TWMS J. App. Eng. Math. V.9, N.2, 2019, pp. 287-293

A DIGITAL SCRAMBLING METHOD BASED ON BALANCING NUMBERS

P. K. RAY[1], B. K. PATEL[2], D. P. CHOWDHURY[3], S. KUJUR[4], §

Abstract. In this article, a new approach to the study of image scrambling based on balancing numbers, balancing transformation is presented. The properties of the proposed transformation and its periodicity are studied in details. In order to reduce the periods of the balancing transformation, we separate the consecutive pixels as far as possible from each other in that domain of the digital images.

Keywords: balancing numbers, Fibonacci transformation, Lucas transformation, balancing transformation, periodicity.

AMS Subject Classification: 11B37, 11B39, 11T71.

1. Introduction

Digital image scrambling is commonly approached to secure the image data security. In recent years, researchers have developed a number of methods to scramble the (x, y) positions of images [1, 3, 4, 5, 6, 11, 14]. There were several image scrambling schemes for protecting the confidentiality of sensitive images basically through cryptographic and stenographic techniques [4]. In [5], Dong-xu et al., have formed and studied extensively on two nonlinear transformations, i.e., one is higher dimensional Arnold transformation and other is higher dimensional Fibonacci-Q transformation. They used the properties of these two transformations for scrambling digital images. Bai et al., presented a digital image scrambling algorithm based on Knight-tour problem (KTP) [1]. In [13], Zou et al., has introduced two new methods for scrambling digital images and established the periodicity of these transformations. In a subsequent paper [15], Zou et al., presented two transformations, namely Fibonacci transformation and Lucas transformation, based on the well known Fibonacci numbers and Lucas numbers. They have also shown that the Fibonacci transformation and Lucas transformation are uniform and can be applied to digital image scrambling. Bing et al., studied the periodicity of the Arnold transformation

[1] School of Mathematical Sciences, Sambalpur University, Sambalpur, 768019, India.
e-mail: rayprasanta2008@gmail.com; ORCID: https://orcid.org/0000-0002-1208-8113.
[2] International Institute of Information Technology, Bhubaneswar, 751003, India.
e-mail: iiit.bijan@gmail.com; ORCID: https://orcid.org/0000-0001-7637-8489.
[3] Department of CSE, National Institute of Technology Rourkela, Rourkela, 769008, India.
e-mail: debbrota@gmail.com; ORCID: https://orcid.org/0000-0002-4622-2157
[4] Department of Mathematics, National Institute of Technology Rourkela, Rourkela, 769008, India.
e-mail: satyapriyakujur94@gmail.com; ORCID: https://orcid.org/0000-0001-9622-6714.
§ Manuscript received: March 3, 2017; accepted: September 18, 2017.
TWMS Journal of Applied and Engineering Mathematics, Vol.9, No.2;

up to two dimensions [3]. Also in [3], they proposed a new method for computing the periods of the Arnold transformation. It is experimentally proved that any transformation with higher periodicity may reduce the level of image security [6]. The periodicity of the above methods are high reaching. In this paper, we present digital image scrambling method based on the sequence of balancing numbers and also discuss its uniformity and periodicity.

The concept of balancing numbers was first introduced by Behera et al., [2] in the year 1999 which are obtained from a simple Diophantine equation

$$1 + 2 + \cdots + (n-1) = (n+1) + (n+2) + \cdots + (n+r),$$

calling n as balancing number and r as balancer corresponding to n. The balancing numbers, though obtained from a simple Diophantine equation, are very useful for the computation of square triangular numbers. If n is a balancing number then $8n^2 + 1$ is a perfect square, and hence n^2 is a square triangular number and the positive square root of $8n^2 + 1$ is called a Lucas-balancing number. The balancing numbers satisfy the recurrence relation $B_{n+1} = 6B_n - B_{n-1}$, for $n \geq 1$ with initial conditions $B_0 = 0$ and $B_1 = 1$, where B_n denotes the n-th balancing number. The first four balancing numbers are $1, 6, 35$ and 204 with balancers $0, 2, 14$ and 84 respectively. The n-th Lucas-balancing number is denoted by C_n and defined as $C_n = \sqrt{8B_n^2 + 1}$. These numbers satisfy the same recurrence relation as that of balancing numbers with different initials $C_0 = 1$ and $C_1 = 3$. It is observed that Lucas-balancing numbers are very closely associated with balancing numbers just like Lucas numbers are associated with Fibonacci numbers [7].

The balancing numbers and Lucas-balancing numbers are related to Pell and associated Pell numbers by several means. Every even Pell number is twice of a balancing number and the sum of first $2n-1$ Pell numbers is equal to the sum of n-th balancing number [8].

