An Image Encryption Scheme Based on Permutation-subsitution Architecture at Half Pixel Level

Ruisong Ye[1, a], Junqin Zhao[2]

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

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

[a]email: rsye@stu.edu.cn

Keywords: Arnold map; Chaos; Permutation; Substitution; Image Encryption

Abstract. An image encryption scheme using permutation-substitution mechanism at half pixel level is proposed. One round of permutation and one round of substitution achieve desirable results. In the permutation process, the image sized $H \times W$ is expanded to one sized $H \times 2W$. The generalized Arnold map is applied to generate the pseudo-random sequences for the permutation and substitution processes implemented row-by-row/column-by-column instead of pixel-by-pixel to increase the encryption rate. The security and performance of the proposed scheme have been analyzed as well.

Introduction

With the dramatic development of communication technologies and multimedia processing techniques, digital image application and exchange over Internet and wireless networks have become much more prevalent than before. Usually, some digital image information contains private or confidential information and some is associated with financial interests, and consequently the security problems have attracted researchers as well as general public's attentions. Cryptographic approaches are therefore critical for secure image transmission and storage over public networks. It is well-known that traditional encryption algorithms, such as DES, AES, are typically presented for textual information. It has been found that traditional encryption algorithms are not suitable for image encryption due to the intrinsic natures of images like high redundancy and high correlation among pixels [1]. Shannon pointed that confusion and diffusion are two basic techniques to obscure such high redundancy and correlation [2]. 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, ergodicity, pseudo-randomness, orbit inscrutability, etc. These good chaotic natures agree with the fundamental requirements such as confusion and diffusion in cryptography, and therefore chaotic systems provide a potential candidate for constructing cryptosystems [3-7].

Fridrich firstly presented the fundamental permutation-diffusion architecture of chaos-based image encryption in 1998 [3]. Since then, a great number of chaos-based image encryption algorithms have been studied and designed, and the Fridrich's architecture forms the basis of numerous chaos-based image encryption algorithms subsequently proposed. However Wang et al. pointed out that the typical permutation-diffusion architecture with fixed parameters has one fatal flaw, that is, the two processes will become independent if the plain-image is a homogeneous one with identical pixel gray value [8]. Therefore, such a kind of image encryption algorithms have been shown insecure and can be cryptanalyzed by chosen-plaintext or known-plaintext attacks [9].

In this paper, we propose an image encryption scheme based on generalized Arnold map with permutation-substitution mechanism. Permutation-substitution mechanism has been shown to be one effective mechanism for constructing ciphers [7]. The image encryption scheme proposed here consists of two stages: one permutation and one substitution, and they are performed at half pixel level different from pixel level and bit level. The image sized $H \times W$ is expanded to one sized $H \times 2W$ by dividing the plain-image into two parts: one consisting of the higher 4 bits and one consisting of the lower 4 bits. To achieve desirable key sensitivity and plaintext sensitivity, the

permutation is designed to be dependent on the plain-image. As a result, the proposed image scheme owns good resistance to known-plaintext and chosen-plaintext attacks. The proposed substitution process is performed row by row and column by column and good diffusion effect is also achieved, showing good resistance against differential analysis. The security and performance analysis of the proposed image encryption are carried out using the histograms, correlation coefficients, information entropy, differential analysis, etc. All the experimental results show that the proposed image encryption scheme is highly secure and owns excellent performance.

The Proposed Image Encryption Scheme

Read a 256 gray-scale level plain-image PI with size $H \times W$, then expand it to a new image P with size $H \times 2W$ and 16 gray-scale level. The plain-image is divided into 2 parts, the higher 4 bits are treated as one part and the lower 4 bits are integrated into the second part shown in Fig. 1.

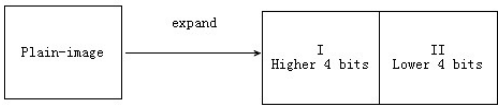


Fig.1. The expansion of plain-image

The proposed image encryption scheme is composed of one permutation stage and one substitution stage. The whole image encryption scheme is outlined as follows.

Step 1. Generation of two 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 for N times and reject the first N points $\{(x_k, y_k) : k = 0,1,\cdots,N-1\}$ to avoid harmful effect. The values of (x_N, y_N) are stored and iterate generalized Arnold map with initial values (x_N, y_N) to yield IVR, IVC. We still write (x_N, y_N) as (x_0, y_0). Let $T = \max(H, 2W)$ and execute

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_{i-1} \\ y_{i-1} \end{pmatrix} \bmod 1,\ IVR(i) = floor(x_i * 16) + 1, IVC(i) = floor(y_i * 16),\ i = 1,\cdots,T, \quad (1)$$

where $floor(x)$ returns the largest integer not larger than x. Truncate the first H elements of IVC and transpose it to get one column vector IVC with H elements. Truncate the first $2W$ elements of IVR to get one row vector IVR with $2W$ elements.

