THE NOVEL IMAGE DIFFUSION ALGORITHM BASED ON THE PSEUDO RANDOM BLOCK

[1]ZONGYING LI
[1]School of Logistics, Linyi University, Shandong, Linyi, China 276005
E-mail: [1]zongying_li@126.com

ABSTRACT

In this article, we firstly introduce a novel image diffusion algorithm, which is based on the two pseudo random image block, and then we encrypt the digital image with it. The large number of simulations is carried on, and the simulation results show that the proposed algorithm is a very efficient diffusion algorithm.

Keywords: *Tent Map, Pseudo Random Distance Sequence, Histogram, Entropy.*

1. INTRODUCTION

With the rapid development of information technology, internet has become an important part of our daily lives. Under these circumstances, the Cryptographic schemes are therefore critical for secure multimedia content storage and distribution over open networks. At present, many researchers dedicated to the study of image encryption and obtained a lot of very meaningful results [1,2,3,4], however, these classic traditional image encryption algorithm may still need improvement.

In the following sections, we present a whole novel digital image encryption algorithm, and the experimental results and analysis have both shown that the algorithm is a very efficient digital image encryption algorithm.

2. PAPER PREPARATION

The Tent Chaotic System. The tent map [5] is one of the simplest and most widely studied nonlinear dynamical systems capable of exhibiting chaotic system which can be written as:

$$x_{n+1} = a - (1+a)\,abs(x_n) \tag{1}$$

When $a \in (0,1)$ and $x \in (0,1)$, the system dynamic shape is very complex, the system is a chaotic, and the form of $a \in (0.99,1)$ is a more complex systems dynamics.

We can get a chaotic sequence $C = \{c_1, c_2, \cdots, c_{100}\}$ through iterating Eq.1 enough rounds, and for $\forall i \in \{1,2,\cdots,100\}$, let $t_i = \lceil 10000 * c_i \rceil \bmod S_0$,where $S_0 \in Z$ and the symbol $\lceil a \rceil$ means that getting the smallest integer which is not smaller than a, then the new integral sequence $T = \{t_1, t_2, \cdots, t_{100}\}$ is generated, and we name it the pseudo random distance sequence.

The Distance Between Two Block Matrix. Suppose A and B are squares with the size of $N \times N$, and represent the gray value matrix on the image block, we define the following expression as the distance between two block matrixes.

$$d_{A,B} = \frac{Index_{A(1,1)} - Index_{B(1,1)}}{N} \tag{2}$$

Where $Index_{A(1,1)}, Index_{B(1,1)}$ mean the index of the first element of matrix A and B.

The Pixel Gray Value Diffusion Equation. When we encrypt the digital image, we introduce the spread of pixel gray value transformation in order to make the statistical histogram of the encrypted image become more uniform. And the expression is given as follow:

