A Permutation-substitution Based Image Encryption Scheme with Bit-plane Exchanging Strategy

Ruisong YE[1,a], Ming YE[1], Yafang LI[1], Xiaoyun SHI[1], Wenhao YE[1]

[1]Department of Mathematics, Shantou University, Shantou, Guangdong, 515063, China

[a]rsye@stu.edu.cn

Keywords: Bit-plane; Generalized Arnold map; Permutation; Substitution; Image encryption

Abstract. A novel image encryption scheme with permutation-substitution mechanism is proposed. In the permutation process, the discrete generalized Arnold map is applied to disorder pixel positions and exchange the gray values of corresponding pixels at bit-plane pair. The continuous generalized Arnold map is utilized to generate pseudo-random sequences to realize the diffusion effect in the substitution process. One round of permutation and substitution can achieve desirable perfect security effect. The security and performance of the proposed image encryption scheme have been analyzed as well. Experimental results show that the proposed encryption scheme is secure and effective for practical application.

Introduction

With the fast development of communication network and multimedia processing technology, people use the network at all aspects of daily life for rapid and massive transmission of multimedia data, and consequently more digital images are stored, transmitted and shared over the public network. The increment of the volume of data as well as user in the public network makes the security of confidential data an urgent and significant issue. As a result, the study on information security becomes a research hotspot. As we known, traditional encryption algorithms, such as DES, AES, IDEA are typically designed for textual information data and therefore they are not suitable for practical image encryption application due to the intrinsic natures of images like high redundancy and high correlation among pixels [1]. Thanks to the good features of chaotic systems, such as ergodicity, high sensitivity to initial conditions and control parameters, pseudo-randomness etc., chaos-based image encryption schemes are extensively studied and developed in the last decades. The desirable chaotic natures are in line with the fundamental requirements such as confusion and diffusion in cryptography, and therefore chaotic systems provide a potential candidate for constructing cryptosystems [2][3][4].

Since Fridrich firstly presented the fundamental permutation-diffusion mechanism of chaos-based image encryption in 1998, a large number of chaos-based image encryption algorithms with such mechanism have been proposed [5][6][7][8]. However, Wang et al. found that the typical permutation-diffusion architecture with fixed parameters has one fatal defect. The two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value. Therefore such image encryption schemes may be broken by analyzing the diffusion process and then the permutation process respectively [9]. As a matter of fact, some image encryption algorithms with permutation-diffusion architecture have been cryptanalyzed by chosen-plaintext or known-plaintext attacks [10][11]. Therefore how to construct image encryption schemes resisting cryptanalysis attracts much attention recently, for example, see [12][13].

In this paper, we present a novel image encryption scheme with permutation-substitution mechanism instead of permutation-diffusion mechanism. Permutation-substitution mechanism has been shown to be one effective mechanism for constructing ciphers [5]. The permutation is performed between bit-planes pair. Such a kind of permutation process achieves two aspects of encryption effects because the bit-level permutation will not only disorder the pixel positions, but also change their intensity values. The 8-bit gray plain-image sized $H \times W$ is first divided into two images I_1, I_2

with the same size, each of which is of 16 gray levels. They consist of the 1-4, 5-8 bit planes respectively. The discrete generalized Arnold map is applied to confuse the pixel positions and exchange the gray values between I_1 and I_2. To achieve large key space and more security performance, one substitution process is designed using pseudo-random gray value sequences generated by a continuous generalized Arnold map with positive real number parameters. The security and performance analysis of the proposed image encryption are carried out in detail. Experimental results show that the proposed image encryption scheme is highly secure and demonstrates excellent performance.

