COLOR IMAGE ENCRYPTION BASED ON MULTIPLE CHAOTIC SYSTEMS

Yuting Xi, Xing Zhang and Ruisong Ye

Department of Mathematics, Shantou University
Shantou, Guangdong, 515063, P. R. China

ABSTRACT

This paper proposed a novel color image encryption scheme based on multiple chaotic systems. The ergodicity property of chaotic system is utilized to perform the permutation process; a substitution operation is applied to achieve the diffusion effect. In permutation stage, the 3D color plain-image matrix is converted to a 2D image matrix, then two generalized Arnold maps are employed to generate hybrid chaotic sequences which are dependent on the plain-image's content. The generated chaotic sequences are then applied to perform the permutation process. The encryption's key streams not only depend on the cipher keys but also depend on plain-image and therefore can resist chosen-plaintext attack as well as known-plaintext attack. In the diffusion stage, four pseudo-random gray value sequences are generated by another generalized Arnold map. The gray value sequences are applied to perform the diffusion process by bitxoring operation with the permuted image row-by-row or column-by-column to improve the encryption rate. The security and performance analysis have been performed, including key space analysis, histogram analysis, correlation analysis, information entropy analysis, key sensitivity analysis, differential analysis etc. The experimental results show that the proposed image encryption scheme is highly secure thanks to its large key space and efficient permutation-substitution operation, and therefore it is suitable for practical image and video encryption.

KEYWORDS

Generalized Arnold Map, Permutation, Substitution, Chaotic System, Image Encryption

1. INTRODUCTION

Nowadays more and more images and videos are transmitted through network due to the dramatic developments of IT era. Cryptographic approaches are therefore critical for secure image storage and distribution over public networks. As an effective technique to protect contents from being intercepted, tampered and destroyed illegally, encryption has attracted much attention recently. Chaos has been extensively adopted in encryption due to its ergodicity, pseudo-randomness and sensitivity to initial conditions and control parameters, which are in line with the fundamental requirements like confusion and diffusion in cryptography [1]. These properties make chaotic systems a potential candidate for construction cryptosystems and many chaos-based image encryption algorithms are proposed [2,3,4,5,6,7,8,9,10]. Ye proposed an image encryption scheme with an efficient permutation-diffusion mechanism, which shows good performance, including huge key space, efficient resistance against statistical attack, differential attack, known-plaintext attack as well as chosen-plaintext attack [6]. In both the permutation and diffusion stages, generalized Arnold maps with real number control parameters are applied to generate pseudo-random sequences and therefore enlarge the key space greatly. Meanwhile, a two-way diffusion operation is executed to improve the security of the diffusion function. Wang et al. [11] employed Logistic map in the permutation process and Gravity Model in the diffusion process to achieve good security and performance. Wen et al. constructed a new improved chaotic system by

DOI: 10.5121/ijnsa.2016.8503

a nonlinear combination of 1D Logistic map and sine map. Wang et al. [13] pointed out that Arnold map has short periodic and is easy to be cracked by chosen-plaintext attack, so they used this map in a different way to overcome the short periodic issue and enhance the security. In [14,15], Chebyshev maps and ordinary differential equations were used to generate key stream respectively to enhance the security and performance of the proposed image encryption. In [16], Chen et al. presented a novel image encryption scheme using Gray code based permutation approach. The new permutation strategy takes full advantage of Gray-code achievements, and is performed with high efficiency. A plain pixel-related image diffusion scheme is introduced to compose a complete cryptosystem.

In this paper, we use multiple chaotic systems to generate pseudo-random sequences for color image encryption with permutation-substitution mechanism. In the permutation stage, we use two chaotic systems to disorder the pixels' positions of the plain-image based on the ergodicity of generalized Arnold maps. Firstly, the 3D color plain-image matrix is converted to 2D image matrix, then the sum of the pixel values of the 2D image matrix will be used to be the initial gray value seed. The key streams applied to perform the permutation are yielded by randomly choosing one of two generalized Arnold maps according to the yielded seed and each pixel' gray value of the plain-image. As a result, the permutation process strongly depends on the plain-image and therefore the image encryption scheme can resist efficiently known-plaintext attack and chosen-plaintext attack. In the diffusion stage, four vectors are generated by another generalized Arnold map, then the gray values of row and column pixels of 2D image matrix are mixed with the pseudo-random number sequences via bitxoring operation. The security and performance of the proposed image encryption scheme has been analyzed thoroughly, including statistical analysis (histograms, correlation coefficients, information entropy), key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis, etc. All the experiment results show that the proposed image encryption scheme is highly secure and demonstrates excellent performance.