$$A(x,y) = bitxor\left(A(x,y), B(x,y)\right) \tag{3}$$

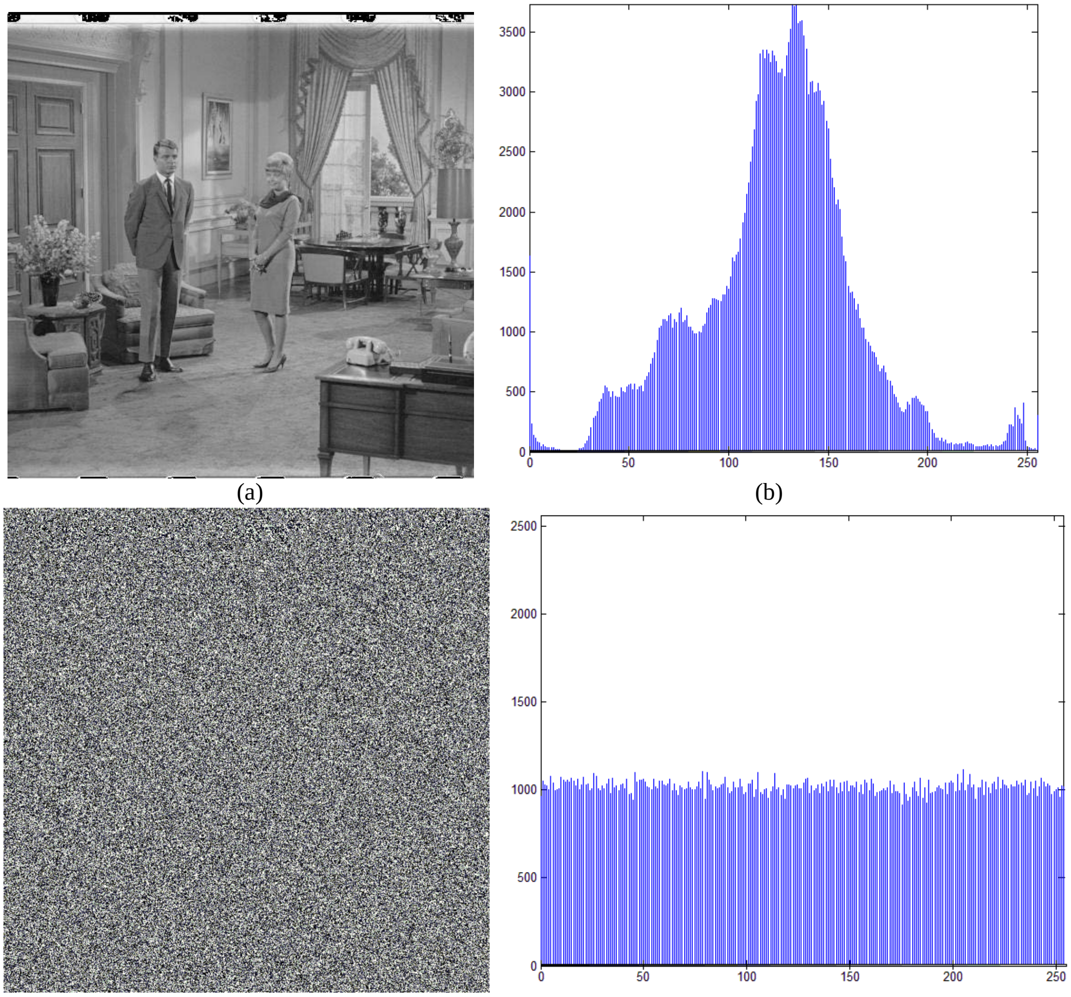
where $A(x,y)$ means the gray value of the pixel at the grid (x,y) in the block A, and $B(x,y)$ means the gray value of the pixel at the grid (x, y) in the block B. We name Eq.3. as the diffusion equation based on the pseudo random block, obviously, it's a reversible transformation.

The Encryption Algorithm Steps. The integrated image encryption scheme which is based on the pseudo random block consists of the following three steps of operations:

Step1 Select the key: Tent map include the initial value x_0, the controlling parameter a. The parameter of the pseudo random distance sequence S_0. The size of image block is N and the image iteration rounds is k.

Step2 For every image pixel block, the previously Eq.3. is used to build a newly image with the corresponding image block.

Step3 Repeat Step2 for k rounds to satisfy the requirement of security. Finally we can get the encrypted image.



(a) (b)

(c) (d)

Figure 1. Image And Its Histogram.

where m is the total number of symbols; $p(m_i)$ represents the probability of occurrence of symbol m_i. For a random source emitting 256 symbols, its entropy is $H(m) = 8$.

3. THE EXPERIMENTAL RESULTS ANALYSIS

In order to test the effect of encryption algorithm, a large number of simulation results and performance analysis are provided in this section to investigate the quality of encryption， which are based on the proposed image encryption scheme.

In this paper, we take image Couple of size 512×512 and 256 gray levels as the experimental image. The simulation results and performance analysis of the proposed image encryption scheme are provided in the following section.

The Histogram Analysis. As we all known, statistical analysis has been performed on the proposed image encryption algorithm, which demonstrates its superior confusion and diffusion properties to strongly resist statistical attacks.

Histograms[6,7,8,9,10] of encrypted images: one typical example among them is shown in Figure1.; one can see that the histogram of the encrypted image for Couple image is fairly uniform and is significantly different from that of the original image.

The Information Entropy Analysis. Entropy[3,9] is a statistical measure of randomness which can be used to characterize the texture of the input image. Entropy is defined as:

$$H(m) = \sum_{i=0}^{m-1} p(m_i)\log_2 \frac{1}{p(m_i)} \qquad (4)$$

The entropy of the original image selected in the paper is 7.23297, Figure2 indicates the various values of the entropies about the different encryption rounds. It is not difficult to find that the entropy of the encrypted image which is very close to the maximum value on the random gray image， when encryption rounds is more than 4, which means that the cipher-images are close to a random source , therefore, the proposed algorithm in the paper is secure against the entropy attack.

