CHIN. PHYS. LETT. Vol. 26, No. 6 (2009) 060502

Multidimensional Z-Matrix with Control Parameters and Its Applications in Image Encryption *

ZHAO Liang(赵亮)**, LIAO Xiao-Feng(廖晓峰), XIANG Tao(向涛), XIAO Di(肖迪)

College of Computer Science, Chongqing University, Chongqing 400044

(Received 2 February 2009)

An n-dimensional Z-matrix with control parameters is presented, and its periodicity and chaos are testified. Experimental results show that the proposed Z-matrix has a long period and changeable periodicity with different dimensions. Some examples of image encryption with a Z-matrix of different dimensions are listed for demonstrating its applications.

PACS: 05.45.Vx, 05.45.Pq, 43.72.+q, 47.10.Fg

The Arnold cat map used for image encryption was first set up by Arnold. Then, Zhao[1] presented a class of high-dimensional Arnold transformations which can be named as the standard Arnold cat map and discussed the periodicity of them. Meanwhile, Chen *et al.*[2] introduced another kind of three-dimensional Arnold transformations which can be called Chen's Arnold cat map and the corresponding high-dimensional matrix was also presented by Kwok *et al.*[3,4] As it has wide applications in image encryption, the high-dimensional chaotic map is a new interest of many researchers, e.g. a T-matrix,[5] which has long periodicity, is proposed by Zhang. In this Letter, a novel chaotic matrix called a Z-matrix is defined. At the same time, its periodicity and chaos are testified, and its applications in image encryption are listed.

Three high-dimensional matrices: The high-dimensional standard Arnold matrix is as follows:

$$A = \begin{bmatrix} 1 & 1 & \cdots & 1 & 1 \\ 1 & 2 & \cdots & 2 & 2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 2 & \cdots & n-1 & n-1 \\ 1 & 2 & \cdots & n-1 & n \end{bmatrix}, \tag{1}$$

where $\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ is the famous two-dimensional (2D) Arnold matrix.

Relatively, the high-dimensional Chen's Arnold matrix is defined as

$$A' = A'_{1,2} \cdots A'_{1,m} A'_{2,3} \cdots A'_{m-1,m}, \tag{2}$$

where $A'_{i,j}$ $(i < j)$ is an identity matrix except that $c_{i,j} = a_{i,j}$, $c_{j,i} = b_{i,j}$ ($a_{m,n}$ and $b_{m,n}$ are elements at row $m(n)$ and column $n(m)$), which are positive constants in $[0, 2^L - 1]$ and $c_{j,j}$. In particular, in matrix $A'_{i,j}$, $c_{j,j} = 1 + a_{i,j}b_{i,j}$, such as $A'_{1,3}$:

$$A'_{1,3} = \begin{bmatrix} 1 & 0 & a_{1,3} & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ b_{1,3} & 0 & 1 + a_{1,3}b_{1,3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}. \tag{3}$$

Meanwhile, the T-matrix in Ref. [5] is

$$T_{n\times n} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 2 & 2 & \cdots & 2 & 2 & 2 \\ 1 & 3 & 4 & \cdots & 4 & 4 & 4 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 1 & a_1 & a_2 & \cdots & a_{n-3} & a_{n-2} & a_{n-1} \\ 1 & 1 + a_1 & a_1 + a_2 & \cdots & \cdots & a_{n-3} + a_{n-2} & a_{n-2} + a_{n-1} \end{bmatrix}, \tag{4}$$

where the initial 2D T-matrix is the same with the 2D Arnold matrix.

For the above high-dimensional matrices, they all satisfy the following transformation:

$$\begin{bmatrix} x'_1 \\ x'_2 \\ \vdots \\ x'_n \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \cdots & c_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \bmod N, \tag{5}$$

*Supported by the National Natural Science Foundation of China under Grant No 60703035, the National Science Foundation for Post-doctoral Scientists of China under Grant No 20080430741, the Natural Science Foundation of Chongqing under Grant Nos 2008BB2182 and 2008BB2193, the Postgraduate Technology Innovation Foundation of Chongqing University under Grant No 200903A1B0010303, the Program for New Century Excellent Talents in University of China under Grant No NCET-08-0603, the Natural Science Foundation Project of Chongqing under Grant No CSTC2009BA2024.

