A New Image Encryption Arithmetic Based on a Three-dimensional Map

Feng Huang, Chao Wang, Shijun Li
Department of Electrical and Information Engineering
Hunan Institute of Engineering
Xiangtan, P.R.China
huangfeng@hit.edu.cn

***Abstract*—The paper proposes a new image encryption arithmetic. Firstly, the paper introduces a new two-dimensional map. A square image is divided into two isosceles triangles according diagonal. Each pixel in a column is inserted to the adjacent column which utilizes the difference of the number of pixel of two adjacent columns. Then the plain image can be stretched to a line of pixels. The line is fold over to a new square image which size is same as the plain image. Secondly, the map is further extended to the three-dimensional one. The algorithm of the map is formulated, a method for key generation is designed and the security of the proposed image encryption arithmetic is analyzed. The simulation results show that the proposed encryption arithmetic is valid.**

***Keywords*—image encryption, chaos, chaotic map, security**

I. INTRODUCTION

More and more images are transmitted over the Internet with the fast developments of information technology. How to protect images has increasingly become an important issue. The encryption is an important tool to protect important information from attackers. But for some intrinsic features of images, such as bulk data capacity and high correlation among pixels, prevalent encryption technology such as DES and RSA, and other algorithms [1] are not absolutely fit to image encryption [2].

Chaotic maps have been used in cryptography in recent years. Matthews firstly suggested using a logistic map for generating a sequence of pseudo-random numbers to encrypt information [3]. For chaotic maps has many characteristics can be connected with the "confusion" and "diffusion" property in cryptography, chaotic maps are well applied in cryptography [4]. In fact the idea of using chaos for encryption can be traced to the classical Shannon's paper [5] where the basic stretch-and-fold mechanism of chaos was mentioned which can form good mixing transformations for encryption.

In chaotic cryptography, there are two design methods. One is based on chaos synchronization which is realized in analog circuits. The other method of chaotic cryptography is realized in digital computers. There are some typical chaotic maps such as the Cat map and Baker map can be used in image encryption. In [6] a symmetric image encryption scheme is proposed which is based on three-dimensional chaotic Cat maps. The scheme employs the Cat maps to shuffle the positions of image pixels and uses logistic map to confuse the relationship between the cipher-image and the plain-image. In [7] it is shown that the permutations induced by the Baker map behave as typical random permutations. The cipher has good diffusion properties with respect to the plain-text and the key. But the Baker map does not have simple formula and the key is limited by size of image. In [8] some functions were proposed which include changing the gray level values of the pixels, transposing the pixel by shifting and binding a password were introduced to increase the encryption strength. In [9] a new image encryption scheme was constructed based on the extended three-dimensional chaotic Baker map.

This paper firstly proposes a new two-dimensional map, which a process of stretch-and-fold which Shannon suggested in [5]. Then the map is extended to three-dimensions. The algorithm of the map is formulated, a method for key generation is designed and the security of the proposed image encryption. The simulation results show that the proposed encryption arithmetic is valid.

II. THE INTRODUCTION OF THE TWO-DIMENSIONAL MAP

A. The principle of the map

Assume that a square image to be encrypted consists of $N \times N$ pixels with L gray levels. The new map utilizes an important characteristic of images, which each pixel of image can be inserted between the adjacent two pixels.

It can encrypt images by processing image stretch-and-fold. Firstly a square image is divided into two isosceles triangles according diagonal. Utilizing the difference of the pixel numbers of two adjacent columns of the triangles, each pixel in a column is inserted to the adjacent column. Then, the plain image can be stretched to a line. Finally the line is fold over to a new square image which size is same as the plain image.

The principle of the map is shown in Fig. 1. The map is divided into two sub-maps: the left map and the right map, as shown in Fig.1 respectively. The left map means that an $N \times N$ square image is first mapped to a line of N^2 pixels, then the line are further mapped to another $N \times N$ square image. As shown in Fig. 1 (b), the right map is the symmetric to the left one.

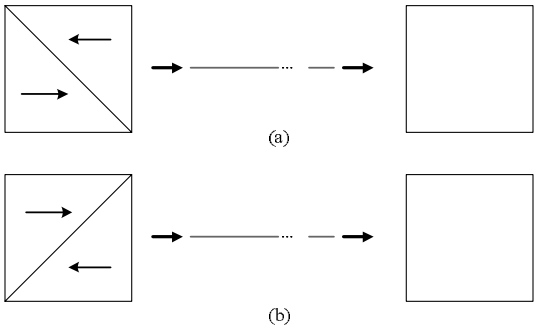


Figure 1. The principle of the map (a) the left map; (b) the right map.

