The novel adaptive image encryption scheme based on the chaos map and the pseudo vector multiplication

Li Zongying[1, a] and Liu Xiang[2,b]

[1]School of Logistics,Linyi University,Shandong,Linyi,China 276005

[2] School of Architecture,Linyi University,Shandong,Linyi,China 276005

[a]zongying_li@126.com, [b]liuxiang0632@126.com

Keywords: The Arnold map, Pseudo vector multiplication, Histogram, Entropy, Correlation.

Abstract. In the paper, an adaptive image encryption scheme is proposed, which is designed by means of the Arnold map and the pseudo vector multiplication. In order to testify the scheme, the large number of experimental simulations are carried out, and its results show that the scheme is suitable for image encryption, and some statistical tests are provided to show the higher security in the end.

Introduction

As we all known, more and more images are transmitted and stored through the internet in recent years. Under this circumstance, the image encryption schemes are therefore more and more critical. At present, many researchers dedicated to the study of image encryption and obtained a lot of very meaningful results [1,2,3,4]. The present paper proposes a novel adaptive image encryption scheme based on the chaos map and the pseudo vector multiplication.

In the following sections, the paper is organized as follows. In Section 2, some paper preparations are introduced. The proposed encryption scheme is investigated in Section 3. Experimental results and some security analyses are performed and discussed in Section 4. Finally, Conclusions are drawn in Section 5.

Paper preparation

The 2D Arnold map. The Arnold map can be regarded as the process of tensile, compression, folding and stitching. The general 2D Arnold transformation [4] is an invertible chaotic map, which may be described as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \qquad (1)$$

And its reversible form can be described as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \bmod N \qquad (2)$$

The Arnold map is chaotic map, Eq. 1 is a standard 2D Arnold map when N =1, and its geometrical explanation is shown in Fig.1[4].

The 2D Arnold map also can be generalized by introducing two control parameters a and b as follows:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \bmod N \qquad (3)$$

where a, b, N are positive integer and such that $a, b < N$.

The pseudo vector multiplication. Only permutate the location of the image pixel by the 2D Arnold map when we want to encrypt one digital image, we can’t change the statistical histogram of the image. Therefore, we must apply the diffusion function to change the statistical histogram of the □

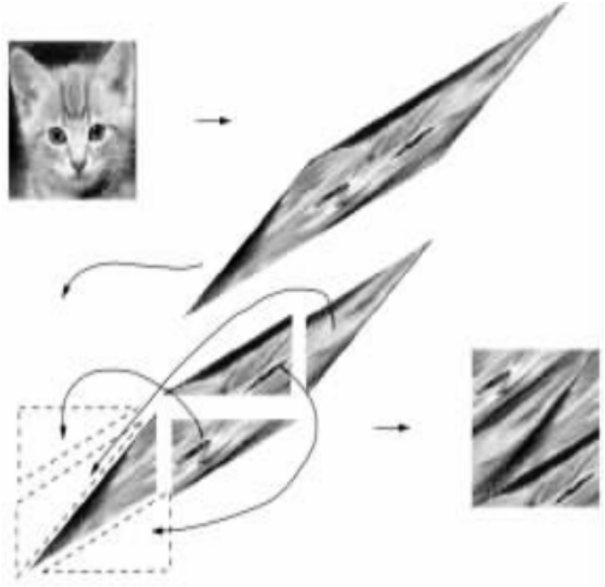

Fig.1 the generalized discrete 2D Arnold map

image, the pseudo vector multiplication is presented as one kind of gray value diffusion function, which is described as:

$$A \otimes B' = a_1 \otimes b_1 \oplus \cdots \oplus a_n \otimes b_n \qquad (4)$$

Where $A = \{a_1, a_2, \cdots, a_n\}$ and $B = \{b_1, b_2, \cdots, b_n\}$ dare two integer vectors with the same length. The operation symbol $\otimes$ and $\oplus$ are defined as:

$$a \otimes b = \mathrm{mod}\left(a + b, 256\right)$$

$$a \oplus b = bitxor\left(a, b\right)$$

It's obvious that the result of $A \otimes B'$ is an integer, and $A \otimes B' \in [0, 255]$.

In the paper, let $f_{value} = A \otimes B'$, and regard it as the gray value of one fictitious pixel corresponding to the pixel at the grid (x, y). In order to gain the value f_{value}, firstly,we split the image into some small blocks, then make the elements of the xth row and the yth column in every small block into the vector A and B, at last by means of the following expression(Eq.4) to achieve the gray value diffusion.

$$. \qquad f\left(x, y\right) = \mathrm{mod}\left(f\left(x, y\right) + f_{value}, 256\right) \qquad (5)$$

The image encryption scheme

The novel adaptive digital image encryption scheme is presented, and the integrated image encryption scheme consists of the following four steps of operations:

Step 1. Select the initial keys: the 2D Arnold map controlling parameters a and b; the size of the small blocks N and the image encryption scheme iteration rounds k.

