

An Image Encryption Algorithm Based on Multi-Dimensional Orthogonal Sequence

Shuhong Li¹ Li Jing¹ Xing Gao²

1.College of Information, Henan University of Finance and Economics
No. 80, WenHua Road, Zhengzhou, Henan, 450002 P.R.China
Tel: +86-371-63518436, E-mail: lishuhong_1@hotmail.com

2. C-TECH CO.LTD
2-4-1 Shinjuku, Shinjuku-ku, Tokyo, 163-0806 Japan
E-mail: cgjgx75@yahoo.co.jp

Abstract: - This paper proposes a new approach for image encryption using multi-dimensional orthogonal sequence. The sequence can provide an orthogonal transform for digital data, which is useful for image encryption. The key to decrypt is a set of the parameters to generate the sequence. For a gray scale image and a binary image, four different sequences are used to encrypt. Two of them are used to encrypt original image directly, the others are used for divided image. The experimental results show that this method has the characteristic of high security, because the number of the sequence is large and the digital image after encryption is noise-like and random Gaussian distribution.

Key-Word: - Image Processing; Image Encryption; Multi-Dimensional Orthogonal Sequence; Orthogonal Transform; Random Gaussian distribution.

1 Introduction

With the rapid development of multimedia and network technologies, the security of digital images becomes more and more important, since the communications of digital products over networks occur more and more frequently. Furthermore, special and reliable security in storage and transmission of digital images is needed in many applications, such as pay-TV, medical imaging systems, military image database and communications as well of saving and exchanging digital images via the support of multimedia messaging services over wireless networks. To meet the challenges arising from different applications, good encryption of digital images is necessary.

Since the 1990s, many specific algorithms have been proposed, aiming to provide better solutions to

image encryption [1]–[4]. At the same time, cryptanalytic work on proposed image encryption schemes has also been developed, and some existing schemes have been found to be insecure from the cryptographical point of view [5]–[7].

A perfect sequence, sometimes called an orthogonal sequence, whose periodic auto-correlation takes zero except the zero-shift, i.e., impulsive response, has been applied in communications and signal processing. It can provide an orthogonal transform, which can scramble digital data and can encode some data simultaneously [8]. The multi-dimensional orthogonal sequence [9] is the generation of one-dimensional orthogonal sequence. But it can provide more sequences and security than one-dimensional orthogonal sequence. So an image

encryption algorithm based on the multi-dimensional orthogonal transform is proposed.

The paper is organized as follows. In Section 2, the definition and construction of the multi-dimensional orthogonal transforms are introduced. The image encryption scheme with multi-dimension orthogonal transform is introduced in Section 3. Section 4 presents the simulation results and also briefs about the effectiveness of the proposed scheme. In section 5, the paper is concluded by summarizing the present work along with the scope of future work.

2 Multi-Dimensional Orthogonal Transform

2.1 Multi-dimensional orthogonal sequence

Let a be an n -dimensional sequence of period $N_0=N_1N_2\cdots N_n$ expressed by

$$a^n = \{a_{i_1, \dots, i_j, \dots, i_n} \in R\}, 0 \leq i_j < N_j, \quad (1)$$

where N_j denotes period for j -direction, and R real numbers. We assume that the sum of the powers of the elements is equal to period N_0 , i.e.,

$$N_0 = \sum_{i_1=0}^{N_1-1} \cdots \sum_{i_n=0}^{N_n-1} |a_{i_1, \dots, i_n}|^2. \quad (2)$$

The periodic auto-correlation function of the multi-dimensional real sequence an is defined as

$$R_a^n(\tau_1, \dots, \tau_n) = \sum_{i_1=0}^{N_1-1} \cdots \sum_{i_n=0}^{N_n-1} a_{i_1, \dots, i_n} a_{i_1+\tau_1, \dots, i_n+\tau_n}, \quad (3)$$

where $a_{i_1+\tau_1, \dots, i_n+\tau_n}$ denotes the shift $\tau_1, \dots, \tau_j, \dots, \tau_n$ of sequence a^n , and a subscript i_j denotes a value of modulo N_j , i.e., $0 \leq i_j + \tau_j < N_j$. If it is the impulse function defined by

$$R_a^n(\tau_1, \dots, \tau_n) = \begin{cases} N_0 & \tau_1 = \dots = \tau_n = 0 \\ 0 & \text{otherwise} \end{cases}, \quad (4)$$

the sequence a^n is called n -dimensional orthogonal sequence of period N_0 .