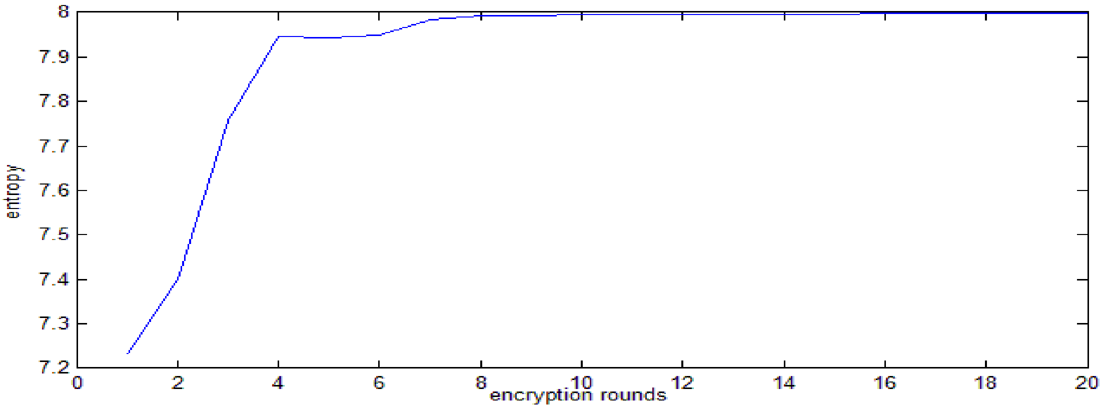


Figure 2. Entropy Vs. Encryption Rounds.

The Key Sensitivity Test. We perform this test on the 512×512 Couple image. First of all, 5 sub-keys, namely, Key_{x_0} , Key_a , Key_{S_0} , Key_N and Key_k are chosen. The encryption is then carried out to obtain the cipher image. Then one sub-key is changed and the encryption is performed again with all other sub-key remain unchanged. The pixel gray scale values of the two cipher images are then compared.

In addition, testing with slightly different encryption keys, decryption using keys with only one sub-key changed is also performed. Figure3. shows the experimental results. As observed from the figure, the decrypted image is totally different from the plain one even when there is only one sub-key changed in the decryption key. Similar results for other sub-keys Key_{x_0} , Key_a , Key_{S_0} , Key_N and Key_k are tabulated in Table I.

