Matrix transformation of digital image and its periodicity *

QI Dongxu(齐东旭)[1], WANG Daoshun (王道顺)[2]** and YANG Dilian (杨地莲)[2]

1. CAD Research Center, North China University of Technology, Beijing 100041, China and CAD Laboratory, Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080, China
2. College of Mathematics, Sichuan University, Chengdu 610064, China

Received October 8, 2000; revised November 3, 2000

Abstract The periodicity of a general matrix modular transformation is discussed, and a simple proof of a sufficient and necessary condition that a matrix transformation has periodicity is given. Using a block matrix method, the higher dimensional transformation and its inverse are studied, and a simple algorithm for calculating their periods is put forward. The security of n-dimensional Arnold transformation and its inverse is also discussed. The results show that the two transformations are applicable in scrambling and recovering images.

Keywords: digital image, scrambling transformation, Arnold transformation, periodicity, matrix transformation, security.

There are many ways for scrambling a digital image. Different encoders are used for different requirements. Arnold transformation is an interesting one with good transformation periodicity, which, as the encoder and decoder, can control randomly the number of the transformations in the image transportation.

Using the properties of Arnold transformation, some good effects on scrambling images have been achieved. The application of Arnold transformation[1] in the covering of image information has been discussed in Refs. [2 ~ 9] and Ding's Ph.D dissertation1). However, the classical Arnold transformation has only four parameters which are not sufficient for data-cryptoguard. The two-dimensional Arnold transformation has been extended to higher dimensional by Zou et al.2). It is valuable to generalize Arnold transformation in view of mathematics. Enlightened by the idea of Arnold transformation, Qi et al.[9] have studied the higher dimensional transformation (module operation) and have given a sufficient and necessary condition that a matrix transformation has periodicity. They have also discussed the function of the scrambling transformation in the gray level space of a digital image.

Can we simplify the proof of the sufficient and necessary condition for the matrix transformation in Ref. [9]? Do a higher dimensional transformation and its inverse have periodicity or not? Can we present a simple algorithm to calculate the periods of a matrix transformation? These problems remain unsolved.

---

* Project supported by the National Natural Science Foundation of China (Grant No. 19671003, 68973001) and the National 973 Program (Grant No. G1998030608).

** Corresponding author, E-mail: daoshun@263.net.

1) Ding, W. Research on digital image information security algorithms, Ph. D Dissertation, Institute of Computational Technology, Chinese Academy Sciences, 2000, 6.

2) Zou, J.C. et al. The Arnold transformation of digital image with three-dimensional transformation and its periodicity. ChinaGraph'2000, The 3rd Computer Graphics Conference of China, Hangzhou, 2000, 8: 163.

This paper will address them.

It should be emphasized that the results of higher dimensional Arnold inverse transformation are different from those presented in Refs. [2 ~ 9] and Ding's Ph.D dissertation. The algorithm put forward in this paper is a new method. The inverse transformation gives a new method of scrambling images. On the other hand, a new way for restoring the scrambled images has been found.

1 Condition for a matrix transformation to have periodicity

A digital image can be regarded as a relevant numerical matrix, each element of which corresponds to a pixel of the digital image. All kinds of transformations of the digital image can be realized by changing the positions of the elements in the matrix or the color value of image (RGB for short). A digital image is not restored after a series of the same transformations until the numerical matrix corresponding to the digital image has periodicity. Therefore, the study on periodicity of matrix transformation is important for encoding and decoding a digital image. In this section, we will concentrate on the periodicity of the matrix transformation.

In the sequel, for convenience, let $X_n = (x_1, \cdots, x_n)^T$, $X'_n = (x'_1, \cdots, x'_n)^T$, $x_1, \cdots, x_n \in \{0, 1, \cdots, N-1\}$; $K_n = (k_1, \cdots, k_n)^T$ and $K'_n = (k'_1, \cdots, k'_n)^T$.

Definition 1. For an arbitrarily given positive integer N and a digital image P, the following transformation

$$X'_n = AX_n(\bmod N),\ (A = (a_{ij})_{n\times n},\ a_{ij} \in \mathbb{Z}) \tag{1}$$

has a period m_N with respect to the image P and m_N is the minimal times that make the image P return to its original status. For an arbitrary matrix $A = (a_{ij})_{m\times n}$, we have $A(\bmod N) = (a_{ij}(\bmod N))_{m\times n}$.

