A Chaos-based Image Encryption Scheme Using Permutation-Substitution Architecture

Junqin Zhao, Weichuang Guo, Ruisong Ye
Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, P. R. China

ABSTRACT : *Recently, a great number of chaos-based image encryption algorithms have been proposed. But most of them are either deficient in security or complicated. In this paper, we propose a permutation-substitution image encryption scheme based on generalized Arnold map. Only one round of permutation and one round of substitution are performed to get the desirable results. The generalized chaotic Arnold maps are applied to generate the pseudo-random sequences for the permutation and substitution. The permutation and substitution are both performed row-by-row/column-by-column instead of pixel-by-pixel to increase the speed of encryption. The security and performance of the proposed scheme have been analyzed, including statistical analysis, key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis etc. All the experimental results suggest that the proposed image encryption scheme is efficient and highly secure.*

Keywords *-Arnold map, chaotic dynamical system, permutation-substitution architecture, image encryption*

I. INTRODUCTION

With the rapid development of network technology and multimedia processing techniques, multimedia data, including images, sounds and videos, are increasing shared over the internet or stored in hard disk in digital form. Often, multimedia data contain private or confidential information or are associated with financial interests. So the security problems have attracted researchers as well as general public's attentions. Encryption is a classical and efficient way to solve these problems. Visual data are mainly characterized by the high redundancy and high correlation among pixels. According to Shannon [1], confusion and diffusion are two basic techniques to obscure such high redundancies and strong correlation. And the easiest and effective way is to combine the two basic techniques with chaotic systems. Chaotic system possesses several perfect features, such as determinacy, high sensitivity to initial conditions and control parameters, orbit inscrutability, ergodicity, pseudo-randomness, etc. These good chaotic natures agree with the fundamental requirements like confusion and diffusion in cryptography. These properties make chaotic system a potential candidate for constructing cryptosystems [2-6].

Since Fridrich firstly proposed the fundamental permutation-diffusion mechanism of chaos-based image encryption in 1998 [2], a great number of chaos-based image encryption algorithms have been studied and designed. All the chaos-based image encryption schemes have shown their superior performance. Fridrich's proposed image encryption mechanism is usually composed of two processes: image shuffling of pixel positions by permutation process and image diffusion of pixel gray values by diffusion process. The shuffling process permutes the plain-image pixel positions governed by certain chaotic map, while the diffusion process changes the pixel gray values sequentially so that a tiny change for any one pixel can spread out to almost all pixels in the whole image. The Fridrich's mechinism has become the most popular structure adopted in many chaos-based image encryption algorithms subsequently proposed [2-12]. A good permutation process should show good shuffling effect and a good diffusion process should cause great modification over the cipher-image even if only a minor change for one pixel in the plain-image. However Wang et al. pointed out in [13] that such a kind of permutation-diffusion architecture with fixed parameters has one big drawback, that is, the two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value. Therefore, such a kind of encryption algorithms can be attacked by the following steps: (i) a homogeneous image with identical pixel gray values is adopted to eliminate the confusion effect; (ii) the key-stream of the diffusion process is obtained via known-plaintext or chosen plaintext attacks; (iii) the remaining cipher-image can be regarded as the output of a kind of permutation-

only cipher, which has been shown insecure and can be cryptanalyzed by known-plaintext or chosen plaintext attacks [14,15]. To overcome the fatal flaw existing in the image encryption schemes with permutation-diffusion architecture abovementioned. Patidar et al. [16] proposed a permutation-substitution based image encryption scheme consisting three processes: preliminary permutation, substitution and main permutation. The proposed image encryption scheme demonstrates strong robustness and great security. All the three processes are done row-by row and column-by-column instead of pixel-by-pixel to improve the speed of encryption. To yield excellent key sensitivity and plaintext sensitivity, both preliminary permutation and main permutation are designed to be dependent on the plain-image and controlled through the pseudo-random number sequences (PRNS) generated from the chaotic standard map. The substitution process is initialized with the initial vectors generated via the cipher keys and chaotic standard map, and then the pixel gray values of row and column pixels of input 2D matrix are bitxored with the PRNS generated from the standard map. Although the proposed substitution process is operated row-by row and column-by-column, which is different from conventional diffusion functions acting on the input image pixels subsequently one by one, the diffusion effect is also obtained, showing good resistance against differential analysis.

