Digital image scrambling*

DING Wei(丁 玮)[1], YAN Weiqi (闫伟齐)[1**] and QI Dongxu(齐东旭)[1,2]

1. CAD Laboratory, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China

2. CAD Research Center, North China University of Technology, Beijing 100041, China

Received September 18, 2000; revised November 1, 2000

Abstract The purpose of digital image scrambling is to transform a given digital image into a rather scrambled one so as to make it difficult for other people to find out the true meaning of the scrambled image. This paper comes up with a certain number of approaches to scrambling digital images, which, when thus processed, cannot be reconstructed in a common way. As a result, the original image is encrypted and protected.

Keywords: **digital image scrambling, cryptography, magic square, gray code, Conway's game.**

Digital image scrambling can be used in both pre-processing and post-processing of digital image hiding, as well as in digital image encryption. Its main purpose is to make a given image so scrambled that no one is able to find out the true meaning of the image by using human visual system (HVS) or computer system. This technology can be implemented in a spatial domain (such as the color domain or position domain), or in a frequency domain of a given digital image.

Compared with the object of cryptography, a digital image contains a larger amount of data, or in other words, it needs a larger space for plain texts and cipher texts[1~7]. The most important thing is that the self-correlation of the digital image is represented in two directions perpendicular to each other, while the self-correlation of a text, such as one-dimensional signal sequence, is rather difficult to be obtained. With these two features of the digital image in mind, attackers may try to find a fixed frequency of each pixel, but, since different images have different histograms, it will be very difficult for them to find it out. Then how can we establish a map of conversion between the original image and disguised one?

In Ref.[4], a brief introduction was made to some of the existing cryptographic mechanisms of TV analog images, including random row inverse scrambling, row shifting scrambling, row substitution scrambling, row cycle scrambling, row component cropping scrambling, pixel scrambling and so on. Shamir, a cryptographic expert, proposed a scrambling technique based on space filling curves[8]. In addition, some work has been done on the security of TV signals[9~11]. In the following sections, we will introduce some digital image scrambling techniques, which can be applied alternately. Using different parameters and pseudo random factors, we can obtain distinctive results, and, if we use them crosswise, we will improve the security of digital images.

* Project supported by the National Natural Science Foundation of China (Grand No. 69873001) and "973" Project (Grand No. G1998030608).

** Corresponding author; E-mail: yanweiqi@263.net

1 Digital image scrambling based on magic square

Magic square is an old mathematical problem, whose mention can be found in some ancient books. Because of its splendid properties and fantastic structure it has attracted the attention of numerous scholars[11,12].

1.1 Standard magic square

The standard magic square is an n order matrix with natural numbers $1,2,\cdots,n^2$ as its elements:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

which satisfies the following equations:

$$\sum_{j=1}^{n} a_{ij} = c(i = 1,2,\cdots,n), \quad \sum_{i=1}^{n} a_{ij} = c(j = 1,2,\cdots,n),$$

$$\sum_{i=1}^{n} a_{ii} = c, \quad \sum_{j+1=n+1} a_{ij} = c, \tag{1}$$

where $$c = \frac{n^2(n^2+1)}{2}.$$

The matrix A is referred to as the standard magic square.

1.2 Digital image scrambling based on magic square

Let the nth-order matrix of a given digital image be denoted by B. For a fixed nth-order magic square A, we construct a map between B and A. Then we establish a sequence of operations in A: move element 1 to the position of element 2, move element 2 to the position of element 3, generally, element $m \in \{1,2\cdots,n^2-1\}$ to the position of element $m+1$, and element $m = n^2$ to the position of element 1. After this kind of moving, the magic square A changes to a matrix A_1, denoted by $A_1 = EA$, where E is an operator; for A_1, we can obtain $A_2 = EA_1$ by repeating the above procedure, and then, similarity, $A_3 = EA_2$, $A_4 = EA_3$, etc. This is called a sequence of scrambling transformation. As a result, we will have $A_{n^2} = A$ after n^2 steps of iteration.

