An Image Encryption Scheme Using Bit-planes Pair Exchange Permutation and Diffusion

Ruisong YE[1,a], Li LIU[1], Ming YE[1], Xiaoyun SHI[1], Wenhao YE[1]

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

[a]rsye@stu.edu.cn

Keywords: Generalized Arnold map; Permutation; Diffusion; Bit plane; Image encryption

Abstract. An image encryption scheme using permutation-diffusion mechanism is proposed. The permutation is performed by exchanging the gray values at different bit-planes pair. The diffusion is executed over the shuffled image after permutation. One round of permutation and one round of diffusion achieve perfect security effect. In the permutation process, the generalized Arnold map is applied to disorder pixel positions and exchange the gray values of corresponding pixels at bit-planes pair. Multimodal skew tent map is utilized to generate pseudo-random gray value sequence applied at the diffusion process. The security and performance of the proposed scheme have been analyzed as well.

Introduction

Since Fridrich firstly put forward the fundamental permutation-diffusion mechanism of chaos-based image encryption in 1998, a great number of chaos-based image encryption algorithms with such mechanism have been proposed [1-6]. Chaos-based image encryption algorithms show perfect performance thanks to the fantastic natures of chaotic systems, like high sensitivity to initial conditions and control parameters, ergodicity, pseudo-randomness etc. As a matter of fact, the good chaotic natures agree with the fundamental requirements such as confusion and diffusion in cryptography, and therefore chaotic systems are potential candidates for constructing cryptosystems. However, Wang et al. found 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 [7]. Some image encryption algorithms with permutation-diffusion architecture have been cryptanalyzed by chosen-plaintext or known-plaintext attacks [8, 9]. Therefore how to construct image encryption schemes resisting cryptanalysis attracts much attention recently, for example, see [10, 11].

In this paper, we present a novel image encryption scheme with permutation-diffusion mechanism. The image encryption scheme proposed here is plain-image content dependent, which can resist cryptanalysis efficiently. The permutation is performed between bit-planes pairs. The bit-level permutation will not only disorder the pixel positions, but also change their intensity values. Therefore, such a kind of permutation process achieves two aspects of encryption effects. The plain-image with size $H \times W$ and 256 gray levels is divided into 4 images I_1, I_2, I_3, I_4 with the same size, each of which is of 4 gray levels. They consist of the 1-2, 3-4, 5-6, 7-8 bit planes respectively. The chaotic generalized Arnold map is applied to confuse the pixel positions and exchange the gray values between I_1 and I_4 as well as between I_2 and I_3. To achieve desirable plain-image sensitivity, the system parameters in generalized Arnold map are related to the content of plain-image. As a result, the proposed image scheme owns good resistance to known-plaintext and chosen-plaintext attacks. To achieve large key space and more security performance, one diffusion function is designed using one pseudo-random gray value stream generated by a multimodal skew tent map. Multimodal skew tent map shows perfect chaotic natures. Therefore the diffusion process provides good diffusion effect and shows good resistance against differential analysis as well. The security and performance analysis of the proposed image encryption are carried out thoroughly. All the experimental results

show that the proposed image encryption scheme is highly secure and demonstrates excellent performance.

The Proposed Image Encryption Scheme

Generalized Arnold Map and Multimodal Skew Tent Map. Classical Arnold map is also called cat map. It is a two-dimensional invertible chaotic map introduced by V. I. Arnold in the research of ergodic theory in 1960s. The classical Arnold map is described by

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

Map (1) is not suitable for image encryption because its security just relies on the initial condition values. To improve the security, a map called generalized Arnold map with two positive system parameters a, b is given by

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

The generalized Arnold map (2) has one Lyapunov exponent $\sigma_1 = 1 + \frac{1+ab+\sqrt{a^2b^2+4ab}}{2} > 1$. One can also conclude that 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) is stronger chaotic, and therefore can perform better data mixing, which makes it a better choice for designing encryption schemes than the classical Arnold map (1) . We will apply the generalized Arnold map in the permutation process.