** To whom correspondence should be addressed. Email: zhaoliang@cqu.edu.cn;zhaoliang_916@163.com

© 2009 Chinese Physical Society and IOP Publishing Ltd

where $c_{i,j}$ is an element of $\{A, A', T\}$ at row i and column j. At the same time, they have different periodicities with different N, i.e. there is a positive integer P, which is the period of these transformation satisfying $C^P r_0(\mathrm{mod} N) = r_0$, where $r_0 = [x_1, x_2, x_3, \ldots x_m]^T$.

Definition of n-dimensional Z-matrix: The 2D Z-matrix with control parameters is the same as the generalized 2D Arnold matrix and can be defined as $Z_{2\times 2} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$, when $n > 2$, the corresponding $Z_{n\times n}$-matrix is

$$Z_{n\times n} = \begin{bmatrix} 1 & a & a & \cdots & a & a & a \\ b & ab+1 & ab+1 & \cdots & ab+1 & ab+1 & ab+1 \\ b & ab+2 & ab+3 & \cdots & ab+3 & ab+3 & ab+3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ b & ab+(n-2) & ab+(n-2) & \cdots & ab+(n-2) & ab+(n-1) & ab+(n-1) \\ b & ab+(n-1) & ab+(n-1) & \cdots & ab+(n-1) & ab+(n-1) & ab+n \end{bmatrix}. \tag{6}$$

Theorem 1: The proposed high-dimensional Z-matrix is area-preserving.

Proof: According to the definition of the Z-matrix, the 2D Z-matrix and three-dimensional (3D) Z-matrix are

$$Z_{2\times 2} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}, \quad Z_{3\times 3} = \begin{bmatrix} 1 & a & a \\ b & ab+1 & ab+1 \\ b & ab+2 & ab+3 \end{bmatrix},$$

then $\det Z_{2\times 2} = |Z_{2\times 2}| = 1$, $\det Z_{3\times 3} = |Z_{3\times 3}| = 1$.

Supposing $\det Z_{n\times n} = 1$, $n \geq 4$, where $\det Z_{n\times n}$-matrix is as follows:

$$|Z_{n\times n}| = \begin{vmatrix} 1 & a & a & \cdots & a & a & a \\ b & ab+1 & ab+1 & \cdots & ab+1 & ab+1 & ab+1 \\ b & ab+2 & ab+3 & \cdots & ab+3 & ab+3 & ab+3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ b & ab+(n-2) & ab+(n-2) & \cdots & ab+(n-2) & ab+(n-1) & ab+(n-1) \\ b & ab+(n-1) & ab+(n-1) & \cdots & ab+(n-1) & ab+(n-1) & ab+n \end{vmatrix} = 1,$$

Then, $\det Z_{(n+1)\times(n+1)}$ can be presented as

$$|Z_{(n+1)\times(n+1)}| = \begin{vmatrix} 1 & a & a & \cdots & a & a & a \\ b & ab+1 & ab+1 & \cdots & ab+1 & ab+1 & ab+1 \\ b & ab+2 & ab+3 & \cdots & ab+3 & ab+3 & ab+3 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ b & ab+(n-1) & ab+(n-1) & \cdots & ab+(n-1) & ab+n & ab+n \\ b & ab+n & ab+n & \cdots & ab+n & ab+n & ab+(n+1) \end{vmatrix}.$$