In order to explain the map more clearly, one example is given here. The image has 4×4 pixels, that is N=4. The process of the map is shown in Fig. 2. The left map and the right map are depicted in Fig. 2(a) and (b) respectively. It can be seen that pixels of each column of an image can be inserted into pixels of each horizon.

For example, in Fig. 2, firstly a square image is divided into two isosceles triangles according diagonal. Utilizing the difference of the pixel numbers of two adjacent columns of the triangles, each pixel in a column is inserted to the adjacent column. The pixel (3,3) can be inserted before the pixel (2,2), pixel (2,3) can be inserted between pixels (2,2) and (1,2), pixel (1,3) can be inserted between pixels (1,2) and (0,2) and so on. So the pixels join to a line: (3,3), (2,2), (2,3), (1,2), (1,3), (0,2), … . Then it is fold over to a new square image whose size is same as the plain-image. the right map is the symmetric to the left map

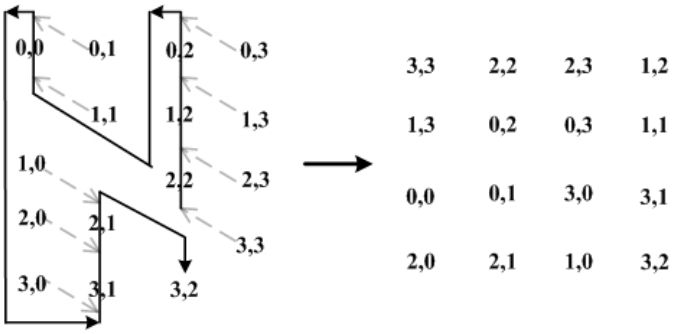


Figure 2. The process of the left map with a 4×4 image.

B. The algorithm of the map

Assume that a square image is N×N, where N is an integer. As shown in Fig. 1(a), the left map can be described respectively with the following formulas:

$$l[\frac{(N+j+2)(N-j-1)}{2}+2(j-i)]=A(i,j) \quad (1a)$$

where $j\geq i$, N-j is the odd number, i=0,1,…,N-1, j=0,1,…,N-1.

$$l[\frac{(N+j+3)(N-j-2)}{2}+2(j-i)+1]=A(i,j) \quad (1b)$$

where $j\geq i$, N-j is the even number, i=0,1,…,N-1, j=0,1,…,N-1.

$$l[\frac{N^2+N+(2N-j-1)\times j}{2}+2(N-i-1)]=A(i,j) \quad (1c)$$

where $j<i$, j is the even number, i=0,1,…,N-1, j=0,2,…,N-1.

$$l[\frac{N^2+N+(2N-j)\times(j-1)}{2}+2(N-i)-1]=A(i,j) \quad (1d)$$

where $j<i$, j is the odd number, i=0,1,…,N-1, j=1,3,…,N-1.

Here $A(i, j)$ is the matrix of a square image, in which each element corresponds to a gray level values of the pixel (i, j), $l(i)$ is a one-dimensional line mapped from A.

As shown in Fig. 1(b), based on the formulas of the left map, the right map can be described respectively with the following formulas:

$$l[\frac{(N+j+2)(N-j-1)}{2}+2(j-i)]=A(i,N-1-j) \quad (2a)$$

where $j\geq i$, N-j is the odd number, i=0,1,…,N-1, j=0,1,…,N-1

$$l[\frac{(N+j+3)(N-j-2)}{2}+2(j-i)+1]=A(i,N-1-j) \quad (2b)$$

where $j\geq i$, N-j is the even number, i=0,1,…,N-1, j=0,1,…,N-1

$$l[\frac{N^2+N+(2N-j-1)\times j}{2}+2(N-i-1)]=A(i,N-1-j) \quad (2c)$$

where $j<i$, j is the even number, i=0,1,…,N-1, j=0,2,…,N-1

$$l[\frac{N^2+N+(2N-j)\times(j-1)}{2}+2(N-i)-1]=A(i,N-1-j) \quad (2d)$$

where $j<i$, j is the odd number, i=0,1,…,N-1, j=1,3,…,N-1

In the preceding subsections, an N×N square image, A, is mapped to a line of N^2 pixels l with either the left map or the right map, as shown in Fig. 1. Now, the line of N^2 pixels l is further mapped to a same size N×N square image, B.

The map from line l to image B is described with the following formula:

$$B(i,j)=l(i\times N+j) \quad (3)$$

where i=0,1,…,N-1, j=0,1,…,N-1.