Benefited from the idea of permutation-substitution structure, we design a novel cryptosystem to avoid the drawback of the conventional Fridrich's architecture. We make two improvements over the algorithm proposed in [16]. One is the use of 2D chaotic Arnold map instead of the use of standard map. The other improvement is that our image encryption scheme is only comprised of two stages: one permutation and one substitution. The 2D generalized Arnold map shows excellent chaotic features, such as ergodicity, pseudo-randomness, and sensitivity to initial conditions and control parameters [6]. It has already been well-tested and proved to be a good pseudo-random number generator. The application of 2D generalized Arnold map will own higher computational efficiency than 2D standard map because sine function exists in the latter map. In more details, there are three multiplication operations, two division operations and two mod operations for one pseudo-random gray value between 0 and 255 in case of standard map, while there are three multiplication operations and two mod operations in case of 2D generalized Arnold map. Furthermore, there exists one sine function operation in standard map. Therefore it is more efficient to generate one pseudo-random gray value via 2D generalized Arnold map, especially for large images. In our encryption scheme, only one permutation stage and one substitution stage are applied, however, two permutation stages and one substitution stage are applied in [16]. Therefore it is obvious to see that our proposed image encryption scheme demonstrates more efficient regarding the speed of encryption. Experiments also verify such a conclusion. The security and performance analysis of the proposed image encryption are carried out using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis etc. All the experimental results show that the proposed image encryption scheme is highly secure and excellent performance, which makes it suitable for practical application.

The rest of the paper is organized as follows. In Section 2, we briefly introduce the 2D generalized Arnold map and discuss its chaotic natures. Section 3 devotes to designing the image encryption scheme. One permutation stage and one substitution stage are presented to encrypt color images. In Section 4, we present the results of security and performance analysis of the proposed image encryption scheme using the histograms, correlation coefficients, information entropy, key sensitivity analysis, differential analysis, key space analysis, encryption rate analysis etc. Section 5 draws some conclusions of the paper.

II. THE GENERALIZED ARNOLD MAP

Arnold map is also called cat map. It is a two-dimensional invertible chaotic map introduced by Arnold and Avez [17]. The classical Arnold map is described by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \qquad (1)$$

where "$x \bmod 1$" means the fractional part of a real number x by adding or subtracting an appropriate integer. Therefore (x_n, y_n) is confined in the unit square $[0,1)^2$. The map is area preserving since the determinant of its linear transformation matrix is 1. As shown in Fig.1, the unit square is first stretch by the linear transform matrix and then

folded back to the unit square by the modulo operation. The classical cat map (1) can be generalized to the following form by introducing two positive real control parameters $a>0$ and $b>0$,

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1. \qquad (2)$$

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 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 in conventional generalized Arnold maps, which enlarges the key space significantly. Fig. 2 (a) shows an orbit of $(x_0,y_0)=(0.5231,0.7412)$ with length 1500 derived 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.

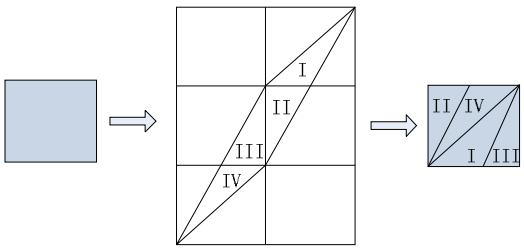
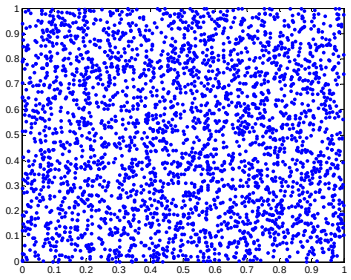
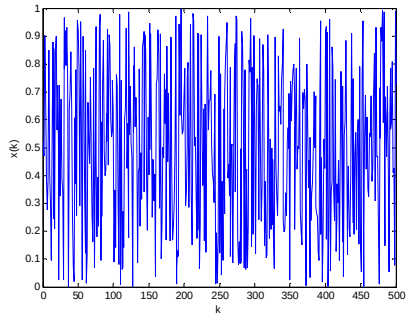


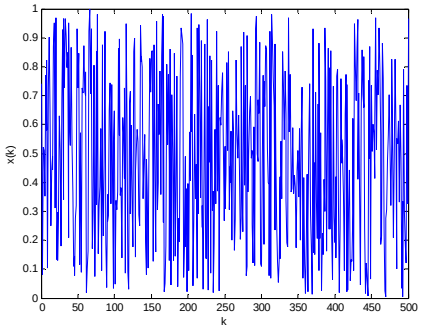
Fig.1. The Arnold map



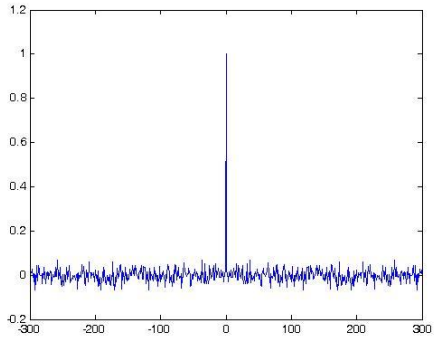
(a) The orbit of (0.5231, 0.7412)



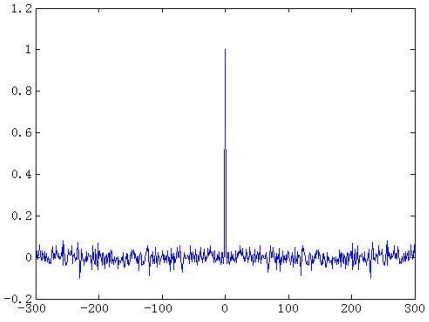
(b) Sequence $\{x_k, k=0,\cdots,1500\}$



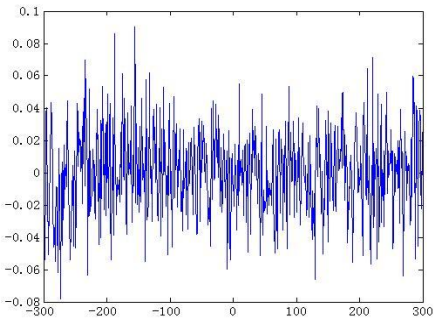
(c) Sequence $\{y_k, k=0,\cdots,1500\}$



(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.