Step 2. By means of the 2D Arnold transformation to the image pixel position of scrambling.

Step3: Split the image into some small blocks with size of $N \times N$, and for every image pixel, the previously Eq.5 is used to get a newly transformed image with the corresponding fictitious pixel which is given by Eq.4.

Step4: Repeating Step2 and Step3 k rounds to satisfy the requirement of security. At last we can achieve the encrypted image.

The deciphering procedure about the image encryption scheme is similar to that of the enciphering process illustrated above.

The experimental simulation analysis.

In this section, the image Lena of size 512×512 and 256 gray levels is taken as the experimental image to testify the quality of encryption scheme.

The histogram analysis. As we all known, the statistical analysis has been performed on the proposed image encryption algorithm[3,4,5,6], which demonstrates its superior confusion and diffusion properties to strongly resist statistical attacks.

Fig.2 shows us that the histograms of the plain image and ciphered image of Lena. As we can see, the histogram of the ciphered image is fairly uniform and significantly different from that of the original image only after five rounds of the diffusion process.

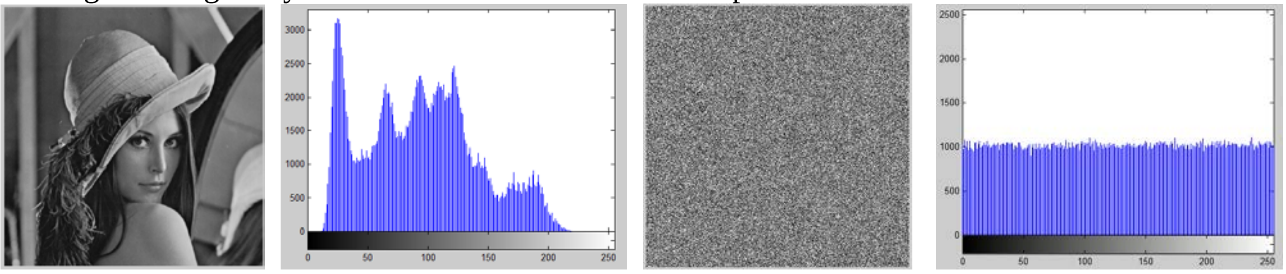

Fig.2 The histogram of the ciphered image and the plain image

The Information Entropy Analysis. Entropy[3,9] is a statistical measure of randomness which can measure the image gray value distribution. Entropy is defined as:

$$H(s) = \sum_{S} P(s_i) \log_2 \frac{1}{P(s_i)} \qquad (6)$$

Where $P(s_i)$ is the probability of symbol s_i.

The entropy of the original image Lena is 7.5851, Fig.3 shows that various values of the entropies for the different encryption rounds. It is obvious that all the entropy values of the encrypted image are very close to the max of entropy value of 8, which means that a high confusion is achieved in the encrypted system.

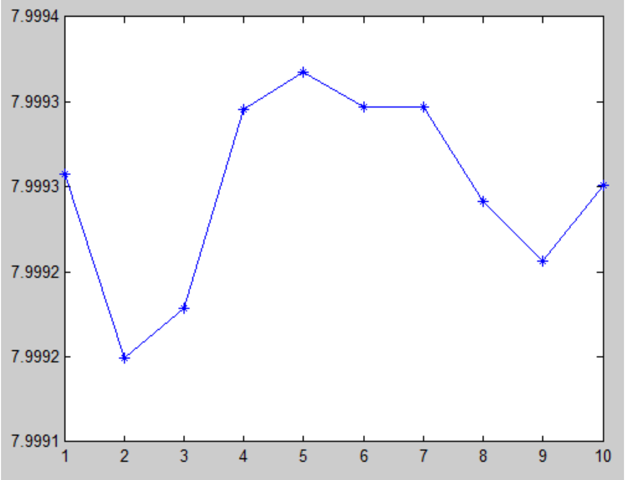

Fig.3 the entropies of the different encrypted image

The Correlation of Adjacent Pixels. The correlations between two adjacent pixels along horizontal, vertical and diagonal directions are calculated to analyze the effectiveness of our cryptosystem in this aspect. The correlation coefficient [6,7,8,9,10] is defined as:

$$r(x,y) = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \qquad (7)$$

Where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \,, D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \,, \operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right)$$

In the paper, 3000 pairs of digital image pixels were selected randomly to calculate the correlations. Fig.4 shows the correlation between the plain image and its encryption image on the different directions. The results imply that the proposed encryption algorithm can effectively make the adjacent pixels lower correlated.