The n -dimensional orthogonal sequence can be expressed by

$$a_{i_1, \dots, i_j, \dots, i_n} = \frac{1}{\sqrt{N_0}} \sum_{\lambda_1=0}^{N_1-1} \cdots \sum_{\lambda_n=0}^{N_n-1} \cos\left\{\frac{2\pi}{N_0} f(\lambda_1, \dots, \lambda_n) + \frac{2\pi}{N_1} \lambda_1 i_1 + \cdots + \frac{2\pi}{N_n} \lambda_n i_n\right\}, \quad (5)$$

where the function $f(x)$ is an odd function, and satisfied

$$0 \leq f(\lambda_1, \dots, \lambda_n) < N_0 \quad (6)$$

$$f(-\lambda_1, \dots, -\lambda_n) = -f(-\lambda_1, \dots, -\lambda_n) \bmod N_0 \quad (7)$$

$$-\lambda_j \bmod N_j = N_j - \lambda_j \quad (8)$$

where λ_j can be generated by pseudo random generator, whose seed can be the key to decrypt.

2.2 Multi-dimensional orthogonal transform

Let $X = x^n = \{x_{i_1, \dots, i_k, \dots, i_n} \in R\} (0 \leq i_k < N_j)$ be n -dimensional real data. We define the orthogonal transform using multi-dimensional orthogonal sequence as

$$y(j_1, \dots, j_n) = \frac{1}{\sqrt{N_0}} \sum_{i_1=0}^{N_1-1} \cdots \sum_{i_n=0}^{N_n-1} x_{i_1, \dots, i_n} a_{i_1+j_1, \dots, i_n+j_n}. \quad (9)$$

From the auto-correlation property of multi-dimensional orthogonal sequence, i.e., orthogonality, its inversion can be given as

$$x(i_1, \dots, i_n) = \frac{1}{\sqrt{N_0}} \sum_{j_1=0}^{N_1-1} \cdots \sum_{j_n=0}^{N_n-1} y_{j_1, \dots, j_n} a_{i_1+j_1, \dots, i_n+j_n}. \quad (10)$$

The transform and its inversion can be simply written as $Y = T_a^n(X)$, $X = T_a^n(Y)$. This orthogonal transform can be used as a scrambler or a decoder with good properties, which is characterized by

- data become random, because of Gaussian distribution,
- security is high against interceptors, because of high linear complexity,
- encoding is compact, because data is multiplexed and encoded,
- decoding is strong against intentional processing of encoding data, and colored noise, because of possession of high process gain (even if period of j -direction N_j is small, n -dimensional orthogonal sequence has long period.).

Therefore the orthogonal transforms using multi-dimensional orthogonal sequence are useful for systems, which can process multi-dimensional data.