For a digital image matrix B, taking into account the correspondence of elements between B and A, we move elements (gray-scale values of each pixel) of B to corresponding position to obtain a new digital image matrix B_1, denoted by $B_1 = EB$, while transforming A to A_1. Similarly, we can have $B_m = E^m B$. It has been proven that the cycle of this kind of digital image scrambling is

$$T = n^2. \tag{2}$$

The experimental result of image scrambling based on magic square is shown in Figure 1.

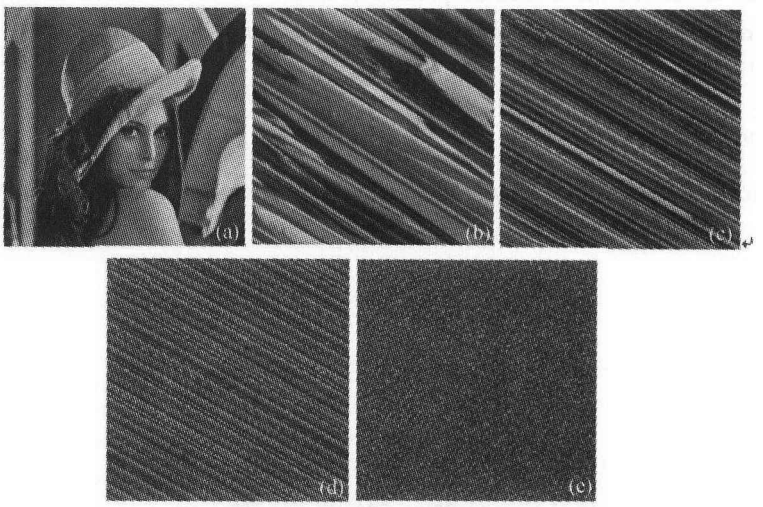

Fig. 1 Digital image scrambling based on magic square. (a) Original image; (b ~ e) the iterated results after 1 ~ 4 step iteration, respectively.

2 Digital image scrambling based on Gray code transformation

Gray code is an integral mapping, and Gray code transformation is a kind of binary representation of digital data, which can be used for error correction and verification of binary data[12,13]. In this section, we will give the definition of Gray code transformation in matrix format, and discuss how to generalize it, and finally, how to use Gray code transformation to scramble digital image.

2.1 On Gray code transformation

For any given non-negative integer n, its binary format can be written as $n = (n_p n_{p-1} \cdots n_1 n_0)_2$, where $n_j \in \{0,1\}$. From such additions: $0 \oplus 1 = 1 \oplus 0 = 1$, $0 \oplus 0 = 1 \oplus 1 = 0$, the following transformation is given:

$$g_j = n_{j+1} \oplus n_j; \qquad j = 0,1,\cdots,p,\ g = (g_p g_{p-1} \cdots g_1 g_0)_2.$$

Thus we have $g = G(n)$. We call G the Gray transformation, and g the relative Gray code of n. In Table 1, we list the results of Gray transformation with respect to the orders of 0 ~ 15.

Table 1 Gray transform results

Transformation	Order of pixel n															
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$(n)_2$	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111
$G(n)_2$	0	1	11	10	110	111	101	100	1100	1101	1111	1110	1010	1011	1001	1000
$G(n)$	0	1	3	2	6	7	5	4	12	13	15	14	10	11	9	8

Gray transformation has a hierarchy of fine stratification, thus assuming a structure of self-similarities. In fact, Gray transformation can be expressed in the following matrix format.

Theorem 1. $I_1 = \tilde{I}_1 = 1$, $I_{2^k} = \begin{pmatrix} I_{2^{k-1}} & \\ & \tilde{I}_{2^{k-1}} \end{pmatrix}$. Then

$$\tilde{I}_{2^k} = \begin{pmatrix} & I_{2^{k-1}} \\ \tilde{I}_{2^{k-1}} & \end{pmatrix}, \quad k = 1,2,\cdots, \tag{3}$$

where matrix I_{2^k} and $\tilde{I}_{2^k}$ are block diagonal matrix and anti-diagonal matrix, respectively, and each sub-block matrix I_{2^k} and $\tilde{I}_{2^k}$ can be divided into a half order diagonal matrix and a half order anti-diagonal matrix.

