Applied Mechanics and Materials
ISSN: 1662-7482, Vols. 556-562, pp 4722-4725
doi:10.4028/www.scientific.net/AMM.556-562.4722

Online: 2014-05-23

A Dual Image Scrambling Method Based on Discrete Cosine Transform

Qiudong Sun[a], Jiancun Zuo[b], Yufeng Shao[c] and Lin Gui[d]

School of Electronic and Electrical Engineering,

Shanghai Second Polytechnic University, Shanghai 201209, China

[a]qdsun@sspu.edu.cn, [b]jczuo@ sspu.edu.cn, [c]yfshao@ sspu.edu.cn, [d]guilin@ sspu.edu.cn

Keywords: discrete cosine transform, 1-D random scrambling, dual scrambling, image encryption.

Abstract. Although the general random scrambling based on pixel can achieve a good chaotic effect, but it can not change the histogram of a digital image. We introduce the random scrambling into the domain of discrete cosine transform (DCT) of image and scramble the coefficients of DCT to improve the performance of scrambling. Firstly, we did 2-D discrete cosine transform to the original image. Secondly, we scanned the coefficients matrix of DCT by Zig-Zag scanning to get a 1-D sequence, and then we scrambled this sequence by 1-D random scrambling algorithm. Thirdly, we did inverse Zig-Zag scanning to the scrambled sequence and reconstructed the scrambled image from the chaotic coefficients matrix by 2-D inverse discrete cosine transform. Finally, to further improve the scrambling degree of the reconstructed result, we scrambled it again in space domain to gain the encryption image. Experiments show that this algorithm is effective at visual evaluation and is more stable in scrambling degree than Arnold transformation.

Introduction

Due to media data (such as digital image, video etc.) are very easy to be intercepted illegally when they are transmitted in the network. Therefore, people pay more attention to the security of media data and have developed four types of information hiding techniques, which are scrambling, watermarking, share storing and hiding [1].

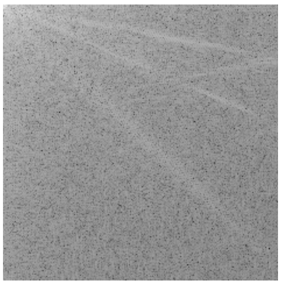
This paper will discuss the scrambling technique for digital image encryption. Many typical image encryption methods scramble the pixels in an image directly [1-6]. These methods restrict the scrambling degree to a certain extent [7]. Some algorithms, also, do scrambling in transformation domain [7, 8]. But they, in general, are too complicated to be realized.

This paper will introduce a simple 1-D random scrambling algorithm [6] to the image in its discrete cosine transform (DCT) domain. We will do first scrambling to the coefficients of DCT of the original image. After reconstructing the shuffle coefficients matrix to a chaotic image, we will also do second scrambling to this image in space domain to further improve its scrambling degree.

1-D Coefficient Sequence of DCT

Discrete Cosine Transform of an Image. In order to scramble an image in its DCT domain, we should do DCT to this image firstly. If the original image is shown as in Fig. 1, which is a “Cameraman”, then its DCT energy spectrum in logarithm domain is shown as in Fig. 2. In Fig. 2, the biggest coefficient of DCT is generally the DC coefficient found in the top left corner of DCT matrix, which is the feature description of mean gray value of the image. Besides the DC coefficient, the other coefficients in DCT matrix are AC coefficients, which stand for the feature description of texture characteristics of the image and their frequencies rise gradually from the upper left to the lower right. So, if we only interchange the AC coefficients, then the texture characteristics of the image can be changed, but its mean intensity can be remained. That is we just want to do.

Zig-Zag Scanning to AC Coefficients. The AC coefficients of DCT matrix can be rearranged into a 1-D sequence by the Zig-Zag scanning, which can ensure the continuity to neighboring coefficients of DCT matrix. Its diagram pattern is shown as in Fig. 3.



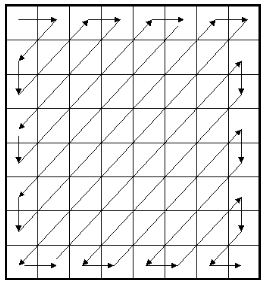


Figure 1. Original image of "Cameraman" Figure 2. DCT energy spectrum of Fig. 1 Figure 3. Zig-Zag Scanning Diagram

1-D Random Scrambling

Random Scrambling. In order to complete the random scrambling of 1-D sequence $\boldsymbol{V}$, we need two random sequences $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$, whichever has a length same as that of $\boldsymbol{V}$. $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$ can be generated by a random natural number generator with the property of uniform distribution using two different seeds respectively. Which two elements in $\boldsymbol{V}$ to be exchanged are determined by the values of relative positions of $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$ [6].

Because both $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$ are of property of uniform distribution and generated by different seeds, they are almost not correlative. The scrambled 1-D vector $\boldsymbol{V}$, therefore, must be of properties of random and uniform distribution. Consequentially, it will have real scrambling effect.