III. THE PROPOSED IMAGE CIPHER

In this section, we discuss the details of the proposed image cipher. The proposed image encryption scheme is composed of two stages, one permutation stage and one substitution stage. The plain colour image to be encrypted is expressed as a 3D matrix defined by

$$PI(i, j, k), 1 \le i \le H,\ 1 \le j \le W,\ 1 \le k \le 3.$$

The values of the 3D matrix are integers between 0 and 255. H is the height of the color image, and W is the width of the image. The colour channels are denoted by the value $k = 1, 2, 3$ standing for the red, green and blue channel respectively. The cipher keys consist of the initial values x_0, y_0, the control parameters a, b of the generalized Arnold map and one integer number N used to eliminate the transient effect. We calculate the height NH and width NW of one new 2D matrix by

$$\begin{cases} \min\ (NW - NH), \\ s.t. \\ NH \times NW = H \times W \times 3, \\ NW \ge NH. \end{cases} \tag{3}$$

A 2D matrix with height NH and width NW calculated by (3) makes its height and width as approximately equal as possible. The best case is $NH = NW$; if it is not possible, then we get a rectangular matrix with the lowest possible difference in the number of rows and columns. The motive of such a calculation is to reduce the workload of the encryption. The whole image encryption scheme is outlined as follows.

Step 1. Two initial pseudo-random gray value vectors IVR, IVC used for the permutation are generated by the the generalized Arnold map. With the initial conditions x_0, y_0, system control parameters a, b and N given in the cipher keys, we iterate the generalized Arnold map (2) for N times and reject the first N orbit points $\{(x_k, y_k) : k = 0, 1, \cdots, N-1\}$. The values of (x_N, y_N) are stored and iterate (2) with initial values (x_N, y_N) to yield the initial pseudo-random gray value vectors IVR, IVC for row and column substitutions respectively. For the sake of convenience, we rewrite (x_N, y_N) as (x_0, y_0).

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_{i-1} \\ y_{i-1} \end{pmatrix} \bmod 1,$$
$$IVR(i) = floor(x_i * 256) + 1,$$
$$IVC(i) = floor(y_i * 256),\ i = 1, \cdots, NW. \tag{4}$$

where $floor(x)$ returns the largest integer not larger than x. Now consider only the first NH elements of IVC and reject the remainder, and then transpose IVC to get one column vector $IVC = transpose(IVC)$. We finally generate a row vector IVR having NW elements and a column vector IVC having NH elements.

Step 2. For the sake of simplicity, we still rewrite (x_{NW}, y_{NW}) as (x_0, y_0) after the generation of row vector IVR via (4). Another two pseudo-random gray value vectors SVR, SVC for the substitution are yielded by

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_{i-1} \\ y_{i-1} \end{pmatrix} \bmod 1,$$
$$SVR(i) = floor(x_i * 256), \tag{5}$$
$$SVC(i) = floor(y_i * 256),\ i = 1, \cdots, NW.$$

Step 3. The 3D matrix PI of size $H \times W \times 3$ is converted to one 2D matrix of size $NH \times NW$. Then we perform the permutation stage. Calculate the number of iterations to skip before starting the permutation by

$$N1 = P(1,1) + P(1,2) + \ldots + P(1, NW) + P(2,1) + \ldots + P(NH, NW) \quad mod\ 256.$$

Starting with the initial conditions (x_N, y_N) generated in Step 1 and the parameter a, b given in the cipher keys, one iterates the 2D generalized Arnold map for $N1$ times and then save the new values (x_{N1}, y_{N1}) as (x, y). The following loop is applied to perform the permutation. For $i = 1$ to NW, do

$$\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1,$$

$$PPR1(i) = floor(x * NH) + 1,$$

$$PPC1(i) = floor(y * NW) + 1,$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1,$$

$$PPR2(i) = floor(x * NH) + 1,$$

$$PPC2(i) = floor(y * NW) + 1.$$

The vectors $PPR1, PPC1, PPR2, PPC2$ are then used to perform the permutation of the matrix P row-by-row and column-by-column by the following loop.

For $j = 1$ to NH, exchange row $PPR1(j)$ with row $PPR2(j)$;

For $j = 1$ to NW, exchange column $PPC1(j)$ with column $PPC2(j)$.