Proposition 1. For a given fixed positive integer N, if $X'_n = AX_n(\bmod N)$, then $A^m X_n(\bmod N)$ can be obtained after m times transformations for X_n.

Proof. If $X'_n = AX_n(\bmod N)$, we have $X'_n = AX_n + K_n N$. Thus

$$AX'_n = A[AX_n + K_n N](\bmod N) = [A^2 X_n + AK_n N](\bmod N) = A^2 X_n(\bmod N).$$

Proposition 1 is proved.

Using Proposition 1, the following results can be obtained.

Proposition 2. If Transformation (1) has the period m, then m is the smallest positive integer which makes $A^m(\bmod N) = E_n$, where E_n is the n-order unitary matrix.

Theorem 1[9]. The sufficient and necessary condition that Transformation (1) has periodicity is that $|A|$ and N are prime to each other, where $|A|$ is the determinant of the matrix A.

Proof(Sufficiency). To prove that (1) has periodicity, it suffices to verify that $\boldsymbol{A\alpha}(\bmod N) \neq \boldsymbol{A\beta}(\bmod N)$, or $\boldsymbol{A}(\boldsymbol{\alpha} - \boldsymbol{\beta})(\bmod N) \neq 0$, for any two different n-dimensional vectors $\boldsymbol{\alpha}$Z and $\boldsymbol{\beta}$. In other words, for any n-dimensional vector $\boldsymbol{X} = (x_1, x_2, \cdots, x_n)^T$, the fact that $\boldsymbol{AX}(\bmod N) = 0$

means $X = 0$.

Set $AX(\mathrm{mod}N) = 0$. By Laplace theorem in the determinant theory, we get

$$|A| \cdot x_1 = (A_{11} \cdot k_1 + \cdots + A_{n1} \cdot k_n)N$$
$$\cdots\cdots$$
$$|A| \cdot x_n = (A_{1n} \cdot k_1 + \cdots + A_{nn} \cdot k_n)N,$$

where A_{ij}, i, $j = 1, \cdots, n$, is the algebraic complement of the element a_{ij} in the matrix A.

Since $|A|$ is prime to N, N is a factor of x_i; and $x_i \in \{0, 1, 2, \cdots, N-1\}$, $i = 1, 2, \cdots, n$, we can see that $X = 0$.

Proof (Necessity). For the given positive integer N, if the transformation has periodicity, then it should be proven that $|A|$ and N are prime to each other. Suppose that m is the period of the transformation defined by (1). From Proposition 2 we have $A^m(\mathrm{mod}N) = E_n$. Hence there exist positive integers b_{ij}, i, $j \in \{1, 2, \cdots, n\}$, making

$$A^m = \begin{pmatrix} 1 + b_{11}N & b_{12}N & \cdots & b_{1n}N \\ b_{21}N & 1 + b_{22}N & \cdots & b_{2n}N \\ \cdots & \cdots & \cdots & \cdots \\ b_{n1}N & b_{n2}N & \cdots & 1 + b_{nn}N \end{pmatrix}.$$

According to the Laplace theorem in the determinant theory, integer K exists and $|A^m| = 1 + KN$. Without loss of generality, we assume that $(|A^m|, N) = t(t > 0)$, $|A| = ts$, $N = tp$. Then $(s, p) = 1$. Therefore, $(ts)^m - Ktp = 1$. It is easy to verify that 1 can be divided by t. Thus $t = 1$; that is, $|A|$ and N are prime to each other.

2 The n-dimensional Arnold transformation and its periodicity

In this section, we study the higher dimensional Arnold transformation and its inverse. Applying the idea of a block matrix, we propose a simple algorithm to calculate the periods so as to avoid sophisticated proof.

Definition 2[9]. For a fixed positive integer, the following transformation is called the n-dimensional Arnold transformation:

$$\begin{pmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 2 & 3 & \cdots & 3 & 3 & 3 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 2 & 3 & \cdots & n-2 & n-1 & n \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} (\mathrm{mod}N), \tag{2}$$

where $x_1, x_2, \cdots, x_n \in \{0, 1, 2, \cdots, N-1\}$.

