APPLICATION OF BALANCING TRANSFORMATION TO IMAGE SECURITY

By

Prasanta Kumar Ray*, Bijan Kumar Patel† and Debbrota Paul Chowdhury‡

*Sambalpur University, Jyoti-Vihar, Burla-768019, India
†International Institute of Information Technology, Bhubaneswar-751003, India
‡National Institute of Technology, Rourkela-769008, India

*rayprasanta2008@gmail.com †iiit.bijan@gmail.com ‡debbrota@gmail.com

(Received : May 11, 2017)

Abstract

In this article a new kind of nonlinear transformation namely the higher-dimensional balancing transformation is introduced. The scrambling action of this transformation targeting on the phase space of the digital images is also discussed .Indeed, the application of higher dimensional balancing transformation in the storage and transportation of image information is highly helpful for the information security purpose.

2010 Mathematics Subject Classification: 11B37, 11B39, 11T71.
Keywords*:* Digital image; Scrambling transformations; Balancing numbers; Periodicity; Balancing matrix; Balancing transformation.

1. Introduction

Image scrambling is a useful approach to secure the image data security by crawling the image into an indiscernible appearance. A number of image scrambling methods have been developed by many researchers [3-6]. The Arnold cat map which is a chaotic map from the torus into itself is widely used for image encryption and was first demonstrated by Arnold in 1967 which is defined as a transformation $\Gamma : T^2 \to T^2$ such that: $\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N)$,

where $x, y \in \{0, 1, 2, \ldots, N-1\}$ and N is the size of a digital image [1]. Arnold transformation can be effectively used in the image scrambling because of its periodicity. In [4], Dong-xu et al. established a new digital image scrambling method based on Fibonacci numbers and studied about the matrix modulo of order n of Arnold transformation and Fibonacci transformation. In [3], Bing has studied some more properties of the period of Arnold transformation by means of introducing a new integer sequence. Zou et al. [9] introduced a subfamily of the generalized Fibonacci sequence family, called as distinguished generalized Fibonacci sequence. They also considered transformations of the members of the subfamily namely Fibonacci transformation and Lucas transformation, which were used for image scrambling. Mishra et al.[6] proposed a new spatial domain image scrambling method which is based on Fibonacci and Lucas series. This method has wide application in various spatial domain image processing techniques of data hiding and secret communications. They have also claimed that the transforms with higher periodicity may reduce the level of security as those can be decrypted by other maps even if the exact map is not known.

In this article, we introduce a new type of chaotic map based on balancing numbers which we later call as balancing Q_B-matrix transformation. Further, we claim that this transformation is used for better image security than the other transformations like Arnold, Fibonacci and Lucas transformations.

2. Balancing Q_B-matrix transformation

Balancing and their balancers are solutions of a simple Diophantine equation posed by Behera and Panda [2]. According to them, the pairs (n, r) where n is a balancing number and r is the corresponding balancer, are solutions of the Diophantine equation $1 + 2 + \cdots + (n-1) = (n+1) + (n+2) + \cdots + (n+r)$.

For any natural number n, all the balancing numbers generate through the recursive relation $B_{n+1} = 6B_n - B_{n-1}$ with initial values $B_0 = 0$ and $B_1 = 1$, where B_n denotes the n-th balancing number. The study of balancing sequence is quite interesting because they closely resembling some properties of natural numbers and trigonometric functions [7]. There is another way to represent balancing numbers through matrices. Ray [8] has introduced the balancing matrix $Q_B$whose entries are the first three balancing numbers 0, 1 and 6, that is $Q_B = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix}$. He has also shown that the sequence of balancing matrices satisfies the same recurrence relation as that of balancing numbers, that is $Q_B^n = 6Q_{B-1}^n - Q_{B-2}^n$, where $Q_B^n = \begin{pmatrix} B_{n+1} & -B_n \\ B_n & -B_{n-1} \end{pmatrix}$.