Figure 2 (a) gives $g = G(n)$ represented in the rectangular coordinates system, and Fig. 2(b) the matrix I_{32}, where the black stands for 1, and the white stands for 0, and the solid line represents the hierarchy of fine stratification and subdivision structures. The curve in Fig. 2 (c) is obtained from the matrix expressions of Fig. 2 (b), and shows the self-similarity.

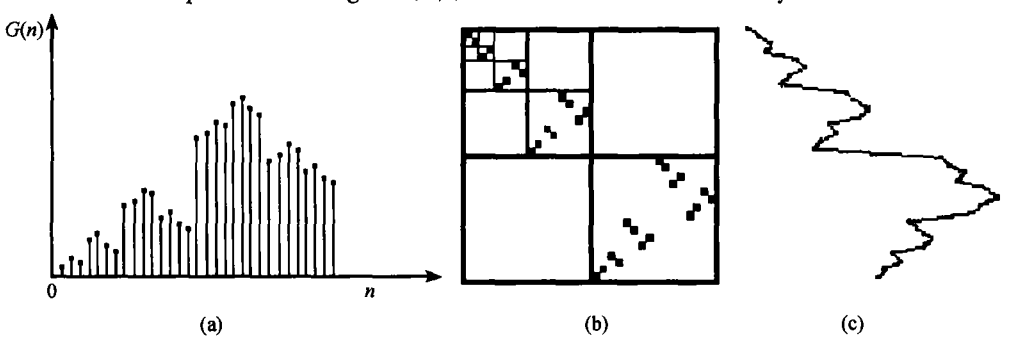

Fig. 2 Self-similarity structure of Gray transformation.

Theorem 2. Suppose the Gray code of nonnegative integer n is $G(n)$, and let $G^0(n) = n$, $G^k(n) = G \circ G^{k-1}(n)$, $k = 0,1,2,\cdots$. Then, for a positive integer n, $2^{k-1} \leqslant n \leqslant 2^k - 1$, we have $G^{2^k}(n) = n$.

Proof. It can be proven using the definition of Gray code and recursive Relation (3).

From Theorem 2 we know that, for any nonnegative integer n, $n \leqslant 2^k - 1$, we have $G^{2^k}(n) = n$. Thus, for any image with gray-scale level of 2^k, if a continuous transformation process is performed for its gray level, we can finally reproduce the accurate image.

Now we will expand Gray transformation into a series of other transformations, which can be represented in the following matrix forms:

$$E_{2^k} = \begin{pmatrix} & E_{2^{k-1}} \\ \tilde{E}_{2^{k-1}} & \end{pmatrix}, \quad \tilde{E}_{2^k} = \begin{pmatrix} E_{2^{k-1}} & \\ & \tilde{E}_{2^{k-1}} \end{pmatrix}, \quad k = 1,2,\cdots \tag{4}$$

$$E_1 = \tilde{E}_1 = 1;$$

$$F_{2^k} = \begin{pmatrix} F_{2^{k-1}} & \\ & \tilde{F}_{2^{k-1}} \end{pmatrix}, \quad \tilde{F}_{2^k} = \begin{pmatrix} & \tilde{F}_{2^{k-1}} \\ F_{2^{k-1}} & \end{pmatrix}, \quad k = 1,2,\cdots \tag{5}$$

$$F_1 = \tilde{F}_1 = 1;$$

$$G_{2^k} = \begin{pmatrix} & G_{2^{k-1}} \\ \tilde{G}_{2^{k-1}} & \end{pmatrix}, \quad \tilde{G}_{2^k} = \begin{pmatrix} \tilde{G}_{2^{k-1}} & \\ & G_{2^{k-1}} \end{pmatrix}, \quad k = 1,2,\cdots \tag{6}$$

$$G_1 = \tilde{G}_1 = 1.$$

Other transformations can be obtained by commuting the position of $I_{2^{k-1}}(E_{2^{k-1}}, F_{2^{k-1}}, G_{2^{k-1}})$ and $\tilde{I}_{2^{k-1}}(\tilde{E}_{2^{k-1}}, \tilde{F}_{2^{k-1}}, \tilde{G}_{2^{k-1}})$ in Expressions (3) ~ (6).