The unimodal skew tent map $T_0 : [0,1] \to [0,1]$ is defined by

$$T_0(x) = \begin{cases} x/a, & \text{if } x \in [0,a], \\ (1-x)/(1-a), & \text{if } x \in (a,1], \end{cases} \tag{3}$$

where $x \in [0,1]$ is the state of the system, and $a \in (0,1)$ is the control parameter. It is a noninvertible transformation of the unit interval onto itself. For any $a \in (0,1)$, dynamical system (3) has positive Lyapunov exponent $-a\ln a - (1-a)\ln(1-a)$, implying that the map is chaotic. In this paper, we extend the unimodal skew tent map (3) to multimodal skew tent map $T : [0,1] \to [0,1]$ by the following way.

$$T(x) = \begin{cases} (x-a_{2i})/(a_{2i+1}-a_{2i}), & \text{if } x \in [a_{2i}, a_{2i+1}], \\ (a_{2i+2}-x)/(a_{2i+2}-a_{2i+1}), & \text{if } x \in (a_{2i+1}, a_{2i+2}], \end{cases} \tag{4}$$

where $i = 0, \cdots, N-1$, $0 = a_0 < a_1 < \cdots < a_{2N-1} < a_{2N} = 1$. See Figure 1 for the case of $N = 3$.

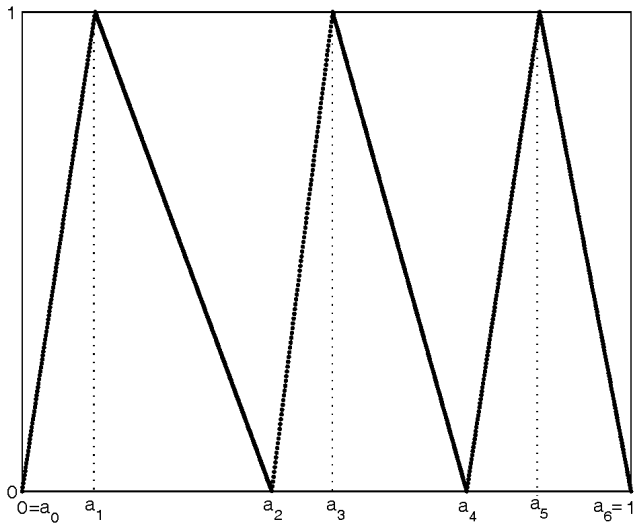


Fig. 1. The diagram of a multimodal skew tent map.

The Lyapuonov exponent of map (4) is $-p_1 \ln p_1 - p_2 \ln p_2 - \cdots - p_{2N-1} \ln p_{2N-1} - p_{2N} \ln p_{2N}$ where $p_i = a_i - a_{i-1}, i = 1, \cdots, 2N$. It is usually larger than that one of map (3). Regarding the unimodal skew tent map (3), the largest Lyapunov exponent $\ln 2 = 0.6931$ occurs at the extreme case $a = 0.5$. As for map (4), for example, let $N = 3$, $a = [0, 0.16, 0.3, \ 0.51, 0.68, 0.78, 1.0]$, then one can get $\lambda = 1.7608$. Therefore the multimodal skew tent map (4) provides stronger chaotic natures and is better for designing encryption schemes. We will use map (4) to generate pseudo-random gray value sequence in the diffusion process. The control parameter $a_1, \cdots, a_{2N-1}$ and the initial condition x_0 can be regarded as cipher keys. In this paper, we set $x_0 = 0.367$, $a = [0, 0.16, 0.3, \ 0.51, 0.68, 0.78, 1.0]$.

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

Step 1. The system parameters p, q in generalized Arnold map are yielded depending on the content of plain-image. They are calculated by

$$p = \mathrm{mod}(\sum_{i=1}^{H}\sum_{j=1}^{W}(I_1(i,j) + I_4(i,j)), H) \ , \quad q = \mathrm{mod}(\sum_{i=1}^{H}\sum_{j=1}^{W}(I_1(i,j) + I_3(i,j)), H) \ ,$$

where I_1, I_2, I_3, I_4 are the 4 gray-level image comprising of the 1-2, 3-4, 5-6, 7-8 bit planes of plain-image I respectively. In this paper, we restrict the plain-images with equal height H and width W, that is, $H = W$. A minor change in the plain-image will cause the change of p, q. It is known that generalized Arnold map is strongly sensitive to system parameters p, q. Therefore the corresponding cipher-images of two plain-images with minor difference will be dramatically different.