For simplicity, let

$$\boldsymbol{A}_n = \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 2 & 3 & \cdots & 3 & 3 & 3 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 2 & 3 & \cdots & n-2 & n-1 & n \end{pmatrix}, \boldsymbol{B}_n = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & 0 & \cdots & 1 & 1 & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & 1 & \cdots & 1 & 1 & 1 \end{pmatrix}_{n\times n}$$

$$0_{1,n-1} = (0, 0, \cdots, 0)_{1,n-1} = 0^{\mathrm{T}}_{n-1,1}, \ \alpha_{1,n-1} = (1, 1, \cdots, 1)_{1,n-1} = \alpha^{\mathrm{T}}_{n-1,1},$$
$$\gamma_{1,n-1} = (1, 2, \cdots, n-1)_{1,n-1} = \gamma^{\mathrm{T}}_{n-1,1}, \ \beta_{1,n-1} = (0, 0, \cdots, 0, -1)_{1,n-1} = \beta^{\mathrm{T}}_{n-1,1},$$

where T denotes transposition of a matrix. Obviously,

$$B_k\alpha_{k,1} = (1, 2, \cdots, k)^{\mathrm{T}} = \gamma_{k,1}, \ 1 + \alpha_{1,k}\alpha_{k,1} = k + 1.$$

Proposition 3. $\boldsymbol{B}_n^2 = \boldsymbol{A}_n$

Proof. It is easy to check that

$$\boldsymbol{B}_n = \begin{pmatrix} 0_{n-1,1} & B_{n-1} \\ 1 & \alpha_{1,n-1} \end{pmatrix} = \begin{pmatrix} 0_{1,n-1} & 1 \\ B_{n-1} & \alpha_{n-1,1} \end{pmatrix}, \ \boldsymbol{A}_n = \begin{pmatrix} A_{n-1} & \gamma_{n-1,1} \\ \gamma_{1,n-1} & n \end{pmatrix}. \tag{3}$$

On the other hand, suppose that $\boldsymbol{B}_k^2 = \boldsymbol{A}_k$ holds. Then

$$B_{k+1}{}^2 = \begin{pmatrix} 0_{k,1} & B_k \\ 1 & \alpha_{1,k} \end{pmatrix}\begin{pmatrix} 0_{1,k} & 1 \\ B_k & \alpha_{k,1} \end{pmatrix} = \begin{pmatrix} B_k^2 & B_k\alpha_{k,1} \\ \alpha_{1,k}B_k & 1 + \alpha_{1,k}\alpha_{k,1} \end{pmatrix} = \begin{pmatrix} B_k^2 & \gamma_{k,1} \\ \gamma_{1,k} & k+1 \end{pmatrix} = A_{k+1}.$$

By induction, we can complete the proof of Proposition 3.

Definition 3. Transformation

$$X'_n = A_n^{-1}X_n (\mathrm{mod} N) \tag{4}$$

is called the inverse transformation of the n-dimensional Arnold transformation defined by (2). And $\boldsymbol{A}_n^{-1}$ in Eq. (4) has the following property.

Proposition 4. If $\boldsymbol{A}_n^{-1} = (a'_{ij})_{n\times n}$, then a'_{ij} is an integer, $i, j = 1, \cdots, n$.

Proof. With Proposition 3, we obtain $|\boldsymbol{A}_n| = 1$. Hence $\boldsymbol{A}_n^{-1} = \boldsymbol{A}_n^* / |\boldsymbol{A}_n| = \boldsymbol{A}_n^*$, where $\boldsymbol{A}_n^*$ is the companion matrix of A_n. Clearly, A_n^* is an integer matrix, so is A_n^{-1}. Proposition 4 is proven.

Proposition 4 implies that the Definition 3 has practical significance. The digital image transformations are usually realized by computing the gray levels of images, which are integers. Hence the inverse matrix $\boldsymbol{A}_n^{-1}$ is suitable for integer computing.

Theorem 2. The n-dimensional Arnold transformation and its inverse transformation have the same periods.

Proof. It follows from (2) that $X'_n = AX_n (\mathrm{mod} N) + K_nN$.

Then

$$A^{-1}X'_n = A^{-1}[AX_n + K_nN] = X_n + A^{-1}K_nN.$$

By what we have shown before, we get $A^{-1}K_n = K'_n$.

Therefore, $A^{-1}X'_n(\mathrm{mod}\,N) = X_n$. The theorem is proven.

Theorem 3. For a given positive integer N, suppose that m_N is the period of n-dimensional Arnold transformation (2). Then $m_N = \underset{N}{\mathrm{Min}}\{m \mid A^m(\mathrm{mod}\,N) = E_n\}$.