III. EXTENSION TO THREE-DIMENSIONS

The square image consists of N×N pixels with L gray levels. The gray level value of each pixel A is in decimal which can be expressed as a binary number.

$$A=\sum K_n 2^n \qquad n=0,1,\ \cdots,\ log_2 L-1 \quad (4)$$

For example, if L=256, then $log_2 L-1=7$,

$$A=\sum K_i 2^i = K_0 2^0 + K_1 2^1 + K_2 2^2 + K_3 2^3 + K_4 2^4 + K_5 2^5 + K_6 2^6 + K_7 2^7$$

So we can split the plain-image into eight layers. As shown in Fig. 3, the first layer is composed by the lowest coefficients of the binary number of image values; the second layer is composed by the second coefficients…and so on.

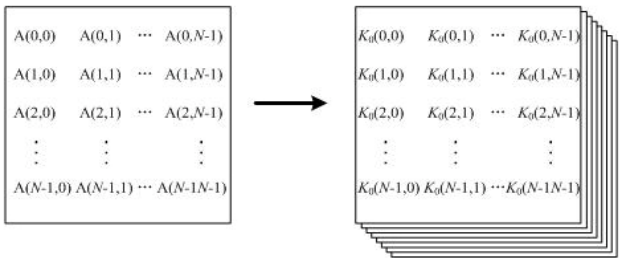


Figure 3. Delamination of image.

Then it can use the map to confuse the each layer of image. From (1a) and (1b) it can be educed the formulas of three-dimensional map respectively. The formulas of the left map are

$$l[\frac{(N+j+2)(N-j-1)}{2}+2(j-i)]=K_n(i,j) \quad (5a)$$

where $j\geq i$, N-j is the odd number, i=0,1,…,N-1, j=0,1,…,N-1, n=0,1,…,log_2L-1.

$$l[\frac{(N+j+3)(N-j-2)}{2}+2(j-i)+1]=K_n(i,j) \quad (5b)$$

where $j\geq i$, N-j is the even number, i=0,1,…,N-1, j=0,1,…,N-1, n=0,1,…,log_2L-1.

$$l[\frac{N^2+N+(2N-j-1)\times j}{2}+2(N-i-1)]=K_n(i,j) \quad (5c)$$

where $j<i$, j is the even number, i=0,1,…,N-1, j=0,2,…,N-1, n=0,1,…,log_2L-1.

$$l[\frac{N^2+N+(2N-j)\times(j-1)}{2}+2(N-i)-1]=K_n(i,j) \quad (5d)$$

where $j<i$, j is the odd number, i=0,1,…,N-1, j=1,3,…,N-1, n=0,1,…,log_2L-1.

The formulas of the right map are

$$l[\frac{(N+j+2)(N-j-1)}{2}+2(j-i)]=K_n(i,N-1-j) \quad (6a)$$

where $j\geq i$, N-j is the odd number, i=0,1,…,N-1, j=0,1,…,N-1, n=0,1,…,log_2L-1.

$$l[\frac{(N+j+3)(N-j-2)}{2}+2(j-i)+1]=K_n(i,N-1-j) \quad (6b)$$

where $j\geq i$, N-j is the even number, i=0,1,…,N-1, j=0,1,…,N-1, n=0,1,…,log_2L-1.

$$l[\frac{N^2+N+(2N-j-1)\times j}{2}+2(N-i-1)]=K_n(i,N-1-j) \quad (6c)$$

where $j<i$, j is the even number, i=0,1,…,N-1, j=0,2,…,N-1, n=0,1,…,log_2L-1.

$$l[\frac{N^2+N+(2N-j)\times(j-1)}{2}+2(N-i)-1]=K_n(i,N-1-j) \quad (6d)$$

where $j<i$, j is the odd number, i=0,1,…,N-1, j=1,3,…,N-1, n=0,1,…,log_2L-1.

The formulas of the map from a line to a square image is

$$K_n'(i,j)=l(i\times N+j) \quad (7)$$

where i=0,1,…,N-1, j=1,3,…,N-1, n=0,1,…,log_2L-1.

IV. A NEW IMAGE ENCRYPTION ARITHMETIC

A. Image Encryption

Because image encryption can be achieved by pixels permutation the map can be used for image encryption. Since the map is divided into the left map and the right map, the numbers of the left map and the right map can be used as secret keys in image encryption. If the key is in decimal, from the least significant digit to the most significant digit, each digit (0-9) corresponds to the iteration number of the left map and the right map alternately. For example, a secret key "32" means that a plain-image is mapped to another ciphered-image through 3 iterations of the left map, 2 iterations of the right map as shown in Fig. 1. In another case where the key is represented in binary digit, from the least significant bit to the most significant bit, every four bits (0-15) correspond to the iteration numbers of the left map and the right map alternately.