Subtracting column n from column $n+1$, $\det Z_{(n+1)\times(n+1)}$-matrix can be described as

$$|Z_{(n+1)\times(n+1)}| = \begin{vmatrix} 1 & a & a & \cdots & a & a & 0 \\ b & ab+1 & ab+1 & \cdots & ab+1 & ab+1 & 0 \\ b & ab+2 & ab+3 & \cdots & ab+3 & ab+3 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ b & ab+(n-1) & ab+(n-1) & \cdots & ab+(n-1) & ab+n & 0 \\ b & ab+n & ab+n & \cdots & ab+n & ab+n & 1 \end{vmatrix}. \tag{7}$$

According to Eq. (7), the determinant of this can be expanded based on the $(n+1)$th column, and can be changed to $\det Z_{n\times n}$:

$$\begin{aligned} |Z_{(n+1)\times(n+1)}| &= 1 \times (-1)^{(n+1)+(n+1)} \times |Z_{n\times n}| \\ &= |Z_{n\times n}|. \end{aligned}$$

As $\det Z_{n\times n} = 1$, the result of $\det Z_{(n+1)\times(n+1)}$ is also equal to 1. Therefore, for any integer n ($n \geq 2$),$|Z_{n\times n}| \equiv 1$. Then, the Z-matrix is area-preserving because the determinant of its transformation matrix is equal to 1.

Theorem 2: For a given positive integer N, the transformation $r_m = Zr_0(\mathrm{mod}\, N)$ has periodicity, where $r_m = [x'_1, x'_2, x'_3, \ldots, x'_m]^T$ and $r_0 = [x_1, x_2, x_3, \ldots, x_m]^T$.

Proof: According to theorem 1 in Ref. [6], as the determinant Z-matrix is identical to 1, for any a and b, $|Z_{n\times n}|$ and N are always prime to each other ($gcd(\det Z_{n\times n}, N) = 1$). Therefore, the Z-matrix transformation is periodical.

Theorem 3: The largest Lyapunov exponent (LE) of Z-matrix transformation is positive.

Proof: The LEs of any matrix transformation are determined by the eigenvalues of this matrix. According to matrix theory, since $Z_{n\times n}$ is full rank, there exist n linear independent eigenvalues $\lambda_1, \lambda_2, \ldots, \lambda_n$. Meanwhile, a modal vector Q and a spectral matrix E can be used for describing $Z_{n\times n}$, i.e. $Z = QEQ^{-1}$:

$$Z_{n\times n} = [\, q_1 \quad q_2 \quad \cdots \quad q_n \,] \cdot \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \lambda_n \end{bmatrix} \begin{bmatrix} q_1 \\ q_2 \\ \vdots \\ q_n \end{bmatrix}, \tag{8}$$

where

$$Q = [q_1, q_2, \ldots, q_n],$$
$$E = \begin{bmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \lambda_n \end{bmatrix}.$$

As the product of the eigenvalues of a matrix is identical to its corresponding determinant, the following equation is satisfied:

$$\prod_{i=1}^{n} \lambda_i = |Z_{n\times n}| = 1, \tag{9}$$

$\forall\, i$, if $\lambda_i = 1$. $Z = QEQ^{-1} = QQ^{-1} = I$, where I is an identity matrix. However, according to the conformation of $Z_{n\times n}$, $Z \neq I$ for any a and b. Therefore, there must be at least one $\lambda_i > 1$ ($\exists\, i$). Otherwise, if $\lambda_i < 1$ for all i, the product of all eigenvalues is less than 1. Then, there must be at least one positive LE ($\sigma_i = \ln|\lambda_i| > 0$), which illustrates that the transformation based on the n-dimensional Z-matrix is chaotic.

Period of Z-matrix transformation: In order to illuminate the merits of the n-dimensional Z-matrix, the periods of a Z-matrix with different N and n are computed, and in particular, the results of a 3D to seven-dimensional (7D) Z-matrix ($a = 7, b = 3$), when N is equal to 2^β (β is an integer), which meets the requirements for general image encryption, are listed in the following Tables 1 and 2.

Table 1. Periods of 3D Z-matrix, T-matrix, Standard Arnold matrix and Chen's Arnold matrix with different N.