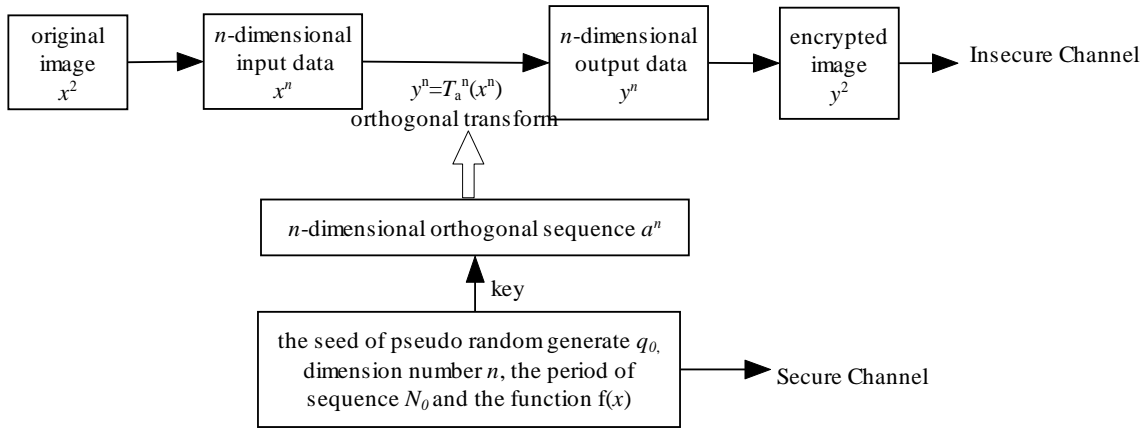


Fig.1 The block diagram of image encryption

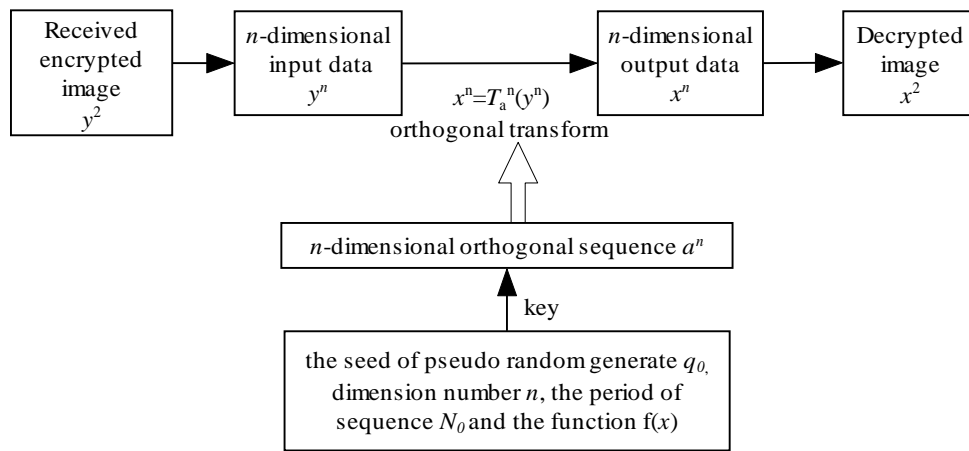


Fig.2 The block diagram of image decryption

3 Image Encryption System Using Multi-Dimensional Orthogonal Sequence

3.1 The process of image encryption and decryption

The block diagrams of the proposed image encryption and decryption system using multi-dimensional orthogonal sequence are shown in Fig.1 and Fig.2. In the process of image encryption, original image (x^2) is two-dimensional data which must be converted into multi-dimensional input data (x^n), then we can use the orthogonal transform $y^n = T_a^n(x^n)$ to get the encrypted multi-dimensional data (y^n). Finally the encrypted image is derived from an inverse process

($y^n \rightarrow y^2$), then it can be transmitted by the insecure channel.

In order to generate the multi-dimensional orthogonal sequence a^n , we must use some parameters as the dimension number n , the function $f(\lambda_1, \dots, \lambda_n)$ (satisfied the Eq.(6),(7) and (8)) and the period $N_0 = N_1 N_2 \dots N_n$ of the multi-dimensional orthogonal sequence. The variables of the function $f(\lambda_1, \dots, \lambda_n)$ are produced by pseudo random generator, whose seed is q_0 . Assume the output value q_j of pseudo random generator is in range $(0,1)$, then we can get integer $\lambda_j (1 \leq j \leq n)$ from q_j by

$$\lambda_j = q_j \pmod{j}. \tag{11}$$

So the key for encryption is the set $\{q_0, n, N_0, \text{ and the function } f(\lambda_1, \dots, \lambda_n)\}$. These parameters can be transmitted by the secure channel.