The Proposed Image Encryption Scheme

Generalized Arnold Map. The classical Arnold map is a two-dimensional invertible chaotic map introduced by V. I. Arnold in the research of ergodic theory in 1960s [14]. The classical Arnold map is defined by

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

Map (1) is not suitable for image encryption due to its weak security. To improve the security, a map called generalized Arnold map with two positive system parameters a,b is given by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+a\times b \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1. \tag{2}$$

The generalized Arnold map (2) has one Lyapunov exponent $\sigma_1 = 1 + \frac{1+ab+\sqrt{a^2b^2+4ab}}{2} > 1$, and furthermore the Lyapunov characteristic exponent of map (2) is larger than that one of map (1) as $a>1$, $b>1$. It implies that map (2) owns stronger chaotic natures than map (1), and therefore can perform better data mixing, which makes it a better choice for designing encryption schemes than the classical Arnold map (1). We refer to [3] for more details about the generalized arnold map. Assume that the gray plain-image is modeled by a 2D matrix I with size $H\times W$ and 256 gray levels. For the sake of application of generalized Arnold map, we deal with the case $H=W$. We will apply the generalized Arnold map in both the permutation process with the discrete version (3) and the substitution process with the continuous version (2). The discrete version of generalized Arnold map is defined by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+p\times q \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod H, \tag{3}$$

where the parameters $p,q \in \{1,\cdots,H-1\}$ are integers and $(x_n, y_n), (x_{n+1}, y_{n+1})$ are the pixel positions.

Permutation Process. The detail permutation process is depicted as follows.

Step 1. The plain-image I is split into two parts: one consisting of the lower four bit planes and the other consisting of the high four bit planes. We denote them by I_1, I_2, which are both 16 gray-level image comprising of the 1-4 and 5-8 bit planes of plain-image I respectively.

Step 2. Exchange the gray values of pixel pairs between I_1 and I_2. The generalized Arnold map is applied to confuse the pixel positions in its discrete version. The exchange positions and gray value exchange operation are defined by

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+p\times q \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \bmod H, \quad I_1(i,j) \leftrightarrow I_2(s,t) \quad i,j = 0,1,\cdots,H-1.$$

Step 3. Integrate the exchanged images together to be one permuted image B by

$$B(i,j) = I_1(i,j) + I_2(i,j)\times 16, \ i,j = 0,1,\cdots,H-1.$$

Substitution Process. The substitution process is outlined as follows.

Step 1. Generation of pseudo-random gray value vectors IVR, IVC. With initial conditions x_0, y_0, control parameters a,b and one positive integer N, we iterate the generalized Arnold map (2) for N

times and reject the transient points $\{(x_k, y_k): k = 0,1,\cdots, N-1\}$. The values of (x_N, y_N) are set to be the new initial values (x_N, y_N) to yield IVR, IVC. We still write (x_N, y_N) as (x_0, y_0).

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+a\times b \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 1,$$

$$IVR(i) = floor(x_{i+1} \times 256), IVC(i) = floor(y_{i+1} \times 256),\ i = 0,\cdots, H-1,$$

where $floor(x)$ returns the largest integer not larger than x. Transpose IVC to get one column vector IVC with H elements.

Step 2. Generation of pseudo-random gray value vectors SVR, SVC. We still denote (x_H, y_H) as (x_0, y_0) for simplicity. Another two pseudo-random gray value vectors SVR, SVC are generated by

$$\begin{pmatrix} x_{i+1} \\ y_{i+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+a\times b \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \bmod 1,$$

$$SVR(i) = floor(x_{i+1} \times 256), SVC(i) = floor(y_{i+1} \times 256),\ i = 0,\cdots, H-1.$$