The remainder of this paper is organized as follow. The proposed image encryption scheme is presented in Section 2. Section 3 shows the experimental results and performance analysis. Finally, conclusions are drawn in the last section.

2. THE PROPOSED IMAGE ENCRYPTION SCHEME

2.1. ARNOLD MAP

There are two stages in the proposed color image encryption scheme, permutation and diffusion. Arnold map, a kind of two-dimensional area-persevering chaotic map, will be adopted in both processes to shuffle the positions of the plain image pixels and weaken the relationship between adjacent pixels. The mathematical formula of classical Arnold map is given by

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1, \tag{1}$$

where "$x \bmod 1$" represents the fractional part of a real number x. The map is area preserving since the determinant of its linear transformation matrix is 1. The unit square is first stretched by the linear transform matrix and then folded back to the unit square by the modulo operation, which can be shown in Fig. 1. The 2D classical Arnold map can be generalized by introducing two real parameters to Eq. (1):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1, \tag{2}$$

where p, q are the real system control parameters. The generalized Arnold map (2) has one Lyapunov characteristic exponent

$$\sigma_1 = 1 + \frac{1+ab+\sqrt{a^2b^2+4ab}}{2} > 1,$$

so the generalized Arnold map is always chaotic for $a>0$, $b>0$. The extension of a, b from positive integer numbers to positive real numbers is an essential generalization of the control parameters, enlarging the key space significantly if it is used to design cryptosystem. Fig. 2 (a) shows an orbit of $(x_0, y_0) = (0.5231, 0.7412)$ with length 1500 generated by the generalized Arnold map (2) with a=5.324, b=18.2, the x-coordinate and the y-coordinate sequences of the orbit are plotted in Fig. 2 (b) and Fig. 2(c) respectively. Some other good dynamical features in the generalized Arnold map, such as desirable auto-correlation and cross-correlation features are demonstrated in Figs. 2(d)-(f). The good chaotic nature makes it can provide excellent random sequence, which is suitable for designing cryptosystem.

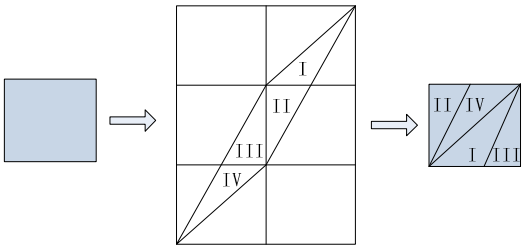
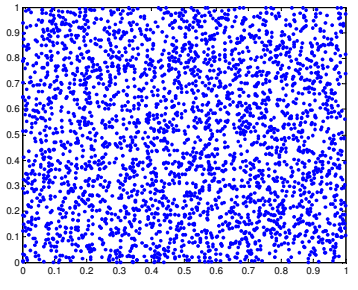
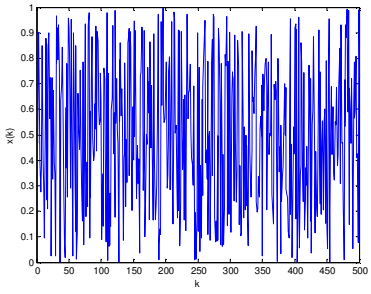


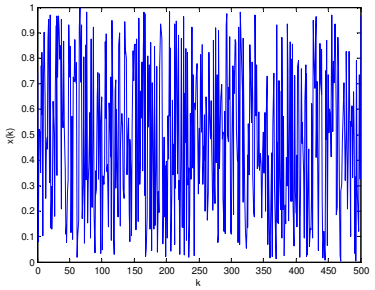
Fig.1. The Arnold map



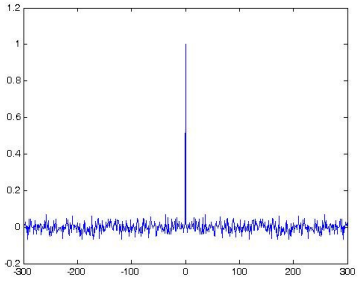
(a) The orbit of (0.5231, 0.7412)



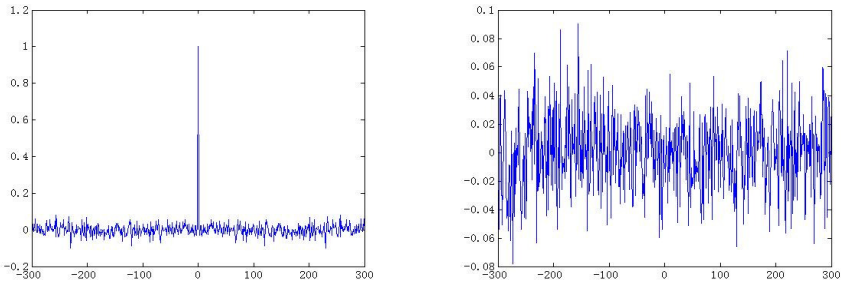
(b) Sequence $\{x_k, k = 0, \cdots, 1500\}$