The balancing numbers satisfy many interesting identities. The Fibonacci numbers satisfy the strongly divisibility $F_{\gcd(m,n)} = \gcd(F_m, F_n)$, while balancing numbers satisfy $B_{\gcd(m,n)} = \gcd(B_m, B_n)$ [7]. The sum of first n odd terms of the sequence of balancing numbers is equal to square of the n-th balancing numbers, a property satisfied by the sequence of natural numbers. This property makes the sequence of balancing numbers a natural sequence.

The identity that connects three adjacent Fibonacci numbers is the famous Cassini formula, which is given by $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$. This formula is used to established many important properties involving Fibonacci numbers and their related sequences. Cassini formula for balancing numbers $B_{n-1}B_{n+1} - B_n^2 = 1$ which was introduced in [7], is also very useful to proof many important identities concerning balancing numbers.

2. The Balancing Transformation

Based on the sequence of balancing numbers, we develop a new transformation, balancing transformation which is applicable to digital image scrambling.

Definition 2.1. *Let $T_1 = a$, $T_2 = b$ and $T_n = 6T_{n-1} - T_{n-2}$ for $n \geq 3$, where a, b are non-negative integers. The sequence $\{T_n\}$ is called the generalized balancing sequence.*

When $a = 1, 3$ and $b = 6, 17$, then the generalized balancing sequence $\{T_n\}$ is the sequence of balancing numbers $\{B_n\}$ and the sequence of Lucas-balancing numbers $\{C_n\}$ respectively.

A repeated application of the recurrence relation for T_n yields the following result.

Theorem 2.1. *Let $\{T_n\}$ be the generalized balancing sequence defined by a and b and $\{B_n\}$ be the sequence of balancing number, then*

$$T_n = bB_{n-1} - aB_{n-2},\ n \geq 3.$$

Now we establish the Cassini formula for generalized balancing sequence T_n where $T_n = bB_{n-1} - aB_{n-2},\ n \geq 3$.

Theorem 2.2. *The Cassini formula for the sequence T_n is given by $T_{n+1}T_{n-1} - T_n^2 = -\mu$, where $\mu = a^2 - 6ab + b^2$.*

Proof. Since $T_n = bB_{n-1} - aB_{n-2}$, and using Cassini formula for balancing numbers, we have

$$\begin{aligned} T_{n+1}T_{n-1} - T_n^2 &= (bB_n - aB_{n-1})(bB_{n-2} - aB_{n-3}) - (bB_{n-1} - aB_{n-2})^2 \\ &= -a^2(B_{n-2}^2 - B_{n-1}B_{n-3}) - b^2(B_{n-1}^2 - B_nB_{n-2}) \\ &\qquad\qquad + ab(B_{n-1}B_{n-2} - B_nB_{n-3}) \\ &= -(a^2 - 6ab + b^2) = -\mu, \end{aligned}$$

which ends the proof. □

The following results are immediate consequence of Theorem 2.3.

Corollary 2.1. *For the sequence of balancing numbers $\{B_n\}$, $B_{n+1}B_{n-1} - B_n^2 = -1$.*

Corollary 2.2. *For Lucas-balancing sequence $\{C_n\}$, $C_{n+1}C_{n-1} - C_n^2 = 8$.*

Definition 2.2. *A generalized balancing sequence $\{T_n\}$ is called a distinguished generalized balancing sequence $\{D_{T_n}\}$ if T_n and T_{n+1} are relatively prime.*

For example, the sequence of balancing numbers $\{B_n\}$ is in $\{D_{T_n}\}$ as the consecutive balancing numbers are relatively prime.

Consider a sequence of consecutive distinct integers $\{0, 1, 2, \ldots, m-1\}$. It can be easily shown that, for a distinguished generalized balancing sequence $\{D_{T_n}\}$, the sequence of integers $\{S_k\}$, $S_k = (kD_{T_n} + r)\ mod\ D_{T_{n+1}}$, for $k = 0, 1, 2, \ldots, m-1$ is a permutation of the original sequence $\{0, 1, 2, \ldots, m-1\}$.

Keeping the above result in mind, we now define the balancing transformation as follows.

Definition 2.3. *For a given positive integer r, the balancing transformation is defined as: $S_k = (kB_n + r)\ mod\ B_{n+1},\ for\ k = 0, 1, 2, \ldots, B_{n+1} - 1$.*

Here the values of r play the role of secret key for balancing transformation. For different applications of this transformations, different values of r may be chosen.

The following results are shown in [7]. These results help to explain the uniformity and periodicity of the balancing transformations which we are going to introduce in the next section.