2.2 Digital image scrambling based on Gray code transformation

Based on the above-mentioned Gray transformation matrix, it is easy to present a kind of digital image scrambling method, which can act not only on the position space of the digital image, but also on the color space or frequency space of the image. Fig. 3 gives the results of the image scrambling using Expressions (3) ~ (6).

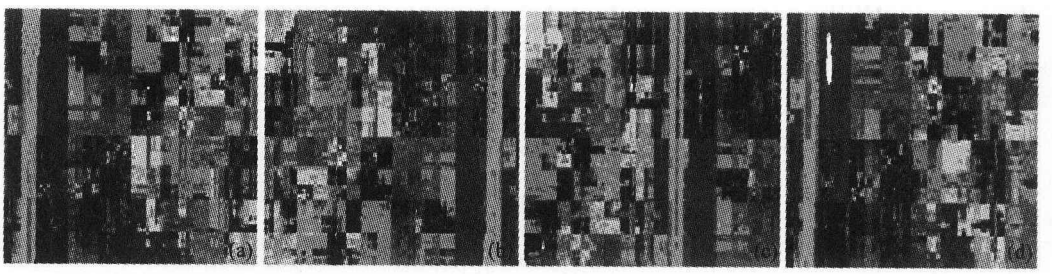

Fig. 3 Digital image scrambling based on generalized Gray transformation. (a ~ d) The scrambling images using Expressions (3) ~ (6) respectively.

3 Digital image scrambling based on Conway's game

3.1 Conway's game

Conway's game is a special image matrix transformation[12,14]. Around the 1970's, British mathematician John Conway and his students established adequate rules after repetitious experiments[13]. Suppose there is a planar grid, in which each node represents a life cell. If it is filled with black color, the cell is believed to be alive; if it is filled with white color, the cell is considered to be dead. Suppose the planar grid is infinitely large (in fact, the upper and bottom, left and right boundaries of a finite planar grid can be linked up), then each cell will have 8 neighbors, and its state will affect the state of the surrounded cell. For the given initial states of all the cells of the planar grid, we should use the following rules.

(i) If the surrounded cell has 3 neighbors of black state, then, no matter what its initial state was, it will be changed to black.

(ii) If the cell happens to have 2 neighbors of black state, it will maintain its initial state unchanged.

(iii) Otherwise, no matter what its initial state was like, it will be changed to white.

If the planar grid is seen as a 1-bit image, then Conway's game will be a kind of special image matrix transformation. Fig. 4 shows a diagram of the multiplying process of Conway's game.

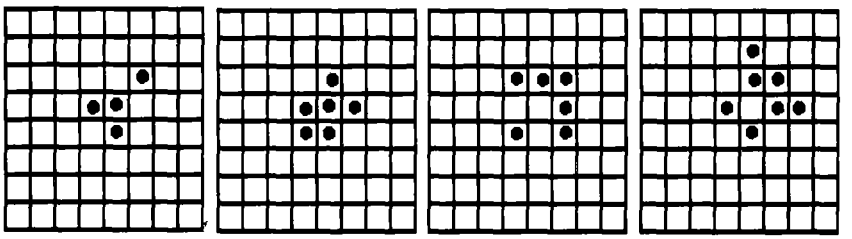

Fig. 4 Diagram of the multiplying course of Conway's game. (a) Initial state; (b) ~ (d) after 1 ~ 3 iteration, respectively.

3.2 Digital image scrambling based on Conway's game

Suppose that set Z represents the alive state of all the cells on the planar grid, i.e. the set of all the cells on the planar grid, set S_0 the initial state of these alive cells, i.e. the set of the cells in the initial state that is alive, and set S_i represents the set of the cells that become alive after the i-th iteration, where $i > 0$. Let set $S^{(i)} = \underset{0 \leqslant j \leqslant i}{U} S_j$ represent all the cells that became alive after i iteration. Our algorithm can be defined as follows.