In the process of image decryption we can use same parameters to generate the same multi-dimensional orthogonal sequence to decrypt the received encrypted image. Because the choice of the key can be varied in big space, the security of the proposed image encryption is high.

3.2 The fast algorithm of the image encryption

Although the security of the proposed algorithm is high, the computed complexity is high. In order to save time, before the image data (x^2 or y^2) is converted into multi-dimensional data (x^n or y^n), we can divide the image into unoverlapped blocks, then for every block the multi-dimensional orthogonal transform can be used efficiently. For example, assume the size of original image Lena is $128 \times 128 \times 256$, we can divide it into four different unoverlapped blocks, the size of each block is $64 \times 64 \times 256$.

4 Simulation Results

The proposed image encryption scheme using multi-dimensional orthogonal transform has been implemented in the Matlab7.0 with several test images. Experimental results applied on the standard Lena gray scale image and a binary image A are shown in Fig.3 and Fig.4 respectively. And we compared the results with that of famous Arnold algorithm. The iterative operator of the Arnold algorithm is defined by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{mod } N \tag{12}$$

where $N=256$, and the time of iterative is 120. Comparing with the algorithm of this paper the Arnold algorithms have the decided iterative formula and periodicity. For the different N , the period is also different and hasn't a uniform formula to get the period. Moreover the value of N is restricted by the size of image. But in this paper the algorithm belong to random encryption and need not the iterative process. The encryption is only based on the set of

keys $\{q_0, n, N_0, \text{ and the function } f(\lambda_1, \dots, \lambda_n)\}$. So the security of this method is higher then the Arnold algorithm.