When the map is extended to be three-dimensional map, the keys can be composed of the iteration number of a set of layers. For example, if L=256, a secret key "1234" means that in 1,3,5,7 layers of the plain-images are mapped to ciphered-images through 1 iteration of the left map and 2 iterations of the right map, in 2,4,6,8 layers the images are mapped to ciphered-images through 3 iterations of the left map and 4 iterations of the right map and so on. That means the $4n$+1 bits in key are the iteration numbers of the left map for 1,3,5,7 layers, the $4n$+2 bits in key are the iteration numbers of the right map for 1,3,5,7 layers, the $4n$+3 bits in key are the iteration number of the left map for 2,4,6,8 layers and the $4n$+4 bits in key are the iteration number of the left map for 2,4,6,8 layers, where n=0,1,2….

The process of image process is shown in Fig. 4. Suppose the $N\times N$ plain-image with L gray levels is A. The steps of the image encryption based on the map can be described as follows:

Step 1: Extend the plain-image A to a three-dimensional image K_n.

Step 2: According to the requirement of security, design a key for image encryption. Permutation of K_n by the key respectively. ((5a)- (5d) for the left map, (6a)- (6d) for the right map).

Step 3: The line of pixels l is mapped to a same size square image K_n' ((7)).

Step 4: Combination all layers. For good diffusion properties the encryption can add a diffusion mechanism.

In step 4, it can design a method to reconstruct the image. The type of method can also be used as a key. At the same time the parameters of the diffusion mechanism usually is a part of a key.

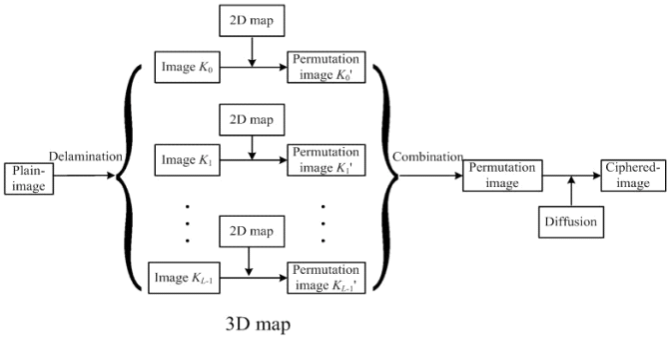


Figure 4. The process of image encryption.

B. *Image Decryption*

Decryption of image is the inverse process of the encryption of image. So the new image encryption is the symmetric cipher system.

Suppose the $N \times N$ ciphered-image with L gray levels is B. The steps of the image decryption based on the map can be described as follows:

Step 1: Decipher the diffusion mechanism.

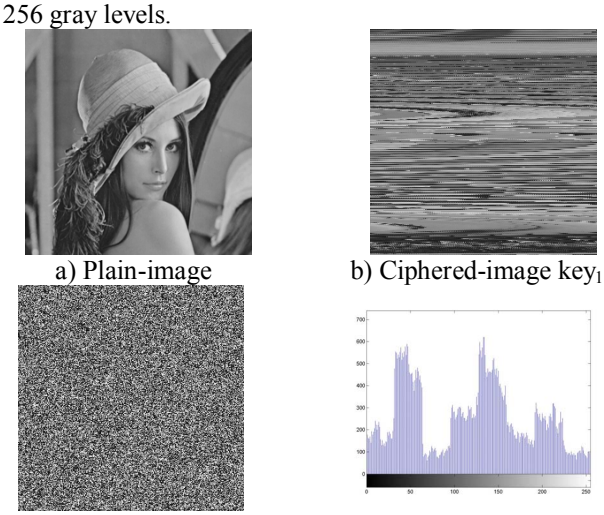
Step 2: Extend the ciphered-image B to a three-dimensional image K_n'.

Step 3: Use the key for image decryption to permute K_n' to K_n respectively.

Step 4: Combination all layers to an image.

V. A NEW IMAGE ENCRYPTION ARITHMETIC

An image encryption based on the three-dimensional map is carried out with diffusion mechanism. The plain-image and ciphered-image are shown in Fig. 5. It has 256×256 pixels with 256 gray levels.



a) Plain-image b) Ciphered-image key_1

c) Ciphered-image of key_2 d) Histogram of key_2

Figure 5. Plain-image and ciphered-image.