(c) Sequence $\{y_k, k = 0, \cdots, 1500\}$



(d) Auto-correlation of $\{x_k, k = 0, \cdots, 1500\}$



(e) Auto-correlation of $\{y_k, k = 0,\cdots,1500\}$ (f) Cross-correlation of x_k and y_k sequences

Fig.2. Orbit derived from the generalized Arnold map with a=5.324, b=18.2.

2.2. PERMUTATION PROCESS

In the permutation process, the 3D color plain-image matrix A with size $M \times N \times 3$ is converted to a 2D image matrix B with size $M \times 3N$ firstly. Then we will create a zero vector C with length $M \times N \times 3$. Now what we need to do is just put the $M \times N \times 3$ pixels in B into C randomly. In this image encryption scheme, we realize it by using two generalized Arnold maps, the detail operation procedures are described as follows.

Step 1. Set the appropriate parameters $a1, b1$, $a2, b2$ for two generalized Arnold maps and their common initial values x, y. Another sufficiently large integer $M1$ is also set to be the iterate times, $M1$ is usually set to be one integer number close to $M \times N \times 3$. In this paper, we set $M1$ to be $M \times N \times 3$.

Step 2. Modulate x, y by iterating two generalized Arnold maps for $N1$ times respectively to avoid the harmful effect of transitional procedure of the chaotic orbits. $N1$ can be set as a secret key. For example, we set $N1 = 200$ in the experiments.

Step 3. Calculate

$$sum = \sum_{i=1}^{M} \sum_{j=1}^{3N} B(i, j), p = mod(sum, 256). \tag{3}$$

We initialize the index matrix $index$ to be zero matrix with size $M \times 3N$ and set the initial ergodic counting number $K = 0$. For $i = 1 : M1$, we execute Steps 4-6.

Step 4. Calculate $q = mod(p, 2)$, q is equal to 0 or 1, so we can use q to dynamically assign one generalized Arnold map to generate hybrid chaotic sequences. If $q = 0$, we iterate the first generalized Arnold map once to generate new x, y, otherwise, the second generalized Arnold map will be iterated.

Step 5. The position coordinates (s,t) can be calculated by

$$s = floor(x \times M) + 1, t = floor(y \times 3N) + 1, \tag{4}$$

where $floor(x)$ returns the nearest integer less than or equal to x.

Step 6. If $index(s,t)=0$, then set $K=K+1$, $C(k)=B(s,t)$, $p=B(s,t)$ and $index(s,t)=1$; otherwise, skip this step.

Step 7. Generally speaking, the traversing counting number K is often less than $M\times N\times 3$ after the loop Steps 4-6 is finished. So we need to put the pixels which are not traversed orderly from left to right and top to bottom into the remainder part of vector C. We finally converted the vector C into one 2D matrix C with height M and width $3N$.

2.3. SUBSTITUTION PROCESS

In the diffusion stage, four vectors are generated by another generalized Arnold map, then the gray values of row and column pixels of 2D image matrix C are masked with the four pseudo-random number sequences via bitwise XOR operation. The detail operation procedures are described as follows.

Step 1. For an given generalized Arnold map with parameter a,b and initial value $x1, y1$, we modulate $x1, y1$ by iterating this generalized Arnold map for 100 times to avoid the harmful effect of transitional process.

Step 2. Generate two chaotic sequences $x(i), y(i), i=1:M$ by the generalized Arnold map, then two row sequence SVR and IVC with length M will be generated by

$$\begin{aligned} SVR(i) &= floor(x(i)\times 256),\\ IVC(i) &= floor(y(i)\times 256), i=1,\cdots,M. \end{aligned} \tag{5}$$

Step 3. Generate two chaotic sequences $x1(i), y1(i), i=1:3N$ by the generalized Arnold map with initial values $x(M), y(M)$, then two row sequences SVC and IVR with length $3N$ will be generated by

$$\begin{aligned} IVR(i) &= floor(x(i)\times 256),\\ SVC(i) &= floor(y(i)\times 256), i=1,\cdots,3N. \end{aligned} \tag{6}$$

Step 4. Get the cipher image CC by masking C with the four pseudo-random number sequences via bitwise XOR operation.