Step 4. Substitute the 2D matrix row-by-row and column-by-column. The substitution of the elements of first row is performed by bitxoring them with the elements of row initialization vector IVR and the first element of row substitution vector, $SVR(1)$, yielded in Step 1 and Step 2 respectively. The substitution of the ith row is performed by bitxoring the ith row with the previous row and the corresponding element $SVR(i)$ of row substitution vector. After finishing the row substitution of all rows, the column substitution is similarly processed. The substitution of elements of first column is realized by bitxoring them with the elements of column initialization vector IVC and the first element of column substitution vector $SVC(1)$. The substitution of remaining columns is performed sequentially by bitxoring them with the previous column and the corresponding element of column substitution vector. The execution for the substitution is outlined as follows.

$$P(1,:) = P(1,:) \oplus IVR \oplus SVR(1);$$

$$P(i,:) = P(i,:) \oplus P(i-1,:) \oplus SVR(i),\ i = 2, \cdots, NH,$$

$$P(:,1) = (P(:,1) \oplus IVC) \oplus SVC(1);$$

$$P(:,j) = (P(:,j) \oplus P(:,j-1)) \oplus SVC(j),\ j = 2, \cdots, NW,$$

where " $\oplus$ " represents the bitwise XOR operation, and $P(i,:), P(:,j)$ denote the i th row and j th column of matrix P.

Step 5. Convert the resulted 2D matrix P back into 3D color cipher image matrix. Create one initialized 3D zero matrix CI with size $H \times W \times 3$ and then read the data of resultant 2D matrix P column-by-column and place them in the 3D matrix CI column-by-column. The 3D matrix $CI(i,j,k)\,(1 \le i \le H,\ 1 \le j \le W,\ 1 \le k \le 3)$ is thus formed and finally converted to a color image, which is the final encrypted image.

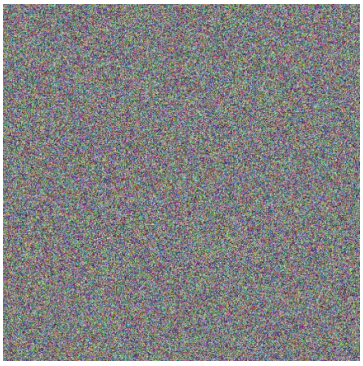
IV. SECURITY AND PERFORMANCE ANALYSIS

According to the basic principle of cryptology [18], an ideal encryption scheme requires desired sensitivity to cipher keys, i.e., the cipher-text should have strong correlation with cipher keys. An ideal encryption scheme should have also a large key space to make brute-force attack infeasible; it should also well resist various kinds of attacks like statistical analysis attack, differential attack, chosen plaintext attack and known plaintext attack, etc. In this section, the security and performance analyses have been carried out with details for the proposed image encryption scheme, including statistical anaylysis (histograms, correlation coefficients, information entropy), key sensitivity analysis, key space analysis, differential analysis, encryption rate analysis etc. Experimental results suggest that the proposed image encryption technique is highly secure and can be used for the secure image and video communication applications.

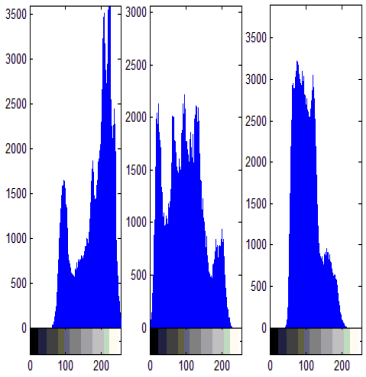
4.1. The histogram analysis

An image histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. The histogram of a cipher-image should have uniform distribution and is completely different from that of the plain-image. For a 24-bit color image, three histograms can be drawn for each 8-bit red, green and blue channel. The histograms of the color plain-image and the cipher-image are plotted in Fig. 3. The histograms of cipher-image are fairly uniform and significantly different from those of the plain-image. They imply that there is no useful statistical information in the cipher-image for an attacker to launch any statistic attacks to the cryptosystem.

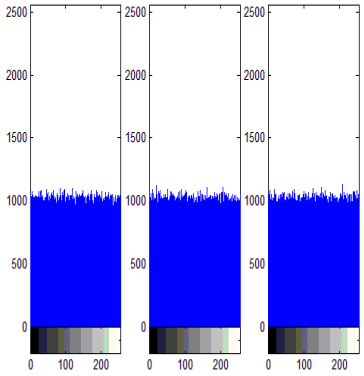
(a) Plain-image Lena



(b) cipher-image



(c) Histograms of R/G/B channel of plain-image



(d) Histograms of R/G/B channel of cipher-image

Fig. 3. Histograms of plain-image Lena and its cipher-image using the proposed encryption scheme with the secret key（0.286295319532476，0.56538639123458，22，33，108）.

