direction.

In order to test the correlation of adjacent pixels, we randomly select 3000 pixels and its adjacent pixels in horizontal, vertical and diagonal directions in plain image and cipher image respectively, and the correlation coefficients in each directions are calculated. Tables 1-2 list the correlation coefficients of plain image and cipher image in each direction. The correlation distribution of r_{xy} are also plotted in Figures 5-6.

TABLE I: Correlation coefficients of the R, G and B components of the plain color image of Baboon.

Component	Horizontal	Vertical	Diagonal
R component	0.9475	0.9436	0.9086
G component	0.9153	0.9112	0.8540
B component	0.9498	0.9495	0.9142

From Tables 1-2 and Figures 5-6, it can be seen that the correlation coefficient values of the original Baboon image are relatively large and close to 1, which indicates that the adjacent pixels of the plain image have strong correlation.

TABLE II: Correlation coefficients of the R, G and B components of the encrypted color image of Baboon.

Component	Horizontal	Vertical	Diagonal
R component	0.0220	-0.0122	-0.0347
G component	-0.0323	-0.0175	0.0123
B component	0.0092	0.0300	0.0053

The correlation coefficients of adjacent pixels in cipher image are all close to 0, which shows that the presented image encryption algorithm can eliminate the correlation of adjacent pixels and resist the corresponding statistical attacks.

D. Information Entropy Analysis

For an image, the greater the randomness is, the greater the information entropy is, and the theoretical maximum value is 8 [18]. The definition of information entropy is as follows:

$$H(m) = -\sum_{i=0}^{255} P(m_i) \log_2 P(m_i) \tag{15}$$

where m_i is the ith gray level for the digital image and $P(m_i)$ represents the probability of m_i.

For a color image, we can calculate the information entropy of R, G and B components respectively. After calculation, the information entropy of R, G and B components of the encrypted color image are 7.9972, 7.9970 and 7.9969, which are all very close to the ideal value 8. As a result, the encryption effect is ideal.

E. Analysis of Differential Attack Resistance

In order to analyze the anti differential attack ability of the image encryption algorithm proposed in this paper, the number of pixels change rate (NPCR) and the unified averaged changed intensity (UACI) [19] are uesd. Suppose there are two plain images and there is only one-pixel difference between them. The NPCR and UACI values can be calculated by

$$NPCR = \frac{\sum_{ij} D_{ij}}{W \times H} \times 100\% \tag{16}$$

$$UACI = \frac{1}{W \times H} \frac{\sum_{ij} (C_1(i,j) - C_2(i,j))}{255} \times 100\% \tag{17}$$

where C_1 and C_2 are the encrypted images for the plain images and D_{ij} is defined by

$$D_{ij} = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \tag{18}$$

TABLE III: The NPCR and UACI values

Component	R	G	B
NPCR	99.6012%	99.6226%	99.6206%
UACI	33.3154%	33.4094%	33.4104%

The ideal values of NPCR and UACI are 1 and 0.334. Table 3 gives the calculation results of NPCR and UACI of the proposed method. From table 3 we could find that both

the values of NPCR and UACI are also all very close to the ideal values, therefore our algorithm has good performance in resisting differential attack.

V. Conclusions

In the paper, a novel color image encryption scheme based on sequence cross transformation and chaotic sequences is introduced. The proposed encryption method has three advantages. Firstly, it can make full use of the R, G and B components of the color image and fuse them in the encryption image well. Secondly, the confusion and diffusion processes are based on distinctive methods and parameters. Therefore, the encryption algorithm is difficult to decrypt. Lastly, the presented image encryption algorithm also has high sensitivity to plain image, which makes the encrypted image more secure. Simulation results and performance analysis are tested on the Baboon image in terms of the histogram, correlation analysis, entropy, number of pixel change rate (NPCR) and unified average change intensity (UACI). The experimental results show that the presented algorithm is effective and is suitable for image encryption.

References

[1] Y.B. Mao, G.R. Chen, S.G. Lian. A novel fast image encryption scheme based on 3D chaotic Baker maps, *International Journal of Bifurcation & Chaos*, vol.14, no.10, pp.3613-3624, 2004.