N	16	32	64	128	256	512	1024	2048
Z-matrix	56	112	224	448	896	1792	3584	7168
T-matrix	56	112	224	448	896	1792	3584	7168
Standard Arnold	28	56	112	224	448	896	1792	3584
Chen's Arnold	24	48	96	192	384	768	1536	3072

From a large amount of calculations and analyses, some useful information and conclusions can be drawn. If $N = 2^\beta$ (β is an integer), the period of the 3D Z-matrix is the same as the 3D T-matrix but two times of that of the 3D Standard Arnold and more than two times of that of the 3D Chen's Arnold (see Table 1). Meanwhile, the period of the Z-matrix is dependent on the dimension which means that for different dimensions, the period is dissimilar and is not less than the least period (LEP). However, with a great number of calculations, we find that the periods of three other matrix transformations are not dependent on dimension. For the control parameters $a$and b, if a and b choose any number, the period of the Z-matrix can change following them. Table 3 presents this phenomenon.

Table 2. Periods of Z-matrix with different N and n.

N	16	32	64	128	256	512	1024
3D	56	112	224	448	896	1792	3584
4D	120	240	480	960	1920	3840	7680
5D	248	496	992	1984	3968	7936	15872
6D	56	112	224	448	896	1792	3584
7D	1016	2032	4064	8128	16256	32512	65024

Table 3. Periods of 3D Z-matrix with different a and b ($N = 16$).

(a, b)	Period	(a, b)	Period	(a, b)	Period
(98, 6)	16	(76, 15)	16	(31, 41)	56
(540, 454)	8	(40, 29)	32	(47, 49)	56
(370, 70)	16	(338, 315)	32	(55, 269)	56
(66, 100)	8	(838, 1401)	32	(273, 485)	56
(1334, 898)	16	(1308, 935)	16	(1195, 1065)	56

The above table gives a very important conclusion that when $N = 2^\beta$ (in Table 3, $N = 16 = 2^4$), if a and b are both odd number, the corresponding period is a fixed number which is the largest period (LAP). Otherwise, the period is changeable among some number which is less than LAP.



Fig. 1. Pixel value of gray image encryption: (a) original image, (b) encryption image ($T_{\rm itm} = 10$), (c) encryption image ($T_{\rm itm} = 526$), (d) encryption image ($T_{\rm itm} = 1920$).

Applications of n-dimensional Z-matrix in image encryption: In order to encrypt an image effectively, the pixel value and position should be considered. The proposed n-dimensional Z-matrix can be applied to pixel value substitution and position confusion. For

a gray image, the method of pixel value substitution is the same as that in Ref. [5]. For a color image, the way we encrypt the image should take into account R, G, B components at the same time. That is to say, for each pixel, we use the following formula to encrypt it:

$$\begin{bmatrix} R'_i \\ G'_i \\ B'_i \end{bmatrix} = \begin{bmatrix} 1 & a & a \\ b & ab+1 & ab+1 \\ b & ab+2 & ab+3 \end{bmatrix} \begin{bmatrix} R_i \\ G_i \\ B_i \end{bmatrix} \bmod N. \quad (10)$$

Meanwhile, for the pixel position confusion, we can take advantage of the corresponding scheme in Ref. [2], which can accelerate de-correlate relations among pixels effectively. In these applications, the control parameters $a = 7$, $b = 3$.