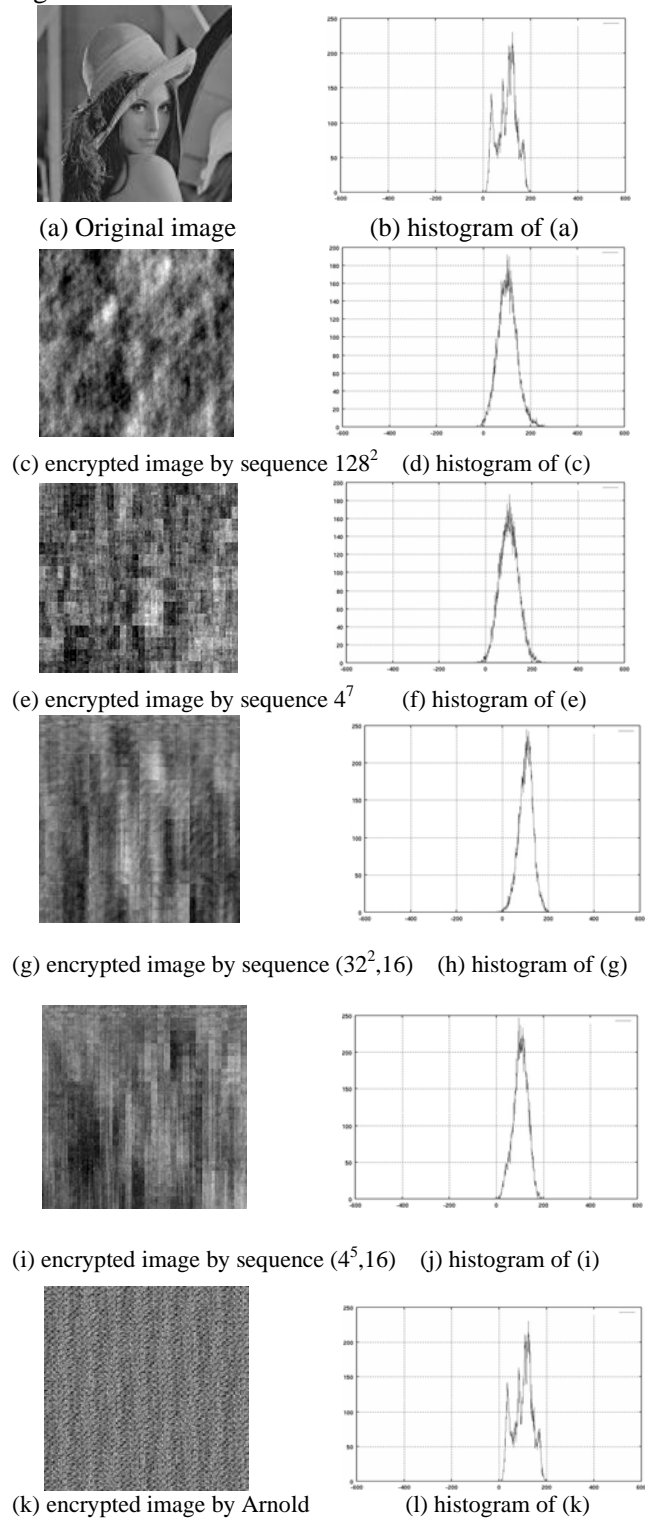


Fig.3 Results of gray scale image lena

In Fig.3, (a) is the original image, the standard *Lena* gray scale image (128×128×256), which is encrypted by four different sequences. And Fig.3.(b) is the histogram of original *lena* image. Then Fig.3.(c), (e), (g) and (i) are the images encrypted by different sequences, the corresponding histograms of them are Fig.3.(d), (f), (h) and (j). Finally Fig.3.(k) is the encrypted image by Arnold algorithm and Fig.3.(l) is its histogram. For the image in Fig.3.(c) and (e), the sequences 128^2 and 4^7 are used to *lena* image directly. But for the image in Fig.3.(g) and (i), the original image is divided into 16 blocks (every block is $32 \times 32 \times 256$), then every block is encrypted by sequence 32^2 and 4^5 respectively. So we write as sequences $(32^2, 16)$ and $(4^5, 16)$. From these results we can see that the images encrypted by different sequences have different histograms. However the characteristic of these histograms is same as random Gaussian distribution. And the histograms of image (g) and (j) is more centralized than that of (d) and (f).

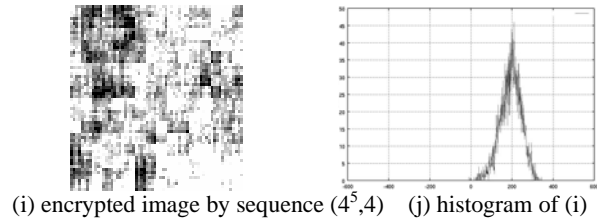
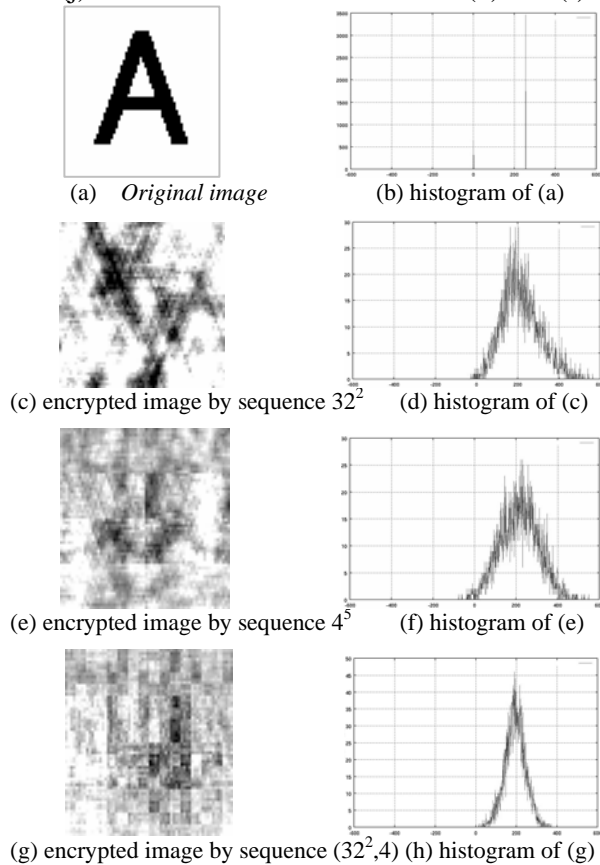