4.2. Correlation coefficient analysis

It is well-known that for a meaningful image having definite visual content, the adjacent pixels' intensity values vary gradually and therefore each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. An ideal encryption technique should produce cipher-images with less correlation in the adjacent pixels. To measure and compare the horizontal, vertical and diagonal correlations of adjacent pixels in the plain and cipher images, we calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels respectively. First, we select 5000 pairs of two adjacent pixels randomly from an image and then calculate the correlation coefficient of the selected pairs using the following formulae

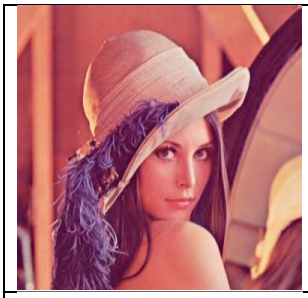
$$Cr = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}},$$

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

$$E(x) = \frac{1}{T}\sum_{i=1}^{T} x_i,\quad D(x) = \frac{1}{T}\sum_{i=1}^{T}(x_i - E(x))^2,$$

where x_i, y_i form the ith pair of horizontally, vertically or diagonally adjacent pixels and T is the total number of pairs of adjacent pixels randomly selected. The correlation coefficients of horizontally, vertically, diagonally adjacent pixels for plain-image Lena, Burn, and their corresponding cipher-images are given in Table 1. It is clear from Table 1 that the proposed image encryption technique significantly reduces the correlation between the adjacent pixels of the plain image.

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

			Correlation between adjacent pixels		
			red	green	blue
	horizontal	plain-image	0.9805	0.9694	0.9323
		cipher-image	0.0121	-0.0032	0.0052
	vertical	plain- image	0.9897	0.9834	0.9602
		cipher-image	-0.0115	-0.0126	0.0171
	diagonally	plain-image	0.9898	0.9837	0.9602
		cipher-image	9.9595e-004	-0.0012	0.0071
	horizontal	plain- image	0.9959	0.9880	0.9854
		cipher-image	0.0057	-0.0132	-0.0019
	vertical	plain- image	0.9936	0.9845	0.9851
		cipher-image	0.0219	-0.0162	-0.0136
	diagonally	plain- image	0.9941	0.9838	0.9822
		cipher-image	-0.0186	0.0371	-0.0047

We have also analyzed the correlation between plain-image and cipher-image by computing the two-dimensional correlation coefficients between various color channels of plain-image and cipher-image. The 2D-correlation coefficients are calculated by

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

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

where A represents one of the red, green and blue channel of the plain image, B represents one of the red, green and blue channel of the cipher image, $\bar{A}$ and $\bar{B}$ are the mean values of the elements of 2D matrices A and B respectively; H and W are respectively the height and width of the plain/cipher image. In this way, we have total nine different correlation coefficients (C_{RR} , C_{RG} , C_{RB} , C_{GR} , C_{GG} , C_{GB} , C_{BR} , C_{BG} and C_{BB}) for a pair of plain and cipher images. We have computed the correlation coefficients for the pair of plain-image Lena and its corresponding cipher-image. The results are shown in Table 2. One can see from the results that the correlation coefficients between various channels of the plain image and cipher image are very small (or practically zero), hence the cipher-image owns the characteristics of a random image.

Table 2. Correction between pairs of plain and cipher images

	plain-image		
Cipher image	Red	Green	Blue
	plain-Image ‘ Lena’		
Red	0.0016	0.0023	0.0030
Green	0.0042	0.0054	0.0063
Blue	-0.00016	0.00073	0.0013
	plain-Image ‘burn’		
Red	0.0025	0.0020	0.0021
Green	-0.0047	-0.0020	-0.0032
Blue	0.0022	0.0023	0.0028

4.3. Information entropy

Information entropy, the most important feature of randomness, is one of the fundamental criteria to measure the strength of a cryptosystem. Information entropy is a measure of the uncertainty associated with a random variable and can be also a measure of disorder and randomness. It quantifies the amount of information contained in data, usually in bits/symbol. Two extremely cases are: a long sequence of repeating characters and a truly random sequence. The former has entropy of 0 since every character is predictable, and the latter has maximum entropy since there is no way to

predict the next character in the sequence. Regarding image, it can be used to measure the uniformity of image histograms; it is one of the fundamental criteria to measure the strength of a cryptosystem. The entropy $H(m)$ of a message source m can be measured by

$$H(m) = -\sum_{i=0}^{L-1} p(m_i)\log(p(m_i)) \text{ (bits)},$$

where L is the total number of symbols m, $p(m_i)$ represents the probability of occurrence of symbol m_i and log denotes the base 2 logarithm so that the entropy is expressed in bits. For a random source emitting 256 symbols, its entropy is $H(m) = 8$ bits. For a 24-bit color image, the information entropy for each color channel (Red, Green and Blue) is given as

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

We have calculated the information entropy for plain- image Lena and its corresponding cipher image. The results are shown in Table 3. Comparing the results with those presented in [16], one can see that the results obtained here are better than those produced in [16]. The value of information entropy for the cipher-image produced by the proposed image encryption scheme is very-very close to the expected value of truly random image, i.e., 8bits. Hence the proposed encryption scheme is extremely robust against entropy attacks.