Proposition 2.1. *Let B_n is the n-th balancing number, then*

- $B_{2n}^2 - 1 = B_{2n+1}B_{2n-1}$.
- $B_{2n+1}^2 - 1 = B_{2n}B_{2n+2}$.
- B_{2n+2} *divides* $B_{2n+1}^2 - 1$.
- B_{2n+1} *divides* $B_{2n}^4 - 1$.

3. UNIFORMITY AND PERIODICITY OF THE BALANCING TRANSFORMATION

Periodicity of Fibonacci transformation was studied by Wall in the year 1960 [12]. Panda et al. studied the periodicity of balancing numbers modulo primes and modulo terms of certain sequences, which exhibit some important results, some of them are identical with the corresponding results of Fibonacci numbers while some others are more interesting [9]. They observed that the period of the balancing sequence coincide with the modulus of congruence if the modulus is any power of 2. Also, they claimed that there are three known primes for which $\pi(p) = \pi(p^2)$, where $\pi(p)$ denotes the period of the sequence of balancing numbers modulo prime, while there are no such primes are available till date for Fibonacci sequence. Some similar results are also studied using matrix algebra by Patel et al. in [10]. In this section, the uniformity properties and periodicity of balancing transformation are examined.

The following results show the uniformity property of balancing transformation. After applying this transformation to the results, it is observed that the adjacent pixels are uniformly distributed. For the sequence $\{S_k\}$, we have the following results from the above table.

Obsevation 3.1. *Let B_n, C_n and P_n be the n-th balancing number, n-th Lucas-balancing number and n-th Pell number respectively, then*

- $|S_{k+1} - S_k| = B_n$ *or* P_{2n+1}.
- $|S_{k+2} - S_k| = 2B_n$.
- $|S_{k+3} - S_k| = 3B_n$ *or* C_n.
- $|S_{k+4} - S_k| = 4B_n$.
- $|S_{k+B_{n-1}} - S_k| = 6$.

The equidistant pixels are scattered uniformly across the whole images by applying the balancing transformations to each row and then each column to the image. Consequently, the original image can be recovered by implementing the same transformation N times, this we call as balancing periodic transformation. Further, the period of the balancing transformation has a period depending on the values of B_n and B_{n+1}. It is observed that the period of the balancing transformation comes in terms of Pell numbers or Lucas-balancing numbers. In particular, the periods of even balancing numbers are in terms of Pell numbers while for odd balancing numbers, those are distinct Lucas-balancing numbers. In particular, $B_{2n} = P_{2n+1}$ and $B_{2n+1} = C_{n+2}$, where the key r is different for either P_{2n+1} and C_{n+2}. If we choose $r = P_{2n+1}$ for B_{2n} or C_{n+2} for B_{2n+1}, the period of balancing transformation is 2.

Zou et al. showed that the period of the Fibonacci transformation is either 2 or 4, depends on the size of the image [15]. As the period of the Fibonacci transformation is less, distortion of the image is poor. Lucas transformation gives the higher periodicity, as a result having more time complexity. The balancing transformation has less periodicity as compared to Lucas transformation and the distortion is high as compared to Fibonacci transformation, which eliminates the short coming of above two transformations.

3.1. **Examples of Scrambling Digital Images Based on Balancing Transformation.**

In the present study, we have used two different images to implement the entire work. The first one is Lena.jpg shown in Fig. 1(a) and other one is cameraman.jpg shown in Fig. 2(a). The main aim is to reduce the periodicity of balancing transformation, so that the time complexity is lesser. To do this, the balancing transformation is applied on original images [Fig. 1(a) and Fig. 2(a)], first row wise and then column wise. The transformed images of the original images after 7 and 20 iterations are shown in Fig. 1(b), Fig. 1(c), and Fig. 2(b), Fig. 2(c) respectively.

Fig. 1(a) Fig. 1(b) Fig. 1(c)

Figure 1.

Fig. 2(a) Fig. 2(b) Fig. 2(c)

Figure 2.

Peak Signal to Noise Ratio (PSNR) is error metrics used to compare image quality. It is used to find out how much distortion is there in the image. The PSNR is used in the transformed image of cameraman.jpg and Lena.jpg in Fig. 3.

In the above figure blue line indicates for Lena image and the red line indicates for cameraman image.

4. Conclusion

In this article, balancing transformation is introduced and the uniformity and periodicity of this transformation is discussed. A link between the periodicity of balancing transformations with Pell numbers and Lucas-balancing numbers is also developed.

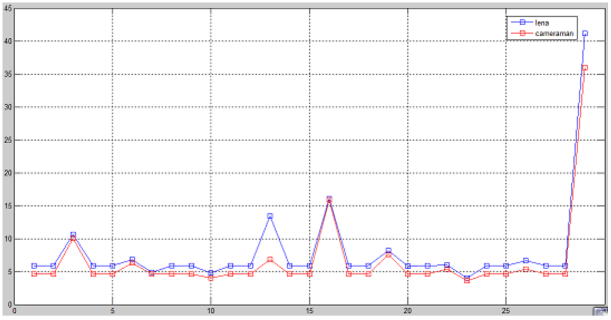

Fig. 3

FIGURE 3.