$$CC(1,:)=C(1,:)\oplus IVR\oplus SVR(1),\quad CC(i,:)=C(i,:)\oplus CC(i-1,:)\oplus SVR(i), i=2,\cdots,M,$$
$$CC(:,1)=CC(:,1)\oplus IVC'\oplus SVC(1),\quad CC(:,j)=CC(:,j)\oplus CC(:,j-1)\oplus SVC(j), j=2,\cdots,3N.$$

3. SECURITY AND PERFORMANCE ANALYSIS

According to the basic principle of cryptology [17], an ideal encryption scheme should have large key space to make brute-force attack infeasible, it should also well resist various kinds of attacks like statistical attack, differential attack, chosen-plaintext attack, etc. In this section, the security analysis has been performed on this proposed encryption scheme, such as, key space analysis, statistical analysis, correlation between plain and cipher images, key sensitivity analysis, differential analysis, encryption rate analysis, etc. Experimental simulations and extensive performance analysis for the proposed scheme and the comparable scheme proposed in [18] have been carried out. The cipher keys for the comparable algorithm are the same as those in [18]. All the simulations are performed on a computer equipped with an Intel Xeon 2.13 GHz CPU 2GB

memory and 300GB hard disk space running Windows 7 Professional. The compilation platform is Matlab 7.1. The experimental results prove the superior security and high efficiency of this scheme.

3.1. KEY SPACE ANALYSIS

Key space is composed of all the possible cipher keys in the proposed image encryption scheme. An ideal image encryption scheme should contain sufficiently large key space for compensating the degradation dynamics in PC and should be large enough to effectively resist brute-force attack and prevent invaders decrypting original data even after they invest large amounts of time and resources. It was pointed out that the key space should beat at least 2^{100} in order to resist all kinds of common attacks [9]. Regarding our proposed image encryption scheme, the key space consists of the initial values x, y and parameters $a1, b1, a2, b2$ of the two chaotic systems in permutation process and the initial values $x1, y1$, parameters a, b in diffusion process. All the initial values $x, y, x1, y1$ and the control parameters $a, b, a1, b1, a2, b2$ are floating point numbers. If they are represented as floating number with precision 10^{-14} as we have used in the key sensitivity test, the total number of cipher keys is $10^{14\times10} = 10^{140}$, which is approximately equal to 465 bits. The key space is large enough to resist the brute-force attack.

3.2. STATISTICAL ANALYSIS

Shannon pointed out the possibility to solve many kinds of ciphers by statistical analysis [17]. Therefore, passing the statistical analysis on cipher-image is crucial for a cryptosystem. Indeed, an ideal cryptosystem should be robust against any statistical attack. To prove the security of the proposed encryption scheme, we perform the following statistical tests.

(i) Histogram analysis. A histogram shows the distribution of pixel values in an image by plotting the number of pixels at each grey level. An ideal histogram of an effectively ciphered image should be uniform and much different from that of the plain image. For an 8-bit gray image, there are 256 different possible intensities, the histogram shows the distribution of pixels among those 256 intensity values. For a 24-bit color image, we can draw the histogram for red, green, blue channels respectively. Encrypt the color image Lena one round with cipher keys $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33, 4, 8, 62, 48)$. Then we plot the histograms for red, green, blue channels of Lena and the cipher-image in Fig. 3. It is obvious that the histograms of the cipher image are uniform and quite different from that of the plain image, which implies that the redundancy of the plain image is successfully hidden after the encryption, so it does not provide any useful information for statistical attacks.