[2] H. Natiq, N.M.G. Al-Saidi, M.R.M. SaidAdem Kilicman. A new hyperchaotic map and its application for image encryption, *The European Physical Journal Plus*, vol.133, no.6, pp.5-18, 2018.

[3] M. Ghebleh, A. Kanso, D. Stevanovi. A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation , *Multimedia Tools and Applications*, vol.77, no.6, pp.7305-7326, 2018.

[4] J.H. Wu, X.F. Liao, B. Yang. Image encryption using 2D Hnon-Sine map and DNA approach, *Signal Processing*, vol.153, no.12, pp.11-23, 2018.

[5] S. Ahadpour, Y. Sadra. A chaos-based image encryption scheme using chaotic coupled map lattices, *International Journal of Computer Applications*, vol.49, no.2, pp.15-18, 2012.

[6] P. Li, J. Xu; J. Mou. F.F. Yang. Fractional-order 4D hyperchaotic memristive system and application in color image encryption, *EURASIP Journal on Image and Video Processing*, vol.26, no.10, pp.11-23, 2017.

[7] Wang Xingyuan, Zhao Yuanyuan , Zhang Huili. A novel color image encryption scheme using alternate chaotic mapping structure, *Optics and Lasers in Engineering*, vol.82, pp.79-86, 2016.

[8] Sun Shuliang, Guo Yongning, Wu Ruikun. A Novel Image Encryption Scheme Based on 7D Hyperchaotic System and Row-column Simultaneous Swapping, *IEEE Access*, vol.7, no.3, pp.28539-28547, 2019.

[9] Guodong Ye. A Chaotic Image Encryption Algorithm Based on Information Entropy , *International Journal of Bifurcation and Chaos*, vol.28, no.1, pp.1-11, 2018.

[10] J.H. Wu, X.F. Liao, B. Yang. Cryptanalysis and enhancements of image encryption based on three-dimensional bit matrix permutation, *Signal Processing*, vol.142, pp.292-300, 2018.

[11] L. Xu, Z. Li, J. Li. A novel bit-level image encryption algorithm based on chaotic maps, *Optics and lasers in engineering*, vol.78, pp.17-25, 2016.

[12] Y.C. Zhou, W.J. Cao, L.P. Chen. Image encryption using binary bitplane, *Singal Process*, vol.100, pp.197-201, 2014.

[13] Z.L. Zhu, W. Zhang, K.W. Wong, Y. Hai. A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, vol.181, no.6, pp.1171-1186, 2011.

[14] W. Zhang, Y. Hai, Y.L. Zhao, Z.L. Zhu. Image encryption based on three-dimensional bit matrix permutation. *Signal Process*, vol.118, pp.36-50, 2016.

[15] Atiyeh Bayani, Karthikeyan Rajagopal, Abdul Jalil M.Khalaf, Sajad Jafari, G.D.Leutcho, J.Kengned. Dynamical analysis of a new multistable chaotic system with hidden attractor: Antimonotonicity, coexisting multiple attractors, andoffset boosting, *Physics Letters A*, Vol.383, pp.1450-1456, 2019.

[16] Jijun Wang, Xianquan Zhang. A novel image scrambling and encryption algorithm based on sequence cross transformation, *Computer Applications and Software*, vol.26, no.12, pp.111-114, 2009. (in Chinese).

[17] X. Wu, H. Kan, and J. Kurths. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps, *Applied Soft Computing*, vol. 37, pp. 24-39, Dec. 2015.

[18] R. E. Boriga, A. C. Dascalescu, and A. V. Diaconu. A new fast image encryption scheme based on 2D chaotic maps, *IAENG International Journal of Computer Science*, vol. 41, no. 4, pp. 249-258, 2014.

[19] Y. Wu, J. P. Noonan, and S. Agaian. NPCR and UACI randomness tests for image encryption, *Journal of Selected Areas in Telecommunications*, vol. 1, no. 2, pp. 31-38, 2011.