Table 3. Information entropy analysis

	red	green	blue
Plain-image 'lena'	7.2531	7.5952	6.9686
Cipher-image of 'lena'	7.9993	7.9992	7.9993
Cipher-image of 'lena'[16]	7.9957	7.9963	7.9951

4.4. Key sensitivity analysis

An ideal image encryption scheme should be extremely sensitive to cipher keys, which is an essential feature for any good cryptosystem in the sense that it can effectively prevent invaders decrypting original data even after they invest large amounts of time and resources. The key sensitivity of a cryptosystem can be observed in two ways: (i) the cipher-image derived from the cryptosystem should be extraordinarily sensitive to cipher keys, i.e., if we use two slightly different keys to encrypt the same plain-image, then two cipher-images should possess negligible correlation; (ii) the cipher-image cannot be decrypted correctly although there is a slight difference between the encryption and decryption keys. To evaluate the key sensitivity property, the plain-image is respectively encrypted with one master cipher key MKEY and five other cipher keys SKEY1—SKEY5 which have only a minor difference in any one of five parts of master cipher key. The following cipher keys are used to perform the simulation and the results are shown in Table 4.

MKEY: (0.286295319532476, 0.56538639123458, 22, 33, 108);
SKEY1: (0.286295319532475, 0.56538639123458, 22, 33, 108);
SKEY2: (0.286295319532476, 0.56538639123457, 22, 33, 108);

SKEY3: (0.286295319532476, 0.56538639123458, 22, 33, 109);
SKEY4: (0.286295319532476, 0.56538639123458, 22+1.0e-14, 33, 108);
SKEY5: (0.286295319532476, 0.56538639123458, 22, 33+1.0e-14, 108);

Table 4. Key sensitivity test I. (a) Key sensitivity analysis of image 'lena'

Correlation coefficients between the encrypted images obtained using MKEY and SkEY1-SKEY5					
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5
C_{RR}	0.0007	0.0023	-0.0023	0.00086	0.0015
C_{RG}	0.0036	0.0021	0.00023	-0.0036	-0.00093

C_{RB}	0.0026	-0.0018	-0.00015	0.00034	0.00095
C_{GR}	0.0026	-0.0015	-0.00089	0.00013	0.0033
C_{GG}	-0.0019	0.00027	-0.00059	-0.0023	0.0025
C_{GB}	-0.00066	-0.0040	-0.00052	-0.00042	0.00093
C_{BR}	0.0026	0.0026	-0.00036	0.0039	-0.00061
C_{BG}	0.00075	0.0014	0.0018	0.0013	0.0033
C_{BB}	0.00095	0.00043	-0.00006	0.0012	-0.0017

(b) Key sensitivity analysis of image 'burn'

Correlation coefficients between the encrypted images obtained using MKEY and SkEY1-SKEY5					
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5
C_{RR}	-0.000731	-0.0021	-0.0032	-0.00078	0.0005
C_{RG}	0.0021	-0.000287	-0.000756	-0.0028	0.00025
C_{RB}	-0.000764	0.0011	-0.0028	0.0025	0.0017
C_{GR}	0.000529	0.000572	0.0016	-0.0019	-0.0021
C_{GG}	0.0024	-0.0032	0.0027	0.0020	-0.0028
C_{GB}	0.000998	-0.0014	0.00074	0.00031	0.0019
C_{BR}	-0.0030	0.0020	-0.0037	-0.00043	-0.0030
C_{BG}	-0.000063	0.0037	0.0025	0.00076	-0.0004
C_{BB}	-0.0023	-0.0039	-0.0009	-0.00022	-0.0013

Table 5. Key sensitivity test II.

Correlation coefficients between the decrypted images of Lena obtained using MKEY and SkEY1-SKEY5					
	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5
C_{RR}	0.0026	0.00031	-0.0015	0.0023	0.0036
C_{RG}	-0.0011	0.0018	0.0011	-0.0032	-0.0014
C_{RB}	0.00093	-0.00042	0.0029	0.00085	0.0015
C_{GR}	0.00092	-0.00028	-0.0028	0.0010	0.0026
C_{GG}	-0.00076	0.0023	0.0013	-0.0019	-0.0016
C_{GB}	-0.00066	0.00029	0.00070	-0.0027	0.0026
C_{BR}	-0.00064	0.00025	-0.0029	-0.00031	0.0022
C_{BG}	-0.0012	0.0032	0.00093	-0.0011	-0.0018
C_{BB}	-0.00054	0.00033	-0.0015	-0.0048	0.0036

(i) For the first kind of key sensitivity analysis, the plain-image Lena is encrypted using MKEY and also using all five slightly different keys SKEY1--SKEY5. Then we have computed the 2D correlation coefficients between the various colour layers of the cipher-image yielded using MKEY and five other cipher-images produced using slightly different keys from SKEY1 to SKEY5. The results have been given in Table 4. All the correlation coefficients are very small or

practically zero indicating that all the cipher-images are highly different and hence the cipher-images produced by the proposed image cipher possess extreme sensitivity to cipher keys.