Random Anti-scramblinge. Due to the interchanging rule is reversible, hence, when two random sequences $\boldsymbol{R}_S$ and $\boldsymbol{R}_D$ in anti-scrambling are same as that of in scrambling, the anti-scrambling can also be completed by doing the random scrambling again [6].

Dual Scrambling

First Scrambling. After the image transformed by DCT, we choose different couple of seeds and do scrambling to all AC coefficients in DCT domain. That is the first scrambling.

Second Scrambling. To improve the efficiency of the algorithm, we just do scrambling one time in DCT domain. In the result, the gray distribution of reconstructed image may not be well-proportioned. Thus, it is necessary to scramble the reconstructed image again in space domain. After that, the gray distribution of scrambled image looks like very uniform at once. That is the second scrambling.

Scrambling Security. Because of the fact that there are two seeds requiring in random number generating both in scrambling and anti-scrambling, the proposed algorithm must be an encryption method based on the key. The key space composed of several couples of seeds, theoretically, is infinite. It is obvious that the proposed algorithm is very safe for image encryption.

Experiment Result Analysis and Comparison

In the experiment, we choose N=1 and do the dual random scrambling to the gray image Cameraman as shown in Fig. 1, which is of size 256×256. The result is shown as in Fig. 6. The four sub-images in Fig. 2(b) are the results of 1-level wavelet decomposing from Fig. 2(a). The scrambled DCT energy spectrum in Fig. 4 are the results of first scrambling to Fig. 2, and the first scrambled result is reconstructed from Fig. 4 as shown in Fig. 5. Fig. 6 is the result of doing second scrambling to Fig. 5, and it is the final scrambled image. The anti-scrambling result is shown in Fig. 7, which is completely same as the original image.

From the experiment results, we know that the scrambled result of image "Cameraman" is very like the white noise although it just goes through one time dual random scrambling. We also know that by comparing the histograms of the original image (as shown in Fig. 8) and the scrambled image (as shown in Fig. 9). The later has already been distributed in a nearly normal fashion and are quite different from the former. The scrambling effect of proposed method, apparently, is very good and better than that of those algorithms need iteration, such as the classical method - Arnold transform.

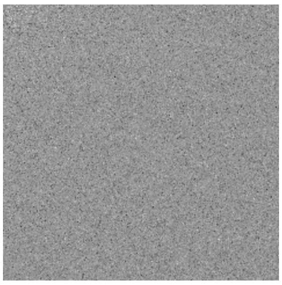


Figure 4. Scrambled DCT of Fig.2

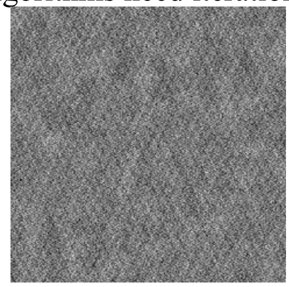


Figure 5. IDWT reconstruction of Fig.4

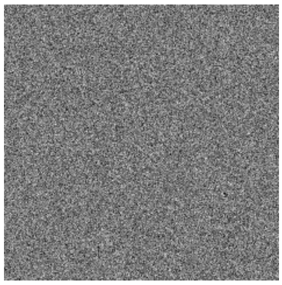


Figure 6. 2nd time scrambling of Fig.5

Figure.7 Anti-scrambling of Fig. 6

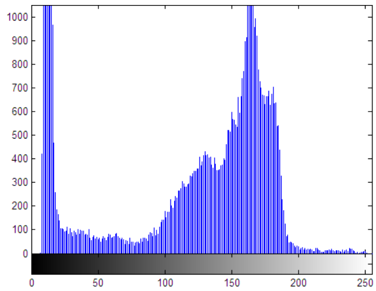


Figure 8. Histogram of Fig.1

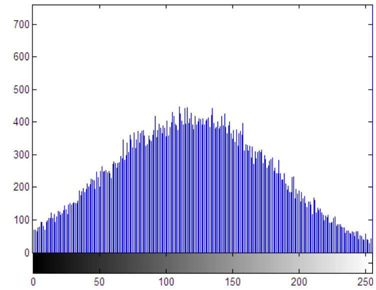


Figure 9. Histogram of Fig.6

The grade of image scrambling can be evaluated quantificationally by scrambling degree (SD) [9, 10]. According to the scrambling degree evaluation method in reference [9], after being transformed into another image ***B*** by a transformation T, a digital image ***A*** has scrambling degree as follows:

$$S(\boldsymbol{A}) = \frac{\sum_{k=1}^{K}\left(\mu(k) \times \frac{H(k)}{H}\right)}{\sum_{k=1}^{K}\mu(k)} \tag{1}$$

where H and $H(k)$ are the entropy of whole image ***B*** and the entropy of k^{th} block of ***B***, $\mu(k)$ is the average of differences between all two connective pixels in block k of ***B***.