It is experimentally observed that as compared to Fibonacci transformation and Lucas transformation, balancing transformation over come both the poor distortion and higher periodicity, respectively.

References

[1] Bai, S., Cao, C., (2002), A novel algorithm for scrambling the details of digital image, Proceeding of the 4-th world congress on Intelligent Control and Automation, pp. 1333-1336.

[2] Behera, A., Panda, G. K., (1999), On the square roots of triangular numbers, The Fibo. Quart., 37 (2), pp. 98-105.

[3] Bing, L., Jia-wei, X., (2005), Period of Arnold transformation and it's application in image scrambling, J. Cent. South Univ. Tech., 12 (1), pp. 278-282.

[4] Chang, C., Lin, I., YU, Y., (2006), A new stenographic method for color and gray scale image hiding, Computer Vision and Image Understanding, 20.

[5] Dong-XU, Q., Jian-cheag, Z., Xiao-you, H., (2000), A new class of scrambling transformation and it's application in the image information covering, Since in China(Series E), 43 (3), pp. 307-312.

[6] Mishra, M., Mishra, P., Adhikary, M. C., Kumar, S., (2012), Image encryption using Fibonacci-Lucas transformation, Inter. Jour. On Cryptography and Information Security, 2(2), pp. 131-141.

[7] Panda, G. K., (2009), Some fascinating properties of balancing numbers, Proc. of the eleventh Inter. Conf. on Fibo. Nos. and Their Applications., Congr. Numer., 194, pp. 185-189.

[8] Panda, G. K., Ray, P. K., (2011), Some links of balancing and cobalancing numbers with Pell and associated Pell numbers, Bulletin of the Institute of Mathematics, Academia Sinica (New Series), 6(1), pp. 41-72.

[9] Panda, G. K., Rout, S. S., (2014), Periodicity of Balancing numbers, Acta Math. Hungar., 143(2), pp. 274-286.

[10] Patel, B. K., Ray, P. K., (2016), The Period, Rank and Order of the sequence of Balancing numbers Modulo m, Math. Reports, 18(68), pp. 395-401.

[11] Qi, D. X., (1999), Matrix transformation and its applications to image hiding, J. North China univ. of tech., 11(1), pp. 24-28.

[12] Wall, D. D., (1960), Fibonacci Series Modulo m, Amer. Math. Monthly, 67, pp. 525-532.

[13] Zou, J. C., Ward, R. K., (2003), Introducing Two New Image Scrambling Methods, Proc. of IEEE Pac. Rim Conf. on Comm., Comp. and Sig. Proc., pp. 708-711.

[14] Zou, J. C., Ward, R. K., (2003), Some novel image encryption methods based on chaotic dynamical systems, Proc. of the 9th Joint Inter. Computer Conf., Zhuhai, Chaina, pp. 188-191.

[15] Zou, J. C., Ward, R. K., Qi, D. X., (2004), The generalized Fibonacci transformations and application to image scrambling, Proc. of the IEEE Inter. Conf. on Acoustic, Speech and Signal Proc., Canda, pp. 385-388.

Prasanta Kumar Ray is currently working as a Professor in the School of Mathematical Sciences, Sambalpur university, India. He has more then twenty five years of teaching and research experiences. Prof. Ray has published over thirty five peer reviewed papers in reputed national and international journals.

Bijan Kumar Patel is currently a postdoctoral fellow in the Department of Mathematics, Indian Institute of Science Education and Research (IISER) Bhopal, India. He received his Doctor degree in Mathematics from International Institute of Information Technology Bhubaneswar, India. His research interest includes Number Theory and Cryptography. Dr. Patel has published over ten peer reviewed papers in reputed international journals.

Debbrota Paul Chowdhury is currently a PhD scholar in the Department of Computer Science and Engineering, National Institute of Technology, Rourkela, India. He received his Masters degree in Computer Science and Engineering from International Institute of Information Technology, Bhubaneswar, India and Bachelors degree in Computer Science and Engineering from University Institute of Technology, Burdwan, India. His research interest includes image processing, computer vision, bio-metrics, machine learning and deep learning.

Satyapriya Kujur has undergone summer internship at International Institute of Information Technology, Bhubaneswar under the guidance of Prof. P. K. Ray. She received her Master of Science degree in Mathematics from National Institute of Technology, Rourkela in 2016. Currently, she is pursuing her Post Graduate Diploma in Rural Management from Xavier Institute of Social Service, Ranchi, India.