(ii) For the second kind of key sensitivity analysis, plain- image Lena is encrypted using MKEY, and the encrypted image is decrypted with five slightly different keys from SKEY1 to SKEY5. Now the 2D correlation coefficients between the various colour channels of plain-image and five decrypted images with slightly different keys from SKEY1 to SKEY5 are calculated. The results are given in Table 5. It is clear that all the correlation coefficients are very small or practically zero, i.e., the images decrypted using slightly different keys are highly different.

4.5. Differential attack analysis

The cryptosystem should be sensitive to a specific change in the plain-image, because some relationship between the plain-image and the cipher-image can be traced by the difference caused by a slight modification in the plain-image. The differential cryptanalysis of a block cipher is the study of how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. It is usually done by implementing the chosen plaintext attack but now there are extensions which use known plaintext as well as ciphertext attacks also. As for image cryptosystems, attackers may generally make a slight change (e.g., modify only one pixel) of the plain-image, and compare the two cipher-images (obtained by applying the same cipher key on two plain-images having one pixel difference only) to find out some meaningful relationships between the plain-image and the cipher-image. If a meaningful relationship between plain-image and cipher-image can be found in such analysis, which may further facilitate the opponents to determine the cipher key. If one minor change in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the encryption scheme will resist differential attack efficiently. To test the robustness of image cryptosystems against the differential cryptanalysis, two performance indices are usually used to test the effect of 1-bit change in the plain-image on the corresponding cipher-image. They are NPCR (number of pixel change rate) and UACI (unified average changing intensity).

NPCR is used to measure the percentage number of pixels in difference of a particular color channel in two cipher-images obtained by applying the same cipher key on two plain-images having one pixel difference only. If $C^{R/G/B}$ and $\bar{C}^{R/G/B}$ represent the *R*, *G*, *B* channels for two cipher-images, then NPCR for each color channel is defined as:

$$\mathrm{NPCR}^{R/G/B} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}^{R/G/B}}{W \times H} \times 100\%,$$

$$D_{i,j}^{R/G/B} = \begin{cases} 0\,, \; if \;\; C_{i,j}^{R/G/B} = \bar{C}_{i,j}^{R/G/B}, \\ 1, \;\; if \;\; C_{i,j}^{R/G/B} \neq \bar{C}_{i,j}^{R/G/B}. \end{cases}$$

The NPCR for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$NPCR_{Expected}^{R/G/B} = (1 - 2^{-L^{R/G/B}}) \times 100\%,$$

where $L^{R/G/B}$ is the number of bits used to represent the red, green or blue channels of the considered image. For a 24-bit true color image (8 bit for each color channel) $L^{R/G/B}=8$, hence $NPCR_{Expected}^{R/G/B} = 99.6094\%$.

UACI, the average intensity difference of a particular channel between two cipher-images $C^{R/G/B}$ and $\bar{C}^{R/G/B}$, is calculated by

$$\mathrm{UACI}^{R/G/B} = \frac{1}{W \times H} \sum_{i=1}^{H}\sum_{j=1}^{W} \frac{C_{i,j}^{R/G/B} - \bar{C}_{i,j}^{R/G/B}}{2^{L^{R/G/B}} - 1} \times 100\%.$$

The UACI for two random images, which is an expected estimate for an ideal image cryptosystem, is given by

$$\mathrm{UACI}_{Expected}^{R/G/B} = \frac{1}{2^{2L^{R/G/B}}} \cdot \frac{\sum_{i=1}^{2^{L^{R/G/B}}-1} i(i+1)}{2^{L^{R/G/B}} - 1} \times 100\%.$$

For a 24-bit true color image, $\mathrm{UACI}_{Expected}^{R/G/B} = 33.4635\%$.

We have performed the differential analysis by calculating NPCR and UACI on plain-image Lena. The analysis has been done by randomly choosing 500 pixels (one at a time, including the very first and very last pixels) in each plain-image and changing their all three color values by one unit. The average values of NPCR and UACI thus obtained for all three images are

given in Table 6. It is clear that the NPCR and UACI values are very close to the expected values, thus the proposed image encryption technique shows extreme sensitivity on the plaintext and hence not vulnerable to the differential attacks. The results by the proposed scheme [16] are also shown in Table 6 for the comparison.

Table 6. Differential analysis

	Average NPCR (%)			Average UACI (%)		
	red	green	blue	red	green	blue
Image 'Lena'	99.5958	99.6248	99.6155	33.3720	33.5120	33.4218
Image 'Lena'[16]	99.6132	99.5984	99.4001	33.4873	33.5203	33.3901

4.6. Resistance to known-plaintext and chosen-plaintext attacks

In the permutation process, we used $N1$ to iterate the chaotic Arnold map $N1$times with the initial conditions to generate chaotic sequences for permuting the plain-image. Since $N1$ depends on all the elements of 2D matrix, when different plain-image are encrypted, the corresponding chaotic sequence applied to permute the plain-images will be different, resulting in different cipher-image. Therefore the attacker cannot find useful information by encryption some special images. The proposed image scheme can thus resist the known-/chosen- plaintext attacks efficiently.