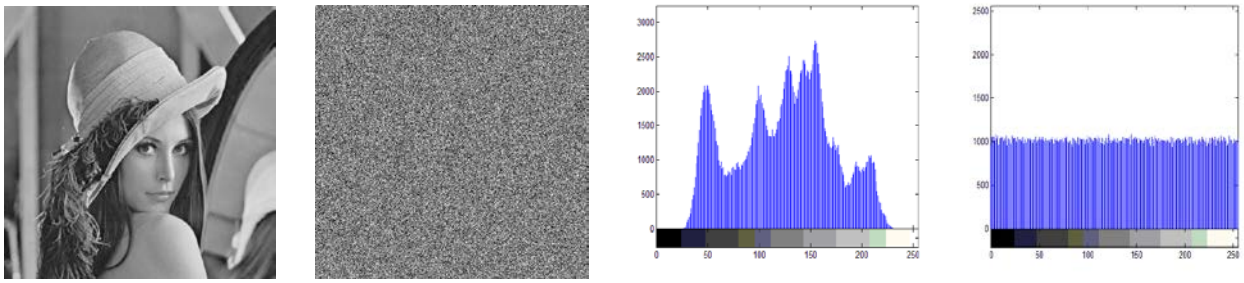
Step 3. Substitute the 2D matrix B row-by-row and column-by-column. The execution for the substitution is defined by

$$B(1,:) = B(1,:) \oplus IVR \oplus SVR(1);\ \ B(i,:) = B(i,:) \oplus B(i-1,:) \oplus SVR(i),\ i = 2,\cdots, H,$$

$$B(:,1) = B(:,1) \oplus IVC \oplus SVC(1);\ \ B(:, j) = B(:, j) \oplus B(:, j-1) \oplus SVC(j), j = 2,\cdots, H,$$

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

Encrypt the plain-image Lena one round with cipher key $p = 67, q = 146$, $x_0 = 0.1971, y_0 = 0.4356$, $a = 22.73, b = 17$ and $N = 33$, the resulted cipher-image for plain-image Lena is shown in Fig. 1(b).



(a) (b) (c) (d)

Fig. 1. The encrypted results: (a) plain-image Lena, (b) cipher-image, (c) histogram of Lena, (d) histogram of cipher-image.

Performance Analysis

The basic principle of cryptology requires that an ideal encryption scheme has strong sensitivity to cipher keys. The cipher-text should have strong correlation with cipher keys. An ideal encryption scheme should also have a large key space to make brute-force attack infeasible as well resist various kinds of attacks like statistical analysis attack, differential attack, etc. In this section, the security and performance analyses have been carried out thoroughly for the proposed image encryption scheme, including statistical analysis (histograms, correlation coefficients and information entropy), key sensitivity analysis, differential analysis, etc.

Histogram Analysis. Histogram analysis visually demonstrates pixel intensity distribution. An image histogram is a graph showing the number of pixels at each different intensity value existing in the image. The histograms of plain-image Lena and its corresponding cipher-image are shown in Figure 1(c)-(d). One can observe that the histogram of the cipher-image is fairly uniform and significantly different from the histogram of plain-image. Therefore the proposed image encryption scheme does not provide any useful information for the opponents to perform any effective statistical analysis on the cipher-image.

Correlation Coefficient Analysis. The adjacent pixels' gray values for one meaningful and nature image vary gradually, implying that each pixel is highly correlated with its adjacent pixels. An

ideal cryptosystem should produce cipher-images with less correlation in the adjacent pixels. We calculate the correlation coefficients for all the pairs of horizontally, vertically and diagonally adjacent pixels in plain and cipher image respectively. Randomly choose T=6000 pairs of horizontally, vertically and diagonally adjacent pixels and calculate the correlation coefficients. The correlation coefficient of the chosen pairs is calculated by

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

where x_i, y_i form the ith pair of horizontally, vertically or diagonally adjacent pixels. The correlation coefficients of horizontally, vertically, diagonally adjacent pixels for plain-images Lena and its corresponding cipher-images are shown in Table 1. The results demonstrate that the proposed image encryption technique significantly reduces the correlation between the adjacent pixels of the plain image.