The plain-image is encrypted using the map by the keys: key_1= "0101" and key_2="1234" respectively. It can be seen that the plain-image has been encrypted.

A. *Key space*

Since the length of the key of the map has no limit, its key space can be calculated according to the length of the key. Suppose the keys are represented in binary bits. The relationship between the key space size and the key length is shown in TABLE I.

TABLE I. KEY SPACE SIZE VS. KEY LENGTH

Key length (bits)	64	128	256
Key space size	1.84×10^{19}	3.4×10^{38}	1.16×10^{77}

B. *Statistical analysis*

The new image encryption arithmetic has very good confusion properties without any diffusion mechanism. Correlation of two adjacent pixels in the ciphered-image can see in [9]:

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{8}$$

where x and y are values of two adjacent pixels in the image, and

$$\mathrm{cov}(x, y) = \frac{1}{N}\sum_{i=1}^{N} |(x_i - E(x))(y_i - E(y))|$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \,, E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \,.$$

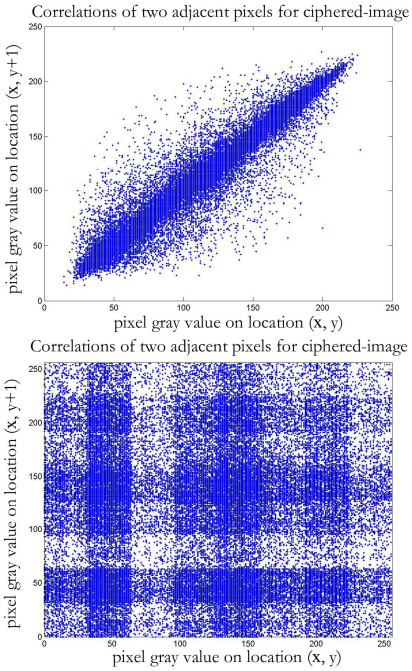


Figure 6. Correlations of two adjacent pixels in the plain-image and the ciphered-image.

Fig.6 shows the correlations of two horizontal adjacent pixels in the plain-image and the ciphered-image: the correlation coefficients are 0.9442 and 0.0024. Similar results for diagonal and vertical directions were obtained and shown in TABLE II.

TABLE II. CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS

	Plain-Image	Ciphered-Image
horizontal	0.9442	0.0024
vertical	0.9711	0.0579
diagonal	0.9187	0.0049

VI. CONCLUSION

In this paper, a new two-dimensional map is proposed at first, then extension to three-dimensional map and composing with a diffusion mechanism. The paper formulates the algorithm of the three-dimensional map. A new image encryption arithmetic based on the three-dimensional map is proposed. The arithmetic designs a method of key generation and utilizes the map to shuffle the positions of image pixels. The experimental tests have been carried out and the results show the efficiency of the arithmetic.

REFERENCES

[1] B. Schneier, Applied Cryptography – protocols, algorithms, and source code in C, 2rd ed., John Wiley & Sons, Inc., New York 1996.

[2] C. C. Chang, M. S. Hwang, T. S. Chen, "A new encryption algorithm for image cryptosystems," The Journal of System and Software, vol. 58, no. 7, pp. 83-91, 2001.

[3] R. Matthews, "On the derivation of a 'chaotic' encryption algorithm," Cryptologia, vol. 13, no. 1, pp.29-42, 1989.

[4] T. Habutsu, Y. Nishio, I. Sasase,and S. Mori, "A secret key cryptosystem by iterating a chaotic map," In Advance in Cryptology-EuroCrypt'91, Lecture Notes in Computer Science, Spinger-Verlag, Berlin, vol.0547, pp.127-140, 1991.

[5] C. E. Shannon, "Communication theory of secrecy systems," The Bell System Technical Journal, vol. 28, no.4, pp.656-715, 1949.

[6] G. Chen, Y. Mao, C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons and Fractals, vol.21, pp.749-761, 2004.

[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," Int J Bifurcat Chaos, vol.8, no.6, pp.1259-1284, 1998.

[8] M. Salleh, S. Ibrahim and I. F. Isnin, "Enhanced chaotic image encryption algorithm based on Baker's map," IEEE Conf. Circuits and Syst, vol.2, pp.508-511, 2003.

[9] Y. Mao, G. Chen and S. Lian, "A novel fast image encryption scheme based on the 3D chaotic Baker map," Int J Bifurcat Chaos, vol.14, no.10, pp.3613-3624, 2004.