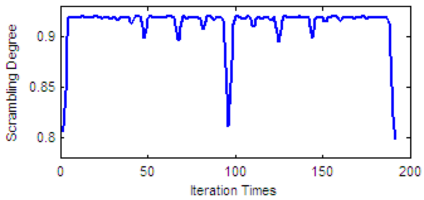


Figure 10. SD curves of Arnold transform

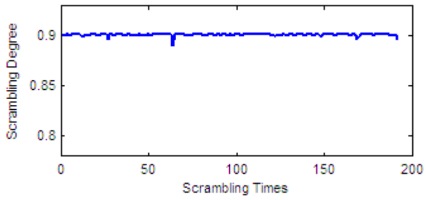


Figure 11. SD curves of one scrambling method

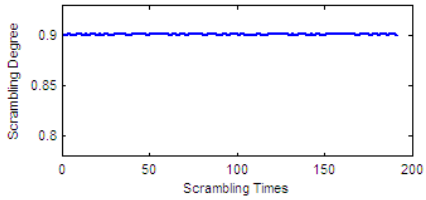


Figure 12. SD curves of dual scrambling method

We now use Eq. 1 to evaluate stability of a scrambling algorithm, which can be represented by the relationship between scrambling degree and iteration times or scrambling times. For Arnold transform, our proposed one scrambling method (just do scrambling in DCT domain) and our proposed dual scrambling method, the results are shown as Fig. 10, 11 and 12 respectively. Comparing with unstable Arnold transform, the scrambling degree of our method, apparently, is very stable. We also know that the scrambling degree of one scrambling method is lower than that of dual scrambling method sometimes. The former is in an interval from 0.891 to 0.903, while the later is in an interval from 0.900 to 0.903. So, the dual scrambling method is a little more stable than the one scrambling method.

When being iterated 192 times by Arnold transformation, the scrambling degree of the image will change substantially from 0.78 to 0.93. In foremost, midterm and aftermost iterations, the scrambling degrees are quite bad. After 192 times iterations, the scrambled image recovers to the original image exactly. It is shown that the Arnold transformation has the property of periodicity and its security is worse. If being scrambled 192 times by our method, the scrambling degree of the image will be almost kept over 0.9, namely the scrambling degree is almost invariableness regardless scrambling times. That is to say, our method can reach the goal of being scrambled rapidly, and is quite stable, also has no security problem of periodically recovering.

Summary

This paper presented a dual scrambling algorithm, which combined wavelet transform with 1-D random scrambling and did scrambling to a digital image in DCT domain and space domain respectively. The first scrambling was executed in DCT domain. It did the random scrambling to the AC coefficients of DCT results of the image. The second scrambling was executed in space domain after scrambled DCT coefficient matrix was reconstructed into a chaotic image. Experiments show that this algorithm is effective at visual evaluation and is more stable in scrambling degree than Arnold transform.

Acknowledgement

This work was supported by the Leading Academic Discipline Project of Communication and Information System of Shanghai Second Polytechnic University Grant (No. XXKZD1302) and the grant from the Technological Innovation Foundation of Shanghai Municipal Education Commission (No. 09YZ456).

References

[1] Qi Dongxu: Matrix Transformation and its Applications to Image Hiding. Journal of North China University of Technology, Vol. 11 (1999), No. 1, p. 24--28.

[2] Zhao Hong, Wen Wenya: A Survey of Digital Image Scrambling Techniques. Fujian Compute, (2007), No. 12, p. 10, 12.

[3] Tan Yuehui, Liang Xin, Zhang Junping, Liu Kai: The Study of Scrambling Technology Based on Arnold Transformation and Sampling Theoretics. Control and Automation, Vol. 22 (2006), No. 36, p. 74-76.

[4] Li Guofu: The Scrambling Method of Digital Image Based on Latin Square Transformation. Journal of North China University of Technology, Vol. 13 (2001), No. 1, p. 14-16.

[5] Zhang Shengyuan, Chen Jie: Digital Image Scrambling Technology Based on Matrix Transformation. Journal of Fujian Normal University (Natural Science Edition), Vol. 22 (2004), No. 4, p. 1-5.

[6] Sun Qiudong, Ma Wenxin, Yan Wenying, Dai Hong: A Random Scrambling Method for Digital Image Encryption: Comparison with the Technique Based on Arnold Transform. Journal of Shanghai Second Polytechnic University, Vol. 25 (2008), No. 3, p. 159-163.

[7] Hou Qibin, Yang Xiaofan, Wang Yangsheng, Huang Xiangsheng: An Image Scrambling Algorithm Based on Wavelet Transform and Knight's Tour. Journal of Computer Research and Development, Vol. 41 (2004), No. 2, p. 369-375.

[8] Yin Dehui, Tang Yan, Li Bingfa: Image Scrambling and Gray-level Diffusion Algorithm Based on Wavelet Transform. Journal of Sichuan University (Natural Science Edition), Vol. 42 (2005), No. 4, p. 706-709.

[9] Zhang Huaxiong, Lv Hui, Weng Xiangjun: Image Scrambling Degree Evaluation Method Based on Information Entropy. Journal of Circuits and Systems, Vol. 12 (2007), No. 6, p. 95-98.

[10] Shang Yanhong, Zheng Zheng, Wang Zhiwei: Digital Image Scrambling Technology and Analysis of Scrambling Degree. Journal of Tangshan Teachers College, Vol. 28 (2006), No. 2, p. 80-82.