Without loss of generality, we present the balancing matrix Q_B in a different way by interchanging the main diagonal elements as $Q_{B_1} = \begin{pmatrix} 0 & -1 \\ 1 & 6 \end{pmatrix}$. The matrix $Q_{B_1}^n = \begin{pmatrix} -B_{n-1} & -B_n \\ B_n & B_{n+1} \end{pmatrix}$ is so formed that its determinant is invariant without loss of generality to the Cassini formula $B_n^2 - B_{n-1}B_{n+1} = 1$ [7]. The following extensions of balancing matrices are so formed that the determinants are invariant without loss of Cassini formula

$$Q_{B_2} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 6 & 0 \end{pmatrix};\ Q_{B_3} = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 6 & 0 & 0 \end{pmatrix};\ Q_{B_4} = \begin{pmatrix} 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 1 & 6 & 0 & 0 & 0 \end{pmatrix};$$ and so

on. In general for $p = 0, 1, 2, \ldots$, the $(p+1) \times (p+1)$ matrix represents the Q_{B_p} matrix whose determinant indeed 1.

In this study, authors develop a new transformation which they call as balancing transformation by replacing 2D Arnold transformation matrix in the Arnold transform by 2D balancing transform matrixQ_{B_1}. The balancing transformation is defined in the following way.

Definition 2.1. *For a given positive integer* $N \geq 2$,

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 6 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N),$$

where $x, y \in \{0, 1, 2, \ldots, N-1\}$ *and N is the size of a digital image.*

Similarly, the balancing $Q_B$transformation is defined as follows.

Definition 2.2. *For a given positive integer* $N \geq 2$,

$$\begin{pmatrix} x_1' \\ x_2' \\ \vdots \\ x_p' \end{pmatrix} \equiv Q_{B_p} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_p \end{pmatrix} (mod\ N), where\ x, y \in \{0, 1, 2, \ldots, N-1\}.$$

2.1 Periodicity of balancing transformation

Let m_N denotes the period of the balancing $Q_B$transformation which is nothing but the smallest positive integer n such that the image p can comeback after n times transforms. The following tables show the periodicity of the balancing-Q transformation. Table-1 and Table-2 show the periods of 3-dimensional and 4-dimensional balancing Q_B-transformations for some positive integer $N \geq 2$.

Table 1: Periods of the 3-dimensional Arnold transformations for some N

N	2	3	4	5	6	7	8	9	11	12	25	50
m_N	7	13	7	31	91	21	14	39	133	91	155	1085

Table 2: Periods of the 3-dimensional balancing Q_B-transformations for some N

N	2	3	4	5	6	7	8	9	11	12	14	16	18	30
m_N	3	3	6	31	3	48	12	9	55	6	48	24	9	93

Table3: Periods of the 4-dimensional Arnold transformations for some N

N	2	3	4	5	6	7	8	9	10	11	12	25	50
m_N	7	9	7	31	63	57	14	27	217	133	63	155	1085

Table 4: Periods of the 4-dimensional balancing Q_B-transformations for some N

N	2	3	4	5	6	7	8	9	11	12	14	16	18	30
m_N	4	8	8	124	8	400	16	24	183	8	400	32	24	248

3. The image scrambling based on the phase spaces

It is well known that a phase space of a dynamical system is a space in which all possible states of a system are represented, with each possible state of the system corresponding to one unique point in the phase space. In a phase space, every degree of freedom or parameter of the system is represented as an axis of a multi dimensional space. Here a digital image can be regarded as a matrix. The position of an element of the matrix is the coordinates of the image pixel and the element of the matrix is the gray level of the pixel. Effective crawling is able to enhance the security of encryption algorithm.