(a) plain-image Lena (b) cipher-image of Lena

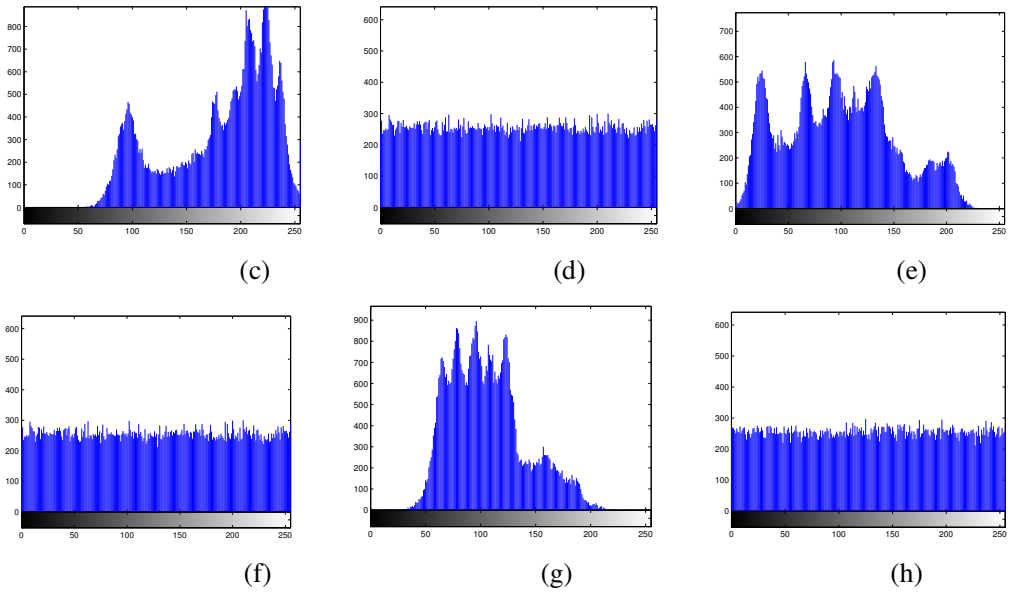


Fig. 3. The histogram analysis result. (c)-(e) Red, green, blue channel component of plain-image; (f)-(h) Red, green, blue channel component of cipher-image.

(ii) Correlation analysis of adjacent pixels. It is of common sense that in a meaningful image each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. For an ideal encryption technique, the cipher image should get rid of the drawback of high correlation between pixels. In order to quantify and compare the correlation between plain-image and cipher-image, we calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels of them respectively. The correlation coefficients of the selected pairs in horizontal, vertical and diagonal direction are calculated according to Eq. (7), where x_i and y_i are the *ith* selected pair pixels. T is the total pixel pairs' number of the sample. The correlation coefficients in horizontal, vertical or diagonal direction of the selected pairs for plain-image Lena and the cipher-image are given in Table 1. From the data in Table 1, we can see that even though there is high correlation in plain-image, the correlation in cipher-image is negligible. The proposed image encryption technique significantly reduces the correlation between the adjacent pixels of the plain-image.

$$Cr = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)D(y)}},\ \operatorname{cov}(x,y) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x)\right)\left(y_i - E(y)\right),$$

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i, D(x) = \frac{1}{T}\sum_{i=1}^{T}\left(x_i - E(x)\right)^2 . \tag{7}$$

(iii) Information entropy analysis. Information entropy is one of the criteria to evaluate the randomness and the unpredictability of an information source. The entropy $H(m)$ of a message source *m* is defined by

$$H(m) = -\sum_{i=0}^{2^L-1} P(m_i)\log_2 P(m_i)(bits), \tag{8}$$

where m is the source, L is the number of bits to represent the symbol m_i, and $P(m_i)$ is the probability of the symbol m_i. For a truly random source consist of 2^L symbols, the entropy is L. So for an effective encryption algorithm, the entropy of the cipher image with 256 gray levels should be close to 8. Otherwise, the information source is not random enough and there exists a certain degree of predictability, which makes the encryption algorithm insecure.
For a 24-bit color image, the information entropy for each color channel (Red, Green and Blue) is given by

$$H^{R/G/B}(m) = -\sum_{i=0}^{2^8-1} P^{R/G/B}(R(I_i)\log_2 \frac{1}{P^{R/G/B}(RI_i)}.$$

We have calculated the information entropy for plain-image Lena and its cipher-image by the proposed encryption scheme. The value of information entropy for the cipher-image produced by the proposed image encryption scheme is very close to the expected value of truly random image, i.e., 8bits. Therefore the proposed encryption scheme shows extremely robustness against entropy attacks. For comparison, we also calculate the information entropy of cipher image of Lena by algorithm in [18]. The results are shown in Table 2. We can see the information leakage in this proposed encryption procedure is negligible and when faced with entropy analysis attack, this proposed encryption show good performance.

Table 1. Correlation between adjacent pixels of plain-image and cipher-image.

Image	color channel	horizontal	vertical	diagonal
Plain-image Lena	R	0.9446	0.9720	0.9212
Cipher-image of Lena	R	-0.0020	0.0030	0.0035
Plain-image Lena	G	0.9465	0.9729	0.9360
Cipher-image of Lena	G	-0.0036	0.0007	0.0041
Plain-image Lena	B	0.9046	0.9465	0.8677
Cipher-image of Lena	B	0.0040	0.0043	0.0031