4.7. Encryption speed analysis

We have also estimated the encryption rate of the proposed image encryption scheme. The operation system, hardware and software are Windows 7 system, Intel(R) Pentium(R) G620 @2.60GHz CPU with 2 GB RAM, and MATLAB 7.11 respectively. In Table 7, we present the average value of encryption rate of the proposed encryption technique for "all-zeros" images of five different sizes (1.5, 6, 9, 12, 24, 44 and 72 Mb (Mega-bits)). Randomly generating 50 cipher keys for each image, we encrypt the image and get the average encryption time. The results show that the proposed image encryption scheme has an average encryption rate of 18.4737Mbps or so in case of encrypting one round. We have also estimated the encryption rate of the proposed scheme in [16] for a comparison using the same computing environment. The average encryption rate of 16.1025Mbps is obtained for the proposed scheme in [16]. All the results indicate that our proposed scheme is more efficient than the proposed one in [16] Anyway, at the case of large image data, our image encryption scheme shows great potential. From the point of view of key space capacity, we note that the proposed scheme here owns actually competitive advantage than that one in [16] as well.

Table 7. Comparison between the encryption rates of the proposed scheme here and one recent chaos-based permutation-substitution image encryption scheme [16]. The encryption time is measured in second and the encryption rate is measured in Mbps.

Image size	Time by the proposed scheme here (s)	Rate by the proposed scheme here (Mbps)	Time by the scheme [16]	Rate by the scheme [16]
1.5Mb	0.0751	20.0179	0.0771	19.4770
6Mb	0.3231	18.5727	0.3700	16.2171
9Mb	0.4897	18.3783	0.5671	15.8710
12Mb	0.6518	18.4118	0.7613	15.7620
24Mb	1.3014	18.4415	1.5449	15.5351
44Mb	2.4240	18.1517	2.8957	15.1953
72Mb	4.1519	17.3419	4.9114	14.6598

V. CONCLUSION

In this paper we proposed an efficient image encryption scheme based on generalized Arnold map and permutation-substitution

mechanism. The encryption process makes the resulted cipher-image dependent on the plaintext as well as the initial cipher keys, and therefore the cipher-image strongly resists known-plaintext and chosen-plaintext attacks. All the experimental results suggest that the proposed image encryption scheme is robust and secure and can be used for secure image and video communication applications.

VI. Acknowledgements

This research is partly supported by National Natural Science Foundation of China (No. 11071152 & No. 11271238).

REFERENCES

[1] C. E. Shannon, Communication theory of secrecy system. Bell Syst. Tech. J, 28(1949), 656–715.

[2] J. Fridrich, Symmetric ciphers based on two-dimensional chaotic maps, International Journal of Bifurcation and Chaos, 8(1998), 1259–1284.

[3] L. Kocarev, Chaos-based cryptography: a brief overview, IEEE Circuits and Systems Magazine, 1(2001), 6–21.

[4] F. Huang, Z.-H. Guan, A modified method of a class of recently presented cryptosystems, Chaos, Solitons and Fractals, 23(2005), 1893–1899.

[5] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(2006), 926-934.

[6] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Optics Communications, 284(2011), 5290–5298.

[7] N. K. Pareek, V. Patidar, K. K. Sud, Image encryption using chaotic logistic map, Image and Vision Computing, 24(2006), 926-934.

[8] N. Masuda, K. Aihara, Cryptosystems with discretized chaotic maps, IEEE Trans. Circuits Syst. I, 49(2002), 28–40.

[9] H. Liu, X. Wang, Color image encryption using spatial bit-level permutation and high-dimension chaotic system, Optics Communications, 284(2011), 3895–3903.

[10] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, A. Akhavan, A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps, Phys. Lett. A, 366(2007), 391–396.

[11] 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.

[12] V. Patidar, N. K. Pareek, K. K. Sud, A new substitution–diffusion based image cipher using chaotic standard and logistic maps, Commun. Nonlinear Sci. Numer. Simulat., 14 (2009), 3056–3075.

[13] Y. Wang, K.W. Wong, X. F. Liao, T. Xiang, G. R. Chen, A chaos-based image encryption algorithm with variable control parameters. Chaos, Solitons and Fractals, 41(2009), 1773–1783.

[14] S. J. Li, C. Q. Li, G. R. Chen, N. G. Bourbakis, K. T. Lo, A general quantitative cryptanalysis of permutation-only multimedia ciphers against plain-image attacks. Signal Process. Image Commun., 23(2009), 212–223.

[15] C. Q. Li, S. J. Li, G. R. Chen, G. Chen, L. Hu, Cryptanalysis of a new signal security system for multimedia data transmission. EURASIP J. Appl. Signal Process., 8(2005), 1277–1288.

[16] Vinod Patidar, N.K. Pareek, G. Purohit, K.K. Sud. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption, Optics Communications, 284(2011), 4331-4339.

[17] V. Arnold, A. Avez, Ergodic problem in classical mechanics, Benjamin, New York, 1986

[18] B. Schiener, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and sons, New York, 1996.