Information Entropy Analysis. Information entropy tests the uncertainty of a random variable and can also measure disorderness and randomness for a set of information. It can be applied to measure the uniformity of image histograms as well. The entropy $H(m)$ of a gray image I can be measured by

$$H(I) = -\sum_{i=0}^{L-1} p(r_i)\log_2(p(r_i))\ \text{(bits)},$$

where L is the number of gray levels of image, $p(r_i)$ stands for the probability of occurrence of gray r_i. For a random gray image with 256 gray scale levels, its entropy is $H(I) = 8$ bits. We have calculated the information entropy values for plain-image Lena and its cipher-image. The results are 7.4474 and 7.9993 respectively. The value of information entropy for the cipher-image is very close to the expected value 8 of truly random image. Hence the proposed encryption scheme is extremely robust against entropy attacks.

Tab. 1. Correlation coefficients between adjacent pixels.

Test image	direction	Plain-image	Cipher-image
Lena	Horizontal	0.9729	0.0069
	Vertical	0.9875	-0.0072
	Diagonal	0.9630	0.0147

Differential Attack Analysis. Differential attack analysis mainly studies how differences in a plaintext influences the resultant differences in the ciphertext with the same cipher key. As for image cryptosystems, attackers usually modify only one pixel with one bit difference of the plain-image, and compare two cipher-images using the same cipher keys to obtain some meaningful relationships between the plain-image and the cipher-image. If the attackers own some meaningful relationships between plain-image and cipher-image, they may further find out the cipher key or equivalent key streams. The encryption scheme will resist differential analysis attack efficiently if a slight difference in the plain-image can cause significant, random and unpredictable changes in the cipher-image. Two most common measures NPCR (number of pixel change rate) and UACI (unified average changing intensity) are calculated to test the robustness of image cryptosystems against the differential cryptanalysis. For a L-bit gray image with size $H \times W$, if C and $\bar{C}$ represent two cipher-images, then NPCR and UACI are defined by

$$\text{NPCR} = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W} D_{i,j}}{W \times H} \times 100\%, D_{i,j} = \begin{cases} 0, & \text{if } C_{i,j} = \bar{C}_{i,j}, \\ 1, & \text{if } C_{i,j} \neq \bar{C}_{i,j}. \end{cases} \quad \text{UACI} = \frac{1}{W \times H}\sum_{i=1}^{H}\sum_{j=1}^{W}\frac{|C_{i,j} - \bar{C}_{i,j}|}{2^L - 1} \times 100\%.$$

We randomly choose ten pixels and calculate the NPCR and UACI values showing in Table 2. We also choose 100 pixels in plain-image randomly, and changing their intensity value by one unit at each selective pixel every time and calculate the NPCR and UACI values. The averages of 100 NPCR values and 100 UACI values are 99.6148 and 33.4796. They are very close to the expected values 99.6094 and 33.4635, implying that proposed image encryption technique shows good sensitivity to plaintext and hence invulnerable to differential attacks.

Tab. 2. Difference analysis of plain-image Lena

Positions	(70,419)	(339,320)	(165,310)	(87,375)	(60,347)
NPCR	99.6216	99.6006	99.6006	99.6208	99.6216
UACI	33.4785	33.4805	33.4726	33.4657	33.4670
Positions	(16,266)	(189,221)	(360,462)	69,468)	(443,115)
NPCR	99.6063	99.6040	99.6048	99.6113	99.6128
UACI	33.4617	33.4365	33.4359	33.4384	33.4403

Key Sensitivity Analysis. An essential feature for any good cryptosystem is that it should be extremely sensitive to cipher keys in the sense that it can effectively prevent invaders decrypting original data. If one uses two slightly different cipher keys to encrypt the same plain-image, then two cipher-images should possess negligible correlation. The plain-image is respectively encrypted with one master cipher key and seven other cipher keys which have only a minor difference in any one of seven parts of master cipher key. Eight cipher keys are used to encrypt image Lena. Master cipher key $(p, q, x_0, y_0, a, b, N)$ is $\mathrm{MKEY}(67,146,0.1971,0.4356,22.73,17.0,33)$. Seven slightly different keys are