(iv) Correlation between plain-images and cipher-images. For an efficient encryption scheme, the cipher image should be much different from plain image and has low correction with plain image. We have already analyzed the correction between plain-image and cipher-image by computing the two-dimensional correlation coefficients between various color channels of plain-image and cipher-image. The two-dimensional correlation coefficients are calculated by

$$C_{AB} = \frac{\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(A_{i,j}-\overline{A})(B_{i,j}-\overline{B})}{\sqrt{(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(A_{i,j}-\overline{A})^2)(\frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}(B_{i,j}-\overline{B})^2)}},$$

$$\overline{A} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}A_{i,j}, \overline{B} = \frac{1}{H\times W}\sum_{i=1}^{H}\sum_{j=1}^{W}B_{i,j},$$

where A represents one of the three channels of plain-image, B represents one of the three channels of cipher-image. $\overline{A}$ and $\overline{B}$ are the mean value of the two-dimension matrix A and B

respectively. H and W are the height and width of image A or B. So we can get nine different correlation coefficients for a pair of plain-image and cipher-image $(C_{RR}, C_{RG}, C_{RB}, C_{GR}, C_{GG}, C_{GB}\ C_{BR},$ C_{BG} and $C_{BB})$. For example, C_{RR} means the correlation between red channel of plain-image and red channel of cipher-image. The results of correction between Lena and its cipher image are shown in Table.3. We can see that the correlation between various channels of plain image and cipher image are very small, hence the cipher-image owns the characteristic of a random image.

3.3. KEY SENSITIVITY ANALYSIS

Extreme key sensitivity is an essential feature of an effective cryptosystem, and key sensitivity of a cryptosystem can be observed in two ways: (i) completely different cipher-images should be produced even if we use slightly different keys to encrypt the same plain-image. (ii) the cipher image cannot be correctly decrypted even if there is tiny difference between encryption and decryption keys. For key sensitivity analysis, we will use the following cipher keys to perform the simulation (one is master cipher key, the other keys are produced by introducing a sight change to one of the parameter of master cipher with all other parameters remain the same). Master cipher key: MKEY $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33, 4, 8, 62, 48)$; Ten slightly different keys:

SKEY1 $(0.3201-10^{-14}, 0.6317, 0.4807, 0.7815, 100, 33, 4, 8, 62, 48)$,
SKEY2 $(0.3201, 0.6317-10^{-14}, 0.4807, 0.7815, 100, 33, 4, 8, 62, 48)$,
SKEY3 $(0.3201, 0.6317, 0.4807-10^{-14}, 0.7815, 100, 33, 4, 8, 62, 48)$,
SKEY4 $(0.3201, 0.6317, 0.4807, 0.7815-10^{-14}, 100, 33, 4, 8, 62, 48)$,
SKEY5 $(0.3201, 0.6317, 0.4807, 0.7815, 100-10^{-14}, 33, 4, 8, 62, 48)$,
SKEY6 $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33-10^{-14}, 4, 8, 62, 48)$,
SKEY7 $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33, 4-10^{-14}, 8, 62, 48)$,
SKEY8 $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33, 4, 8-10^{-14}, 62, 48)$,
SKEY9 $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33, 4, 8, 62-10^{-14}, 48)$,
SKEY10 $(0.3201, 0.6317, 0.4807, 0.7815, 100, 33, 4, 8, 62, 48-10^{-14})$.

(i)To evaluate the key sensitivity in the first case, we encrypt plain-image Lena with MKEY and get the first cipher image, then we encrypt Lena with SKEY1-SKEY10 and get other ten cipher images. We have computed the correlation coefficients between the first cipher image and the other ten cipher images. The results are given in Table 4. From the table, we can see that all the correlation coefficients are very small which indicate that even there is only slightly difference between the cipher keys, the cipher images are greatly different. Hence the proposed encryption scheme is extremely sensitive to the cipher keys.

(ii)Decryption using keys with slight difference are also performed in order to evaluate the key sensitivity of the second case. Firstly, we decrypt the cipher image using MKEY and we get the plain-image Lena. Secondly, ten decrypted images are generated when we decrypt the cipher-image using SKEY1-SKEY10. We have computed the correlation coefficients between Lena and this ten decrypted images, the results have been given in Table 5. From the data, we can see even there is only a slightly difference between the decipher keys, the deciphered images have low correlation coefficients with the plain-image Lena. So for the second case, the proposed encryption scheme is of highly sensitive to the cipher keys too.

Table 2. Information entropy analysis.

Image	R	G	B
Plain-image Lena	7.2763	7.5834	7.0160
Cipher-image	7.9972	7.9971	7.9977
Cipher-image [18]	0.9973	7.9973	7.9967

Table 3. Correlation between plain-image Lena and its cipher-image.