Step 2. Exchange the gray values of pixel pairs between I_1 and I_4 as well as between I_2 and I_3. The generalized Arnold map is applied to confuse the pixel positions. The exchange positions and gray value exchange operation are defined by

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & 1+pq \end{pmatrix} \begin{pmatrix} i \\ j \end{pmatrix} \bmod H, \quad I_1(i,j) \leftrightarrow I_4(s,t), \ I_2(i,j) \leftrightarrow I_3(s,t), \ i, j = 0, 1, \cdots, H-1 .$$

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

$$B(i,j) = I_1(i,j) + I_2(i,j) \times 4 + I_3(i,j) \times 16 + I_4(i,j) \times 64, \ i, j = 0, 1, \cdots, H-1.$$

Diffusion Process. The diffusion process is outlined as follows.

Step 1. Set the values of the control parameters $a_i, i = 1, \cdots, 5$, and the initial condition value x_0. Convert the permuted image B to be a vector denoted as v with length $H \times W$.

Step 2. Iterate map (4) to get the truncated orbit of x_0. To avoid the transient effect, we discard the first 100 points of the orbit and save the next $H \times W$ points. For simplicity, we still write the saved points as $\{x_k, k = 1, \cdots, H \times W\}$.

Step 3. The key stream element $k(n)$ is calculated by (5), in which $floor(x)$ means the nearest integers less than or equal to x, $mod(x, y)$ or $x \ mod \ y$ returns the remainder after x divided by y, $x(n)$ represents the current state of chaotic map (4) calculated in Step 2, and L is the gray level of the plain-image.

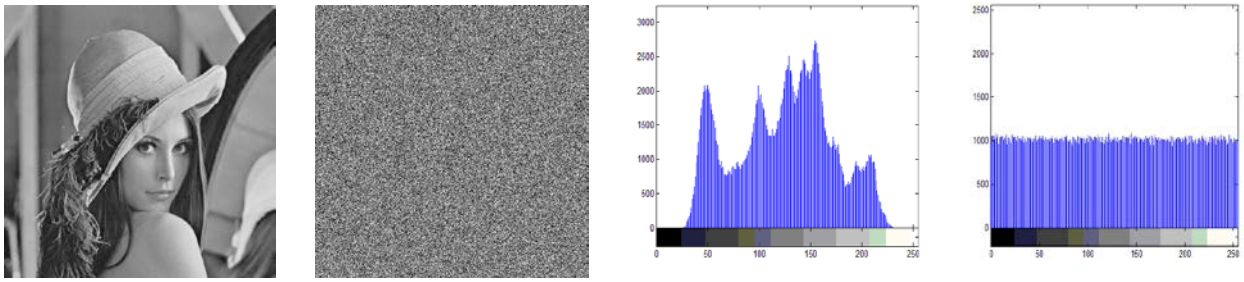
$$k(n) = mod(\ floor(x(n) \times 10^{14}), L) . \tag{5}$$

Step 4. Pixel values are modified sequentially according to (6), where $v(n), \ k(n), \ c(n), \ c(n-1)$ are the current operated pixel, key stream element, output cipher pixel, previous cipher pixel, respectively.

$$c(n) = v(n) \oplus \mathrm{mod}(k(n) + c(n-1), L), n = 1, \cdots, H \times W. \tag{6}$$

An initial seed $c(0)$ is required to calculate the first pixel of cipher-image .

Step 5. Convert the yielded vector c to be one 2D matrix and the final cipher-image is then obtained. Encrypt the plain-image Lena one round with cipher key $x_0 = 0.367$, a =[0, 0.16, 0.3, 0.51, 0.68, 0.78, 1.0] and seed $c(0)$ =87, the resulted cipher-image is shown in Figure 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.