$\mathrm{SKEY1}(67+1,146,0.1971,0.4356,22.73,17.0,33)$, $\mathrm{SKEY2}(67,146+1,0.1971,0.4356,22.73,17.0,33)$,

$\mathrm{SKEY3}(67,146,0.1971-10^{-14},0.4356,22.73,17.0,33)$, $\mathrm{SKEY4}(67,146,0.1971,0.4356-10^{-14},22.73,17.0,33)$,

$\mathrm{SKEY5}(67,146,0.1971,0.4356,22.73-10^{-14},17.0,33)$, $\mathrm{SKEY6}(67,146,0.1971,0.4356,22.73,17.0-10^{-14},33)$,

$\mathrm{SKEY7}(67,146,0.1971,0.4356,22.73,17.0,33+1)$,

then calculate the correlation coefficients of the cipher-image by MKEY and seven other cipher-images by SKEY1,…,SKEY7 respectively. The results are provided in Table 3. All the correlation coefficients are very small or practically zero indicating that all the cipher-images are highly different.

Tab.3. Key sensitivity tests

	SKEY1	SKEY2	SKEY3	SKEY4	SKEY5	SKEY6	SKEY7
MKEY	-2.15×10^{-4}	2.89×10^{-4}	8.25×10^{-5}	4.10×10^{-3}	-4.59×10^{-4}	-0.0027	0.0027

Conclusion

A novel image encryption scheme based on exchanging strategy permutation between higher 4 bit-planes part and lower 4 bit-planes part and substitution using generalized Arnold map is proposed in the paper. The permutation process can not only disorder the plain-image pixel positions, but also change pixel gray values efficiently. An effective substitution process is also designed to alter the gray values of the whole image pixels. Security analysis including statistical attack analysis, differential attack analysis, key sensitivity analysis are performed in details. Experimental results demonstrate that the proposed encryption scheme is secure thanks to its strong sensitivity to the cipher keys and robustness against statistical analysis and differential analysis. All these satisfactory properties make the proposed scheme a potential candidate for encryption of multimedia data such as images, audios and even videos.

Acknowledgement

This research is supported by Science and Technology Innovation-cultivation Fund of Guangdong Undergraduates, Innovation and Entrepreneurship Training Program of Guangdong Colleges and SRP of Science College of Shantou University.

References

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

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

[3] R. Ye, A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism, Opt. Commun., 284(2011), 5290-5298.

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

[5] 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, Opt. Commun., 284(2011), 4331-4339.

[6] R.Ye, A novel image encryption scheme based on generalized multi-sawtooth maps, Fundamenta Informaticae, 133(2014), 87-104.

[7] Ruisong Ye, Huiqing Huang, Xiangbo Tan, A Novel Image Encryption Scheme Based on Multi-orbit Hybrid of Discrete Dynamical System, L.J. Modem Education and Computer Science, 6:10(2014), 29-39

[8] Junming Ma and Ruisong Ye, An Image Encryption Scheme Based on hybrid orbit of hyper-chaotic system, I.J.Computer Network and Information Security, 7:5(2015), 25-33.

[9] 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.

[10] 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.

[11] X. Wang, G. He, Cryptanalysis on a novel image encryption method based on total shuffling scheme. Opt. Commun., 284(2011), 5804-5807.

[12] J. Chen, Z. Zhu, C. Fu, H. Yu, L. Zhang, An efficient image encryption scheme using gray code based permutation approach, Optics and Lasers in Engineering, 67 (2015), 191-204.

[13] Y. Zhang, X. Wang, A new image encryption algorithm based on non-adjacent coupled map lattices, Applied Soft Computing, 26 (2015),10-20.

[14] V. Arnold, A. Avez, Ergodic Problems in Classical Mechanics, Benjamin, New York, 1968.