	Cipher-image R	G	B
Plain-image Lena R	-0.0037	-0.0049	0.0001
G	0.0044	-0.0052	0.0014
B	0.0045	-0.0020	0.0024

3.4. DIFFERENTIAL ATTACK ANALYSIS

For an efficient encryption scheme, a slightly difference in the plain image should cause amount of difference in the cipher image. Two indicators, which are number of pixels change rate (NPCR) and unified average changing intensity (UACI), are used to measure the influence of one pixel change in the plain image on the cipher image. In order to calculate NPCR and UACI, suppose two plain images I_1 and I_2 with difference in only one pixel, and their cipher images are denoted as C_1 and C_2. Then we create a matrix D, when $C_1(i,j) = C_2(i,j)$, $D(i,j) = 0$; otherwise, $D(i,j) = 1$. NPCR and UACI are calculated by

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \quad UACI = \frac{1}{W \times H}\left(\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right) \times 100\%,$$

where W, H are the width and height of the images. We have performed the differential attack analysis in two cases: (i) Encrypt the plain-image Lena using the proposed encryption scheme and get a cipher image. Add 1 to the last pixel value of Lena, then we get a new plain image. Encrypt the new plain-image, then the new cipher image is compared with the old cipher image to calculate NPCR and UACI. The results are given in Table 6. (ii) Randomly choosing 10 pixels (one at a time) from Lena and add their values by one unit. The average NPCR and UACI are given in Table 7. From the two tables, we can see even though the algorithm in [18] have better performance on NPCR in Table 6, but on the whole, the proposed encryption scheme is more stable and has better performance on differential analysis.

Table 4. Key sensitivity analysis I.

	Correlation coefficients between the encrypted images obtained using MKEY and									
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5	SKEY6	SKEY7	SKEY8	SKEY9	SKEY10
Crr	0.0030	-0.0089	-0.0011	-0.0012	0.0021	-0.0030	-0.0000	-0.0021	-0.0080	-0.0027
Crg	0.0027	-0.0039	0.0014	-0.0066	-0.0042	0.0024	0.0024	0.0040	-0.0044	0.0008
Crb	0.0088	-0.0016	-0.0021	0.0084	0.0033	0.0010	0.0047	0.0078	-0.0013	-0.0041
Cgr	0.0001	-0.0038	0.0063	-0.0043	-0.0009	0.0006	-0.0048	-0.0012	0.0020	0.0006
Cgg	0.0009	-0.0005	-0.0010	-0.0025	-0.0042	0.0025	0.0025	-0.0043	0.0039	-0.0018
Cgb	0.0018	0.0004	0.0015	0.0032	0.0048	-0.0003	-0.0029	-0.0036	0.0044	-0.0016
Cbr	0.0064	0.0009	0.0026	0.0009	0.0037	0.0010	0.0025	0.0070	0.0020	-0.0063
Cbg	0.0048	-0.0006	-0.0009	0.0021	0.0005	0.0090	-0.0046	-0.0008	0.0032	-0.0003
Cbb	0.0033	-0.0048	-0.0007	0.0038	0.0033	-0.0032	-0.0054	-0.0006	0.0060	0.0027

Table 5. Key sensitivity analysis II.

	Correlation coefficients between the decrypted images obtained using MKEY and									
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5	SKEY6	SKEY7	SKEY8	SKEY9	SKEY10
Crr	0.0086	0.0038	-0.0065	0.0004	0.0158	0.0015	0.0014	0.0119	0.0097	0.0064
Crg	0.0067	0.0081	-0.0061	0.0044	0.0011	-0.0054	0.0050	0.0046	0.0147	0.0065
Crb	0.0046	0.0014	-0.0005	-0.0051	-0.0023	-0.0078	0.0116	0.0027	0.0090	-0.0044
Cgr	0.0097	0.0054	-0.0044	-0.0014	0.0106	-0.0026	0.0035	0.0091	0.0092	0.0035
Cgg	0.0052	0.0086	-0.0063	0.0015	0.0012	-0.0061	0.0068	0.0090	0.0137	0.0058
Cgb	0.0053	0.0030	-0.0003	-0.0056	-0.0026	-0.0124	0.0103	0.0041	0.0043	-0.0028
Cbr	0.0099	0.0046	-0.0043	-0.0024	0.0099	-0.0029	0.0044	0.0059	0.0088	0.0007
Cbg	0.0050	0.0047	-0.0048	-0.0006	0.0003	-0.0050	0.0057	0.0086	0.0095	0.0046
Cbb	0.0042	0.0027	0.0016	-0.0063	-0.0021	-0.0132	0.0071	0.0021	0.0011	-0.0008

Table 6. Differential analysis I.

	NPCR(%)			UACI(%)		
	Red	Green	Blue	Red	Green	Blue
The proposed scheme	99.61	99.59	99.59	33.55	33.60	33.55
The scheme proposed in [18]	99.57	99.64	99.65	33.42	33.19	33.38

Table 7. Differential analysis II.