Step 2. For simplicity, we still denote (x_T, y_T) as (x_0, y_0) via (1). Another two pseudo-random gray value vectors SVR, SVC to do the substitution are generated by

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x_{i-1} \\ y_{i-1} \end{pmatrix} \bmod 1,\ SVR(i) = floor(x_i * 16), SVC(i) = floor(y_i * 16),\ i = 1,\cdots,T. \quad (2)$$

Step 3. Perform the permutation stage. Calculate the number of iterations to skip before starting the permutation by $N_1 = P(1,1) + \ldots + P(1,NW) + P(2,1) + \ldots + P(NH,NW)\ mod\ 256$. Starting with the initial conditions (x_N, y_N) generated in Step 1, we iterate the generalized Arnold map for N_1 times and then save the new values (x_{N_1}, y_{N_1}) as (x, y). For $i = 1$ to T, do the loop

$$\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1, PPR1(i) = floor(x * H) + 1, PPC1(i) = floor(y * 2W) + 1,$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \leftarrow \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod 1, PPR2(i) = floor(x * H) + 1, PPC2(i) = floor(y * 2W) + 1.$$

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 and get one permuted image $P1$.

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

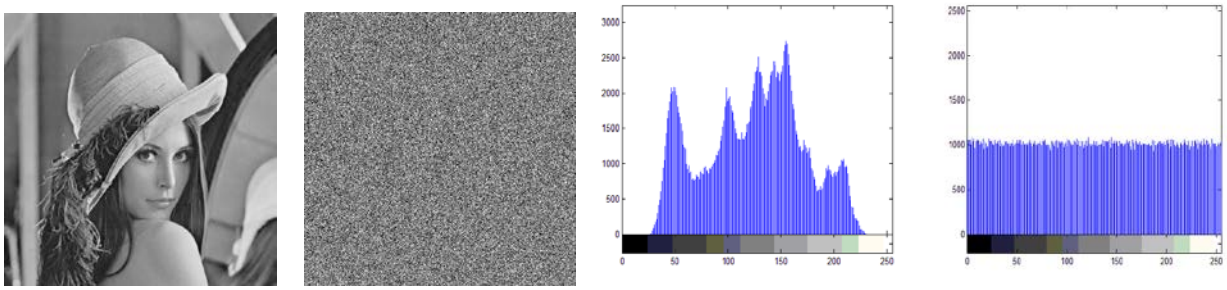
For $j = 1$ to $2W$, exchange column $PPC1(j)$ with column $PPC2(j)$.

Step 4. Substitute the 2D matrix $P1$ row-by-row and column-by-column. The execution for the substitution is outlined as follows.

$$P1(1,:) = P1(1,:) \oplus IVR \oplus SVR(1); P1(i,:) = P1(i,:) \oplus P1(i-1,:) \oplus SVR(i),\ i = 2,\cdots,H,$$

$$P1(:,1) = (P1(:,1) \oplus IVC) \oplus SVC(1); P1(:,j) = (P1(:,j) \oplus P1(:,j-1)) \oplus SVC(j), j = 2,\cdots,2W,$$

where "$\oplus$" represents the bitwise XOR operation, and $P1(i,:), P1(:,j)$ denote the ith row and jth column of matrix $P1$. The resulted cipher-image for plain-image Lena is show in Fig. 2(b).



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

Fig. 2. The encrypted results: (a) plain-image Lena, (b) cipher-image, (c) histogram of Lena, (d) histogram of cipher-image.

Security Analysis

(i) Correlation coefficient analysis. The adjacent pixels' gray values for one meaningful and nature image vary gradually, and thus each pixel is highly correlated with its adjacent pixels in horizontal, vertical or diagonal direction. An ideal cipher 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. The correlation coefficient of the pairs is calculated by the following formulae ($T = H*W$)

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

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 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.

Test image	direction	Plain-image	Cipher-image
Lena	horizontal	0.9857	-0.0028
	vertical	0.9725	-0.0027
	diagonal	0.9571	-0.000074

(ii) Information entropy analysis. Information entropy is a measure of the uncertainty associated with a random variable and can be also a measure of disorder and randomness. Regarding image, it can be used to measure the uniformity of image histograms. The entropy $H(m)$ of a message source m can be measured by $H(m) = -\sum_{i=0}^{L-1} p(m_i)\log_2(p(m_i))$ (bits), where L is the total number of symbols m, $p(m_i)$ represents the probability of occurrence of symbol m_i. For a random gray image with 256 gray scale levels, its entropy is $H(m) = 8$ bits. We have calculated the information entropy for plain-image Lena and its corresponding cipher-image. The results are 7.4451 and 7.9994 respectively. The value of information entropy for the cipher-image is very close to the expected value 8 of truly random image. Therefore the proposed encryption scheme is extremely robust against entropy attacks.

(iii) Differential attack analysis. 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. If one minor change in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the image encryption scheme will resist differential attack efficiently. To test the robustness of image cryptosystems against the differential cryptanalysis, two performance indices, NPCR (number of pixel change rate) and UACI (unified average changing intensity), are usually used to test the effect of 1-bit change in the plain-image on the corresponding cipher-image. 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

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

We randomly choose ten pixels and calculate the NPCR and UACI. The result is shown in Table 2.

Table 2. Difference analysis of plain-image Lena with size 512×512.

positions	(348,165)	(403,181)	(255,455)	(375,36)	(206,313)
NPCR(%)	99.3942	99.3908	99.3729	99.3946	99.3927
UACI(%)	33.3531	33.3403	33.3366	33.3528	33.3519
positions	(59,80)	(27,468)	(506,470)	(420,302)	(224,173)
NPCR(%)	99.3881	99.3954	99.3786	99.4053	99.3824
UACI(%)	33.3477	33.3402	33.3377	33.3526	33.3407

Acknowledgement

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

References

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

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

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

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

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

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

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

[8]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.

[9]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.