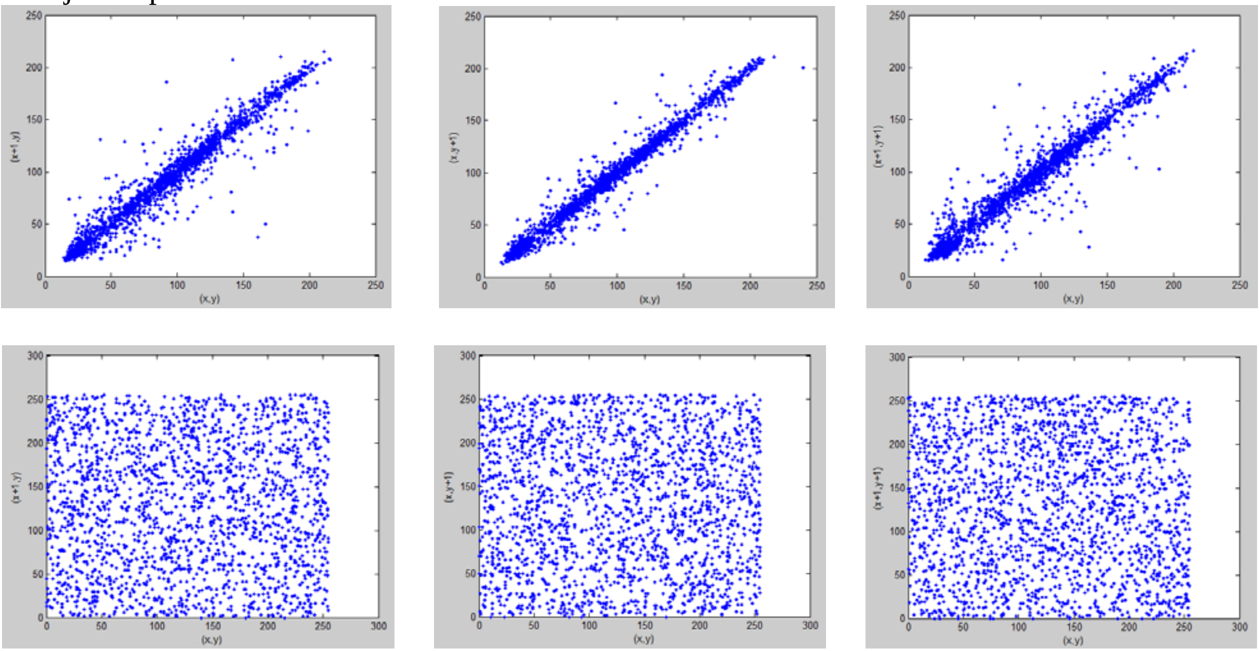

Fig.4 The correlation on the different directions

Conclusions

In the paper, a novel adaptive image encryption scheme is proposed, which is designed by means of the Arnold map and the pseudo vector multiplication. And a large number of simulation experiments were carried out, including the histogram analysis, the information entropy analysis and the correlation of adjacent pixels analysis. The experimental results show that the encryption scheme is a very effective encryption algorithm.

References

[1] K. R. Cast leman. Digital Image Processing. Prent ice Hall, Inc, 1996.

[2] R. C. Gonzalez and R. E. Woods. Digital Image Processing (2nd Edit ion). Elect ronic Indust ry Press, 2003.(in Chinese).

[3] R. C. Gonzalez, R. E. Woods and S. L. Eddins. Digital Image Processing Using MATLAB. Elect ronic Indust ry Press, 2004.

[4] G. R. Chen and X. F. Wang. Dynamical Systems Chaos Theory, Methods and Applicat ions. Shanghai Jiaotong University Press, pp. 80-105, 2006.(in Chinese).

[5] D. X. Qi, J. C. Zou and X. Y. Han. A New Class of Scrambling Transformat ion and Its Applicat ion in the Image Informat ion Covering. Science in China(Series E), vol. 43(3), pp. 304-312, 2000.

[6] Y. W. Zhang, Y. M. Wang and X. B. Shen. A chaos-based on image encrypt ion algorithm using alternate st ructure. Science in China(Series F), vol. 50(3), pp. 334-341, 2007.

[7] Omar A.Saraereh,Qais Alsafasfeh and Aodeh Arfoa. Improving a New Logistic map as s New Chaotic Algorithm for Image Encryption,Modern Applied Science. vol.7(12), pp.24-33, 2013.

[8] J.Qiu,X.F.Liao,D.Xiao and T.Xiang. Adaptive image encryption scheme based on chaotic map , High Technology Letters.vol.19(1), pp.76-81, 2013.

[9] X.J.Tong,Y.Liu M.Zhang and H.Y.Shi. New Chaotic Image Encryption Algorithm Based on Cross-Mapping,Wuhan University Journal of Natural Sciences. vol. 17(6), pp.461-467, 2012.

[10] Z.Wang,X,Huang,N,Li and X.N.Song. Image encryption based on a delayed fractional chaotic logistic system. Chin.Phys.B. vol.21(5). 2012.