(i) Establish the correspondence between the cells and pixels of a given image.

(ii) For the initial state S_0 of a planar grid, arrange, in order of scan lines, the pixels corresponding to the alive cells into the space of the coordinates of scrambled image.

(iii) When reaching the i-th step of iteration, arrange, in order of scan lines, the pixels corresponding to the alive cells in the set $S^{(i)} - S^{(i-1)}$ into the space of the coordinates of scrambled image.

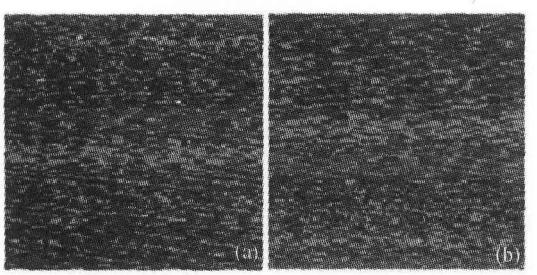

Fig. 5 Digital image scrambling based on Conway's game.

(iv) If the iteration stops at the n-th step, arrange, in order of scan lines, the pixels corresponding to the cells in the set $Z - S^{(n)}$ into the space of the coordinates of scrambled image.

The initial state S_0 of the planar grid can be generated by pseudo random numbers. Fig. 5 shows different scrambled results corresponding to

different initial states. It shows that different initial state will affect scrambling result.

4 Conclusion

The algorithms mentioned above can scramble a given digital image to a certain extent, i.e. can transform an initial image into a "scrambled" or "confused" image. Obviously, these algorithms can be used in combination, and we can set different parameters, or even use a pseudo random number to control the implementation of the algorithms. All these will bring about great difficulties to a potential attacker, even if he knows the algorithm, he has no way to recover the image if he does not know parameters of the algorithm. From this viewpoint, the scrambling technology can be regarded as an encrypting means for digital images with those parameters as secret keys. On the other hand, scrambling techniques can also be used for encryption of one-dimensional digital signals or three-dimensional data, as we can arrange those different dimensional data onto a two-dimensional plane, and extend the algorithms to the data of a specific category.

References

1 Schneier, B. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd. ed., New York: John Wiley & Sons, 1996.
2 Rhce, M. Y. Cryptography and Secure Communications, New York: McGraw-Hill, 1994.
3 Koblitz, N. A Course in Number and Theory and Cryptography, Berlin-Heidelberg: Springer-Verlag, 1994.
4 Shen, S.Y. Modern Cryptography(in Chinese), Guangxi: Guangxi Normal University Press, 1998.
5 Wang, Y. M. et al. Cryptography-Foundation and Application (in Chinese), Xi'an: Xi Dian Press. 1990.
6 Lu, K. C. Computer Cryptography-Data Security and Safety in Computer Networks (in Chinese), Beijing: Tsinghua University Press, 1998.
7 Salomaa, A. Public-key Cryptography, Berlin-Heidelberg: Springer-Verlag,1999.
8 Matias, Y. et al. A video scrambling technique based on space filling curves. In: Proceedings of CRYPTO'87 (Advances in Cryptology), Lect ure Notes in Computer Sciences, Vol. 293, Berlin-Heidelberg: Springer-Verlag, 1988. 389.
9 Zhang, P. S. et al. A scheme for image encryption. Journal of Communication (in Chinese), 1984, 5(3): 85.
10 Zhou, T. H. Discussion about image encryption. Communication Security (in Chinese), 1986, 22 and 23: 93.
11 Xu, G. F. et al. Principle and Methods for Construct Pure Magic Square(in Chinese), Xi'an: Xi'an Jiaotong University Press, 1994.
12 Qi, D. X. Fractal and Its Computer Generation (in Chinese), Beijing: Science Press, 1994.
13 Ding, W. et al. Digital image scrambling technology based on Gray code. In: Proceedings of the 6th International Conference on Computer Aided Design & Computer Graphics, Shanghai: Wen Hui Publishers, 1999, 900.
14 Berlekamp, E. et al. Winning Ways for Your Mathematical Plays, Cambridge: Academic Press, 1982.