This theorem can be proven directly from Proposition 2.

By Theorem 3, we can give a simple algorithm to calculate the periods of higher dimensional Arnold transformation. In view of Proposition 2, a general algorithm for calculating the periods of higher-dimensional matrix transformation can also be obtained, which is different from those presented in Refs. [2 ~ 9] and Ding's Ph.D Dissertation[1)]. On the one hand, the algorithm established in this paper is very simple and can be applied to an arbitrary matrix module transformation. On the other hand, computing the periods of n-dimensional Arnold transformation is independent of their orders. The discussions in Refs. [2 ~ 9] are only some special cases of the new algorithm put forward in this paper.

Table 1 gives some calculated results. According to the periods given in this table, distinct dimensions and orders are purposively selected to scramble images. Receivers, according to the corresponding dimensions and orders, by transformation or inverse transformation, can restore the scrambled images. The periods of other Arnold transformations with different dimensions and orders can also be calculated directly by Theorem 3.

Table 1 The periods of different dimensional Arnold transformations relevant to N

N	Period/ m_N			N	Period/ m_N		
	Dimension				Dimension		
	2	3	4		2	3	4
3	4	13	9	25	50	155	155
4	3	7	7	50	150	1085	1085
5	10	31	31	60	60	2821	1953
6	12	91	63	100	150	1085	1085
7	8	21	57	120	60	5642	3906
8	6	14	14	125	250	775	775
9	12	39	27	128	96	224	224
10	30	217	217	256	192	448	448
11	5	133	133	480	120	22568	15624
12	12	91	63	512	384	896	896

3 Security of n-dimensional Arnold transformation and its inverse

In this section, we discuss the security of scrambling images by n-dimensional Arnold transformation and its inverse. Refs. [2 ~ 9] and Ding's Ph. D Dissertation[1)] discussed scrambling digital

1) See footnote 1) on page 542

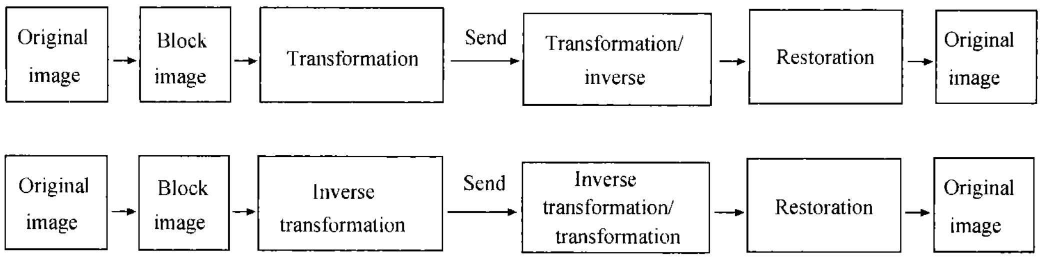

Fig. 1 Flow diagram of transformation and inverse one.

image. However, they did not discuss the security of scrambling images. In what follows, the combinatorial transformation method to scramble digital images is introduced as follows.

Step 1. Divide an original image into different blocks according to the assigned way.

Step 2. Based on step 1, distinct dimensional Arnold transformations or their inverse ones are applied to different block matrices to scramble them.

Using the above-mentioned method, no restora-

Fig. 2 800 × 600, 24 bits original image.