Fig.4 Results of binary image A

Fig.4 shows the results for a binary image A(64×64×2), which is also encrypted by four different sequences, and these sequences are 64^2 , 4^6 , 32^2 and 4^5 . The original image and its histogram are given in Fig.4.(a) and (b). The encrypted images are listed in Fig4.(c), (e), (g) and (i); their corresponding histograms are Fig.4.(d), (f), (h) and (j). From these results, we can see that the encrypted image is highly scrambled, and the characteristic of random Gaussian distribution for binary image is more obvious than that for gray scale image.

At the same time, the encrypted time for different image using different sequences is given in Tab.1. From the table we know that encrypting the divided image can save a lot of time.

Table.1 Computed time (unit: sec.)

image	Not dividing	divided
Lena(128×128)	710.6(128^2)	3.8($32^2, 16$)
	1683.0(4^7)	3.9($4^5, 16$)
A(64×64)	44.5(64^2)	2.9($32^2, 4$)
	138.8(4^6)	2.9($4^5, 4$)

5 Conclusion

In this paper, we have proposed an image encryption method using multi-dimensional orthogonal sequences. The proposed method is based on the fact that the number of the sequence is large and the encrypted image is noise-like and random Gaussian distribution, thereby increasing the security. But it has a problem that the multi-dimensional orthogonal transform need a lot of time. In order to implement the orthogonal transform quickly, the image is divided into small blocks. From the experimental results we can infer

that not only for gray scale image but also for binary image the method is effective.

In the present work the proposed method use a set of keys (parameters to generate the sequence) to ensure the security. In the future work we can use an image as one of the keys to provide better security.

6 Acknowledge

This work is supported by Science Technology Project of Henan Province of China under Grant No.0624260019 and No.072102210001, and Natural Science Foundation of Department of Education of Henan Province of China under Grant No.2004922081.

Reference

- [1] P. P. Dang and P. M. Chau, "Image encryption for secure internet multimedia applications," *IEEE Trans. Consumer Electron.*, vol. 46, no. 3, pp. 395-403, 2000.
- [2] K.-L. Chung and L.-C. Chang, "Large encryption binary images with higher security," *Pattern Recognition Letters*, vol. 19, no. 5-6, pp. 461-468, 1998.
- [3] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Trans. Signal Processing*, vol. 48, no. 8, pp. 2439-2451, 2000.
- [4] C.-C. Chang, M.-S. Hwang, and T.-S. Chen, "A new encryption algorithm for image cryptosystems," *J. Systems and Software*, vol. 58, no. 2, pp. 83-91, 2000.
- [5] J.-K. Jan and Y.-M. Tseng, "On the security of image encryption method," *Information Processing Letters*, vol. 60, no. 5, pp. 261-265, 1996.
- [6] C.-C. Chang and T.-X. Yu, "Cryptanalysis of an encryption scheme for binary images," *Pattern Recognition Letters*, vol. 23, no. 14, pp. 1847-1852, 2002.
- [7] S. Li and X. Zheng, "On the security of an image encryption method," *Proc. IEEE Int. Conference on Image Processing (ICIP'2002)*, vol. 2, pp. 925-928, 2002.
- [8] Y. Tanada, "General Solution for Orthogonal Periodic Real-Number Sequence," in Japanese, *IEICE Trans. Vol.J68-A, No.5*, pp.451-457, 1986.
- [9] S.Matsufuji, Y. Tanada, A. Fujimoto, N.Suehiro, "On Perfect Arrays," *Proceedings of IEEE ISIT 2003*, pp.433, 2003.