The following transformation is called the balancing transformation based on the phase space:

$$P' = AP\ (mod\ T),$$

where

$$P' = \begin{pmatrix} p'_{11} & p'_{12} & \cdots & p'_{1n} \\ p'_{21} & p'_{22} & \cdots & p'_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ p'_{m1} & p'_{m2} & \cdots & p'_{mn} \end{pmatrix}, A = \begin{pmatrix} 0 & -1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 1 & 6 & \cdots & m \end{pmatrix};$$

is the transformation matrix in the m-dimensional balancing transformation,

$$P = \begin{pmatrix} P_{11} & P_{11} & \cdots & P_{1n} \\ P_{21} & P_{22} & \cdots & P_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ P_{m1} & P_{m2} & \cdots & P_{mn} \end{pmatrix},$$

T is the highest level of the gray level of all image elements in P and $p_{ij} \in \{0, 1, 2, \ldots, T-1\}$.

The step wise encoding and decoding procedure of the proposed method is outlined as follows,

Algorithm 1 Image Encoding

1. Consider an image.
2. Balancing transformation is applied on the input image to obtain the temporary image.
3. If temporary image is the original image, then display the temporary image and its period.
4. Choose an encoding image, whose iteration lies in between original image and its period.

Algorithm 2 Image Decoding

1. Input encrypted image (Temporary Image = Encrypted Image).
2. Multiply temporary image with inverse balancing matrix.
3. Take modulus of output image of step-2 with T and take it as temporary image.
4. Continue step-2 and step-3 until final image number reached.
5. Show the final image.

The following example shows the whole process.

Example 3.1. *Consider the original images Fig. 1(a) and Fig. 2(a) of size* 204×204 *and implemented these figures in Matlab environment. Fig. 1(b), 1(c) and Fig. 2(b), 2(c) represent the resulted encrypted images after applying balancing transformation with number of iterations 203, 422 and 255, 460, respectively. To decryption of the original version of encrypted image can be obtained by multiplying the inverse balancing matrix with the encrypted matrix.*

Fig. 1(a)

Fig. 1(b)

Fig. 1(c)

Fig. 2(a)

Fig. 2(b)

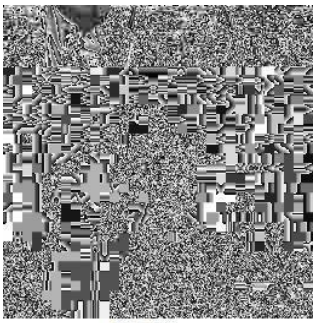

Fig. 2(c)

Conclusion

It is experimentally proved that the transformation with higher periodicity may reduce the level of security as those can be decrypted by other maps even if the exact map is not known [6]. Based on this argument, since balancing transform has lower periodicity, the level of security is high in the image scrambling as compared to Arnold transformation, Fibonacci transformation and Lucas transformation.

References

[1] V.I. Arnold and A. Avez, *Ergodic Problems in Classical Mechanics*, New York, Benjamin, 1968.

[2] A. Behera and G.K. Panda, On the square roots of triangular number, *Fibonacci Quart.* **37** (2) (1999), 98 - 105.

[3] L. Bing and X. Jiawei, Period of Arnold transformation and its application in image scrambling, *J. Cent. South Univ. Tech.* **12** (1) (2005), 278-282.

[4] Q. Dong-xu, Z. Jian-cheng and H. Xiao-you, A new class of scrambling transformation and its application in the image information covering, *Sci. China (Series E)* **43** (3) (2000), 304 - 312.

[5] S. Lee and G. Jeon, Scrambling using phase information, *Adv. Sci. Tech. Letters* **99** (2015), 265-268.

[6] M. Mishra, P. Mishra, M. C. Adhikary and S. Kumar, Image encryption using Fibonacci-Lucas transformation, *Int. Jour. Crypto. Inform. Secur.* **2** (3) (2012), 131-141.

[7] G. K. Panda, Some fascinating properties of balancing numbers, *Congr. Numer.* **194** (2009),185-189.

[8] P. K. Ray, Certain matrices associatedwith balancing and Lucas-balancing numbers, *Matematika* **28** (1) (2012), 15-22.

[9] J. C. Zou, R. K. Ward and D. X. Qi, The generalized Fibonacci transformation and application to image scrambling, Proceeding of the IEEE International Conference on Acoustic, *Speech and Signal Processing* **3** (2010), 385-388.