	Average NPCR(%)			Average UACI(%)		
	Red	Green	Blue	Red	Green	Blue
The proposed scheme	99.64	99.60	99.60	33.44	33.52	33.53
The scheme proposed in [18]	79.68	87.69	79.66	26.75	29.31	26.69

4. CONCLUSIONS

In this paper, we proposed a color image encryption scheme based on multiple chaotic systems. In this encryption algorithm, a parameter depending on the plain-image is applied to dynamically assign two generalized Arnold maps to generate chaotic sequences, so the proposed encryption scheme can well resist chosen/known plain-image attack and the chaotic sequences show good chaotic properties. In the diffusion stage, four vectors are generated by another generalized Arnold map, then the gray values of row and column pixels of 2D image matrix are mixed with the pseudo-random number sequences via bitxoring operation, which greatly weaken the correction between plain-image and cipher-image. Simulation results show that the proposed encryption scheme has good performance to resist all kinds of attacks.

ACKNOWLEDGEMENTS

This research is supported by National Natural Science Foundation of China (No. 11271238).

REFERENCES

[1] D. R. Stinson, Cryptography: Theory and Practice, CRC Press, Boca Raton, 1995.
[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998), 1259–1284.
[3] V. Patidar, N. K. Pareek, K. K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Communications in Nonlinear Science and Numerical Simulation, 14 (2009), 3056–3075.

[4] R. Ye, H. Huang, Application of the Chaotic Ergodicity of Standard Map in Image Encryption and Watermarking, I. J. Image, Graphics and Signal Processing, 1(2010), 19–29.
[5] G. J. Zhang, Q. Liu, A novel image encryption method based on total shuffling scheme, Optics Communications, 284(2011), 2775–2780.
[6] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284(2011), 5290–5298.
[7] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(2011), 3895–3903.
[8] Xiaowen Chang, Kwok-wo Wong, Hai Yu. An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion, Communications in Nonlinear Science and Numerical Simulation, 18(2013): 2066-2080.
[9] Jun-xin Chen, Zhi-liang Zhu, Chong Fu. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. Communications in Nonlinear Science and Numerical Simulation, 23(2014):294-310.
[10] R. Ye, W. Guo, An image encryption scheme based on chaotic system with changeable parameters, I. J. Computer Network and Information Security, 6:4(2014), 37-45.
[11] Xing-yuan Wang, Na Wei, Dou-dou Zhang. A novel image encryption algorithm based on chaotic system and improved Gravity Model. Optics Communications, 338(2015): 209-217.
[12] Wenying Wen, Yushu Zhang, Zhijun Fang, Jun-xin Chen. Infrared target-based selective encryption by chaotic maps. Optics Communications, 341(2015): 131-139.
[13] Xingyuan Wang, Lintao Liu, Yingqian Zhang. A novel chaoic block image encryption algorithm based on dynamic random growth technique. Optics and Lasers in Engineering, 66(2015): 10-18.
[14] Jun-xin Chen, Zhi-liang Zhu, Hai Yu. A fast chaos-based symmetric image cryptosystem with an improved diffusion scheme. Optik,125(2014): 2472-2478.
[15] A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism. Communications in Nonlinear Science and Numerical Simulation, 20(2015):846-860.
[16] Jin-xin Chen, Zhi-liang Zhu, Chong Fu, Hai Yu, Li-bo Zhang. An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering, 67(2015): 191-204.
[17] C. E. Shannon, Communication theory of secrecy systems, Bell Syst. Tech. J, 28(1949), 656-715.
[18] Xingyuan Wang, Hui-li Zhang. A color image encryption with heterogeneous bit-permutation and correlated chaos, Optics Communications, 342(2015): 51-60.

AUTHORS

Yuting Xi, master degree candidate at department of mathematics in Shantou University.

Xing Zhang, master degree candidate at department of mathematics in Shantou University.

Ruisong Ye was born in 1968 and received the B.S. degree in Computational Mathematics in 1990 from Shanghai University of Science and Technology, Shanghai, China and the Ph. D. degree in Computational Mathematics in 1995 from Shanghai University, Shanghai, China. He is a professor at Department of Mathematics in Shantou University, Shantou, Guangdong, China since 2003. His research interest includes bifurcation theory and its numerical computation, fractal geometry and its application in computer science, chaotic dynamical system and its application in computer science, specifically the applications of fractal chaotic dynamical systems in information security, such as, digital image encryption, digital image hiding, digital image watermarking, digital image sharing.