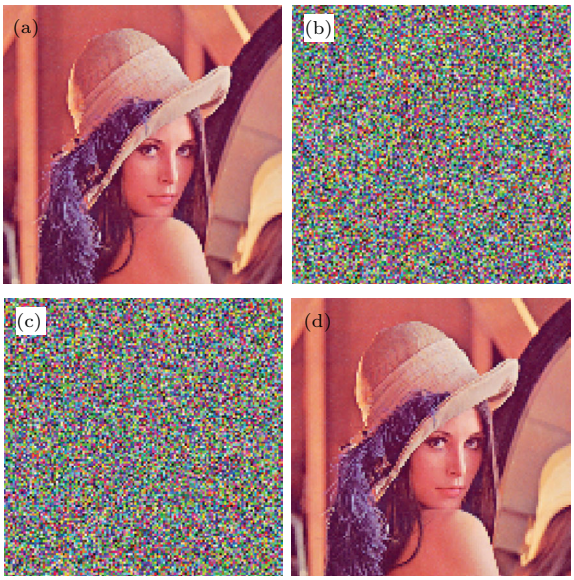


Fig. 2. Pixel value of color image encryption: (a) original image, (b) encryption image ($T_{\rm itm} = 50$), (c) encryption image ($T_{\rm itm} = 321$), (d) encryption image ($T_{\rm itm} = 896$).

Pixel value substitution: Figures 1 and 2 show the results of pixel value substitution for a gray image and a color image with the same size of 128×128, respectively, in which $n = 4$, $N = 256$ for the gray image and n=3, N=256 for the color image. In particular, when the iteration time $T_{\rm itm}$ is equal to the corresponding period, the image can be completely recovered.

Pixel position confusion: In order to encrypt the positions of pixels, it can be found that the 2D plain image is first transformed to a 3D cube. Then, the 3D Z-matrix in Eq. (10) can be applied in position confusion. Figure 3 presents the encryption procedures and the decrypted image when the original image is the gray Lena image with a size of 512×512, in which $n = 3$, $N = 512$, $T_{\rm itm} = 14$. The deciphered image is exactly the same as the plain image after the 3D cipher image is iterated for the same time. For color image confusion, as the process is only dependent on pixel position of an image, a similar way can be used, and the result is also satisfying.

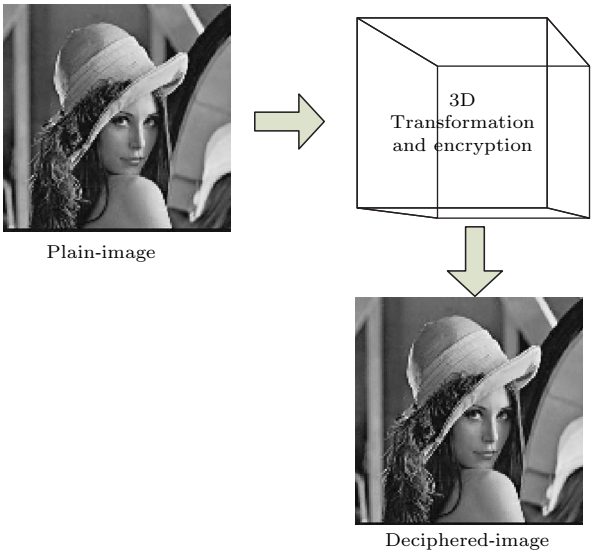


Fig. 3. Pixel position of gray image encryption.

In summary, we have introduced a new chaotic matrix called a Z-matrix. Additionally, the periodicity and chaos are proved. It inherits some good characteristics of the T-matrix and Arnold matrices including long periodicity, chaos and simple structure. In particular, differing from the three other matrices, the period of the Z-matrix with different dimensions is changeable. Therefore, it can be used for digital image encryption with high security.

References

[1] Zhao H 2002 *J. North China University Technol.* **14** 21 (in Chinese)
[2] Chen G, Mao Y and Chui C 2004 *Chaos, Solitons Fractals* **21** 749
[3] Kwok H S, Wallace K S and Tang 2005 *Int. J. Bifur. Chaos* **15** 4043
[4] Kwok H S, Wallace K S and Tang 2007 *Chaos, Solitons Fractals* **32** 1518
[5] Zhang M R, Shao G C and Yi K C 2004 *Electron. Lett.* **40** 1583
[6] Qi D, Zou J and Han X 2000 *Sci. Chin.* E **43** 304