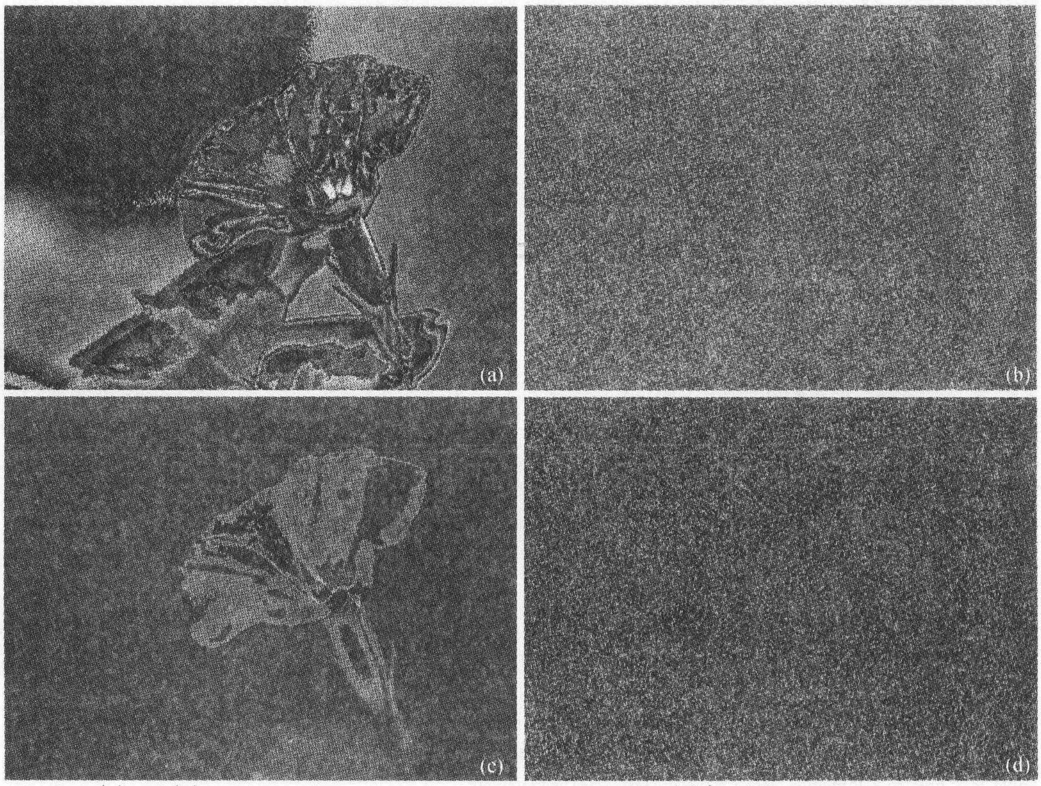

Fig. 3 (a) and (b) Arnold transformation results from Fig. 2 respectively; (c) and (d) are 1 time and 5 times inverse transformations, respectively.

tion image for the original can be obtained unless the special block matrix method is used. It is very difficult to restore the original image for illegal attackers, because there are lots of ways to divide an image into blocks and each block matrix has two choices: transformation and inverse transformation as shown in Fig.1. Therefore expected security can be attained. If a single Arnold transformation is applied to scramble digital images, security is weak. Thus the combinatorial transformation method has an important practical signification in scrambling the digital image.

Now we give some examples showing the difference between the single Arnold transformation and blocking Arnold transformation.

We scramble an original image as shown in Fig.2 by 3-dimensional Arnold transformation and inverse transformation, and combinatorial transformation respectively. The transformed results are shown in Figs.3 and 4. Although the difference in the transformed results is unknown, one can restore the original image by the corresponding times transformations or inverses to Fig. 3 (Fig. 5(a)); while one cannot restore the original image from Fig.4 unless the special block matrix methods used in scrambling image are known. Figs. 5 (b) and 5(c) are the results after 5 times 3-dimensional Arnold transformations (or 2-dimensional ones) and 5 times inverse ones for Figs. 4(b) and 4(d), respectively. One cannot obtain the original image because the block matrix used in scrambling the original