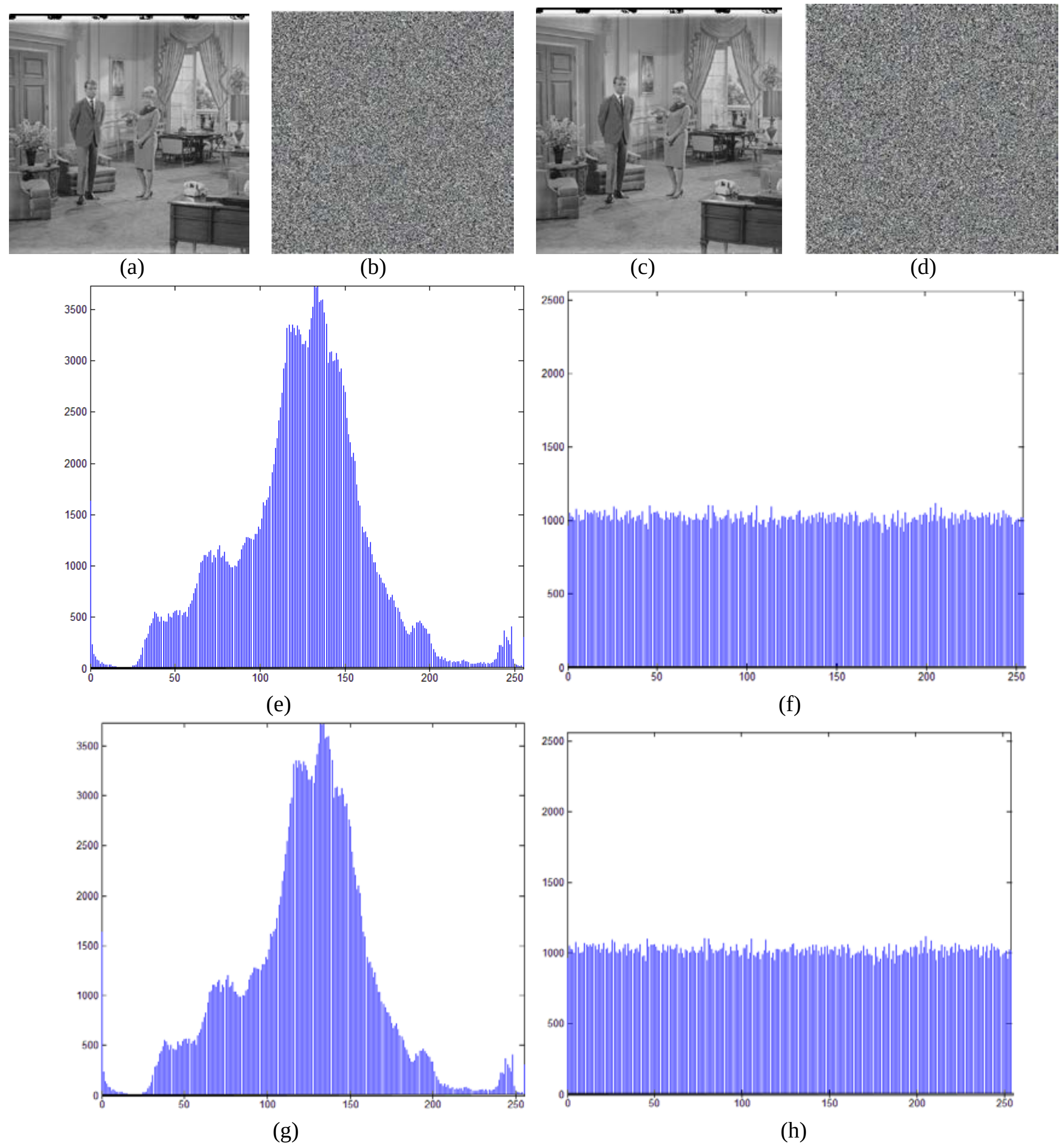


Figure3. *Key sensitivity test: (a) Plain image; (b) Cipher image ($Key_{x_0} = 0.2345$, $Key_a = 0.99825$, $Key_{S_0} = 64$, $Key_N = 8$, $Key_k = 20$); (c) correct decrypted image; (d) decrypted image($Key_{x_0} = 0.23450001$, $Key_a = 0.99825$, $Key_{S_0} = 64$, $Key_N = 8$, $Key_k = 20$);(e) the histogram of (a); (f) the histogram of (b); (g) the histogram of (c);(h) the histogram of (d).*

Table 1. Results Of Key Sensitivity Test

	Key 1 (Originalvalue)	key 2 (Modifiedvalue)	Pixel difference in encryption	Pixel difference in decryption
Key_{x_0}	0.2345	0.2345001	99.618912 %	99.618530%
Key_a	0.99825	0.998250001	99.608231%	99.612045%
Key_{S_0}	64	65	99.600220%	99.589157%
Key_N	8	7	99.607086%	99.591827%
Key_k	20	21	99.630737%	99.612808%

4. CONCLUSIONS

In this paper, we proposed an efficient diffusion approach to address the efficiency problem in image encryption. In the approach, we firstly create one pseudo random distance sequence through the tent map, then make use of it and dot bitxor operation in the diffusion process to encrypt image. At last a large number of simulation experiments are carried on, and the experimental results show that the proposed algorithm is a very efficient diffusion algorithm, which has excellent potential for practical image encryption applications.

REFERENCES

[1] K.R.Castleman. Digital Image Processing. Prentice Hall, Inc, (1996)

[2] R.C.Gonzalez and R.E.Woods. Digital Image Processing (3nd Edition). Prentice Hall, (2008)

[3] R.C.Gonzalez, R.E.Woods and S. L. Eddins. Digital Image Processing Using MATLAB. Electronic Industry Press,(2004)

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

[5] http://wenku.baidu.com/view/7c6f4a000740be1e650e9a75.html

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

[7] Abir Awad and Dounia Awad. Efficient Image Chaotic Encryption Algorithm With No Propagation Error. ETRI Journal. vol. 32(5), pp. 774-783,(2010)

[8] L. H. Zhang, X. F. Liao and X. B. Wang. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals. vol. 24, pp. 759-765, (2005)

[9] Kamlesh Gupta, Sanjay Silakari. New Approach for Fast Color Image Encryption Using Chaotic Map. Journal of Information Security, vol. 2, pp.139-150,(2011)

[10] Wong K W,Kwok B S H,Yuen C H.An efficient diffusion approach for chaos-based image encryption[J].Chaos,Solitons & Fractals, vol.41 (5), pp. 2652-2663,(2009)