Performance Analysis

According to the basic principle of cryptology [12], 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 analysis (histograms, correlation coefficients, information entropy), key space analysis, differential 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.

Histogram analysis. Histogram analysis is a visual test to demonstrate pixel intensity distribution. An image histogram is a graph showing the number of pixels at each different intensity value existing in the considered image. The histograms of plain-image and cipher-image are shown in Figure 2(c)-(d). It follows from the histogram of the cipher-image that it is fairly uniform and significantly different from the histogram of plain-image. Hence 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. It is common sense that 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 yield 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:

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

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.

Information Entropy Analysis. Information entropy is a measure of the uncertainty of a random variable and can be also a measure of disorder and randomness. It can be used to measure the uniformity of image histograms as well. The entropy $H(m)$ of a gray image I can be measured by $H(I) = -\sum_{i=0}^{L-1} p(r_i)\log_2(p(r_i))$ (bits), where L is the 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 calculate the information entropy for plain-image Lena and its cipher-image. The results are 7.4451 and 7.9975 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.

Tab. 1. Correlation coefficients between adjacent pixels.

Test image	direction	Plain-image	Cipher-image
Lena	Horizontal	0.9857	-0.0023
	Vertical	0.9725	-0.0039
	Diagonal	0.9571	-0.0000138

Differential Attack Analysis. Differential cryptanalysis focuses on the study of how differences in a plaintext can affect the resultant differences in the ciphertext with the same cipher key. Regarding image cryptosystems, attackers may usually modify only one pixel with one bit difference of the plain-image, then compare two cipher-images using the same cipher keys to find out some meaningful relationships between the plain-image and the cipher-image. If the attackers can find some meaningful relationships between plain-image and cipher-image, they may further find out the cipher key or equivalent key streams. If one slight difference in the plain-image will cause significant, random and unpredictable changes in the cipher-image, then the encryption scheme will resist differential analysis attack efficiently. Two most common measures NPCR (number of pixel change rate) and UACI (unified average changing intensity) are used 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

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

We randomly choose ten pixels and calculate the NPCR and UACI. The result is shown in Table 2. We also choose 100 pixels in plain-image randomly, and changing their intensity value by one unit at the selective pixel. The averages of 100 NPCR values and 100 UACI values are 99.6139 and 33.4624. It is clear that the NPCR and UACI values are very close to the expected values 99.6094 and 33.4635, thus the proposed image encryption technique shows good sensitivity to plaintext and hence invulnerable to differential attacks.

Conclusion

An efficient image encryption scheme based on bit-plane pairs exchange permutation by generalized Arnold map and diffusion by multimodal skew tent map is proposed in the paper. The proposed scheme can only shuffle the plain-image pixel positions, but also change pixel gray values efficiently in the permutation process. An effective diffusion process is also designed to alter the gray values of the whole image pixels. Security analysis including key space analysis, statistical attack analysis, differential attack analysis are performed numerically and visually. All the experimental results show that the proposed encryption scheme is secure thanks to its large key space, its high sensitivity to the cipher keys and plain-images. 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 and SRP of Science College of Shantou University.

Tab. 2. Difference analysis of plain-image Lena

Positions	(141,105)	(158,205)	(49,120)	(121,20)	(94,91)
NPCR	99.6231	99.6185	99.5926	99.6231	99.6262
UACI	33.4521	33.5716	33.4971	33.2997	33.4503
Positions	(61,59)	(198,137)	(69,196)	(21,220)	(252,145)
NPCR	99.6048	99.6124	99.6109	99.6124	99.6170
UACI	33.4956	33.5116	33.4444	33.5109	33.4716

References

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

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

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

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

[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, Optics Commun., 284(2011), 4331-4339.

[6] W. Guo, J. Zhao, R. Ye, A chaos-based pseudorandom permutation and bilateral diffusion scheme for image encryption, I.J. Image, Graphics and Signal Processing, 6:11(2014), 50-61.

[7] 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.

[8] 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.

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

[10] 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.

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

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