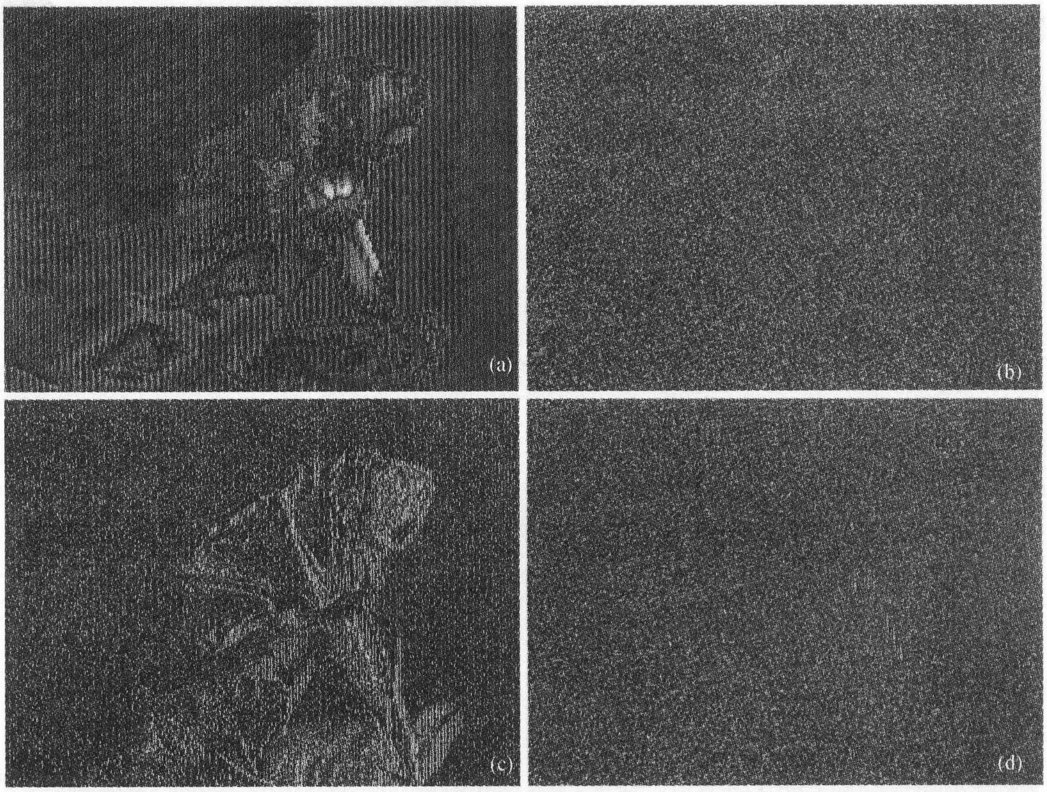

Fig. 4 Results of 2-dimensional and 3-dimensional Arnold transformations and their inverse transformations for the blocked image of Fig. 2. (a) and (b), results of 1 time transformation and 5 times ones respectively; (c) and (d), results of 1 time transformation and 5 times inverse ones respectively.

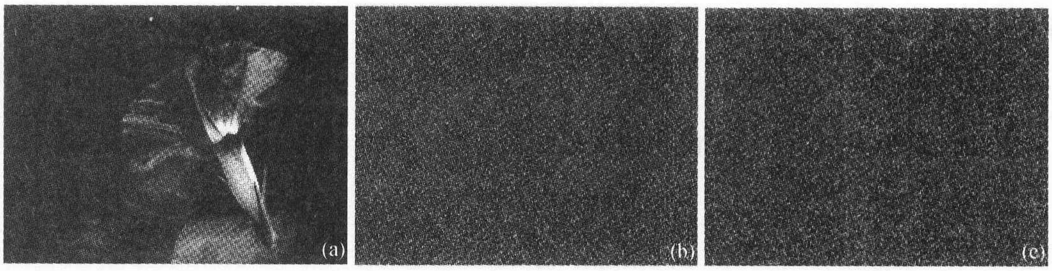

Fig. 5 Recovered results of scrambled images. (a) For Fig. 3; (b) for Fig. 4(b); (c) for Fig. 4(d).

image was not applied. This shows that the combinatorial transformation method has good security.

Acknowledgment We thank Dr. Zou Jiancheng and Dr. Ding Wei for their kind help.

References

1 Arnold, V.I. et al. Ergodic Problems of Classical Mechanics. Mathematical Physics Monograph Series, New York: W.A. Benjamin, INC, 1968.

2 Qi, D.X. Fractal and its Generation on Computer(in Chinese), Beijing: Academic Press, 1994.

3 Ding, W. et al. A new kind of digital image transformation in information disguising. In: Information Sciences and Microelectronic Technology (in Chinese), Beijing: Academic Press, 1998: 309.

4 Qi, D.X. et al. A new image transformation scheme and digital approximation between different pictures. In: Lecture Notes in Pure and Applied Math (ed. Zhong, Y.C. et al.), New York: Marcel Dekker, Inc., 1999, 202: 465.

5 Ding, W. et al. Digital image transformation and information hiding and disguising technology, Chinese J. Computers, 1998, 21 (9): 838.

6 Qi, D.X. Matrix transformation and its applications to image hiding. J. North China Univ. of Tech. (in Chinese), 1999, 11 (1): 24.

7 Sun, W. The periodicity of Arnold transformation. J. of North China Univ. of Tech. (in Chinese), 1999, 11(1): 29.

8 Zou, J.C. et al. The Arnold transformation of digital image with two transformation and its periodicity, J. of North China Univ. of Tech. (in Chinese), 2000.1(12): 10.

9 Qi, D.X. et al. A new class of scrambling transformation and its application in the image information covering. Science in China, Series E, 2000, 43(3): 304.