A Novel Algorithm for Generating pseudo Random Number

Gangyi Hu, Weili Kou
College of Big Data and Intelligence Engineering, Southwest Forestry University
Kunming, China
{hugangyi604@126.com} {kwl_eric@163.com}

*Sumeth Yuenyong
Department of Computer Engineering, Faculty of Engineering, Mahidol University, Bangkok, Thailand
{sumeth.yue@mahidol.ac.th}

Jian Qu
Department of Engineering technology, Panyapiwat Institute of Management, Bangkok, Thailand
{lordjohnquest@gmail.com}

Journal of Digital Information Management

ABSTRACT: *This paper proposes a pseudo random number generation algorithm based on cellular neural networks. It used the hyper-chaos characteristics of the cellular neural networks and sets the appropriate parameters to generate the pseudo random number. The experimental results show that, compared with other similar algorithms, this algorithm has the characteristics of simple operation, low complexity, large key space, and good randomness. It can meet the needs of secure communication and network information security, which has good application prospects.*

Subject Categories and Descriptors: [C.1.3 Cellular Architecture]; [C.2 Computer-Communication Networks]; Security and protection; **[F. 2.1 Numerical Algorithms and Problems]**

General Terms: Cellular Networks, Random Number, Numerical Algorithms, Network Security

Keywords: Cellular Neural Networks, Chaotic System, Pseudo-random Number

Received: 11 January 2020, Revised 31 March 2020, Accepted 5 June 2020

Review Metrics: Review Scale: 0/6, Review Score- 5.02, Inter-reviewer consistency: 77.5%

DOI: 10.6025/jdim/2020/18/4/151-156

1. Introduction

The random number has an important effect on the data encryption, network information security, image communication and satellite navigation. Studying the algorithm which cangenerate the random number with high randomnessis becoming an important topic of information security. At present, some common algorithms such as taking the middle number or the congruence method. Because of the generation circle of the pseudo random number depends on the initial values, The statistical performance of these pseudo random numbers is not perfect[1-2]. Some other method such as shift registered sequence generator and compound prime number generator also have weak random performance[3-4]. Bo proposed a random sequence algorithm based on knight cruising, which can achieve good randomness, but the knight cruising path is complex[5]. Han proposed an algorithm to generate the pseudo random number based on the discrete chaotic synchronization system, and Dong proposed an algorithm to generate the pseudo random number based on the cellular neural networks[6-7]. Both of these two algorithms use multiple chaotic iteration to generate pseudo random numbers. Although they can obtain high performance pseudo random sequences, they also have some problems such as computational complexity and low utilization because of multiple chaotic iterations. In addition, there are also some other algorithms to generate

pseudo random number based on high dimensional chaotic. Wang[8] generated a pseudo random sequence of good random performance by using a three-dimensional Lorenz system. Qi[9] designed a pseudo random number generator using the discrete hyper chaotic mapping system. Although these methods can increase the key space, the weakness is that its cycle is short.

With the purpose of generating pseudo random sequences according to high random performance. We propose an algorithm to generate pseudo random numbers based on the Cellular Neural Networks. It used the hyperchaos characteristics of the Cellular Neural Networks to produce six dimensional chaotic random sequence in high performance. The pseudo-random sequence which is generated by this algorithm is fast and has non repetitive. The experimental results show that these pseudo random sequences had the characters such as the strong sensitivity of the initial value, the key space are large, the speed is fast and can meet the requirement of the detection standard of the National Institute of Standards and Technology (NIST).

2. The Cellular Neural Networks (CNN)

The Cellular Neural Networks was proposed by L.O.Chua[10]. Its basic unit are cells, which are arranged in a planar 2-D lattice. CNN's unique characteristic that sets it apart from other types of neural network is local connectivity; each cell only have connections to cells within its neighborhood. Denoting the cell at row *i* and column *j* as C_{ij}, its neighborhood can be defined as

$$N_{ij}(r) = \{C_{ab} \mid max(|a-i|, |b-j|) \le r, 1 \le a \le M, 1 \le b \le N\} \quad (1)$$

Where $1 \le i \le M, 1 \le j \le N, r$ is the radius of the neighborhood of cell C_{ij}, and C_{ab} is the neighbor cell of cell C_{ij}.

A cell is composed of a circuit which can be modeled by the first order nonlinear differential equation.

$$C\frac{dx_{ij}(t)}{dt} = -\frac{x_{ij}(t)}{R_x} + \sum_{k,\, l \in N_{ij}(r)} A_{kl} y_{kl}(t) + \sum_{k,\, l \in N_{ij}(r)} B_{kl} u_{kl} + I_{ij} \quad (2)$$

Where x_{ij} is a state variable, y_{kl} the outputs of cells, u_{kl} is the input of cells, C and R_x are system constants, I_{ij} is the threshold, A is the feedback parameter matrix and B is the control parameter matrix. The subscripts after the matrices in the equation denote the matrix elements. The behavior of *CNN* is defined by these parameter matrices. Finally, the output equation of *CNN* is given by

$$y_{ij}(t) = \frac{1}{2}(|x_{ij}(t)+1| - |x_{ij}(t)-1|) = f(x) \quad (3)$$

In order to get chaotic sequences to be used for encryption, we utilized a 6-units *CNN*. Since this is a small size, the neighborhood was defined to be the entire network. The challenge was to discover the proper values for the parameter matrices A, B and I that give rise to chaotic state evolution. In order to get these values, we set the system constants to $C = 1$ and $R_x = 1$, then performed a grid-based parameter search. One parameter set that we discovered that give rise to chaotic state evolution is shown in (4).

$\boldsymbol{A} = \mathbf{0}$ except $a_{44} = 404$; $I = 0; 0$

$$B = \begin{bmatrix} 0 & 0 & -1 & -1.2 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 \\ 11 & -12 & 0 & 0 & 0 & 0 \\ 92 & 0 & 0 & -95 & 1 & -1 \\ 0 & 0 & 5 & 0 & -1 & 0 \\ 0 & 0 & 0 & 5 & 0 & -12 \end{bmatrix} \quad (4)$$

Substituting (3) and (4) into (2) and simplifying, we obtained the following state evolution equations for each of the 6 cells in the network. Note that we dropped the second subscript and simply use a single subscript to denote the different cells of the network.

$$\begin{cases} \frac{dx_1}{dt} = -x_3 - 1.2 * x_4 \\ \frac{dx_2}{dt} = 2 * x_2 + x_3 \\ \frac{dx_3}{dt} = 11 * x_1 - 12 * x_2 \\ \frac{dx_4}{dt} = 92 * x_1 - 95 * x_4 + x_5 - x_6 + 202 * (|x_4 + 1| - |x_4 - 1|) \\ \frac{dx_5}{dt} = 5 * x_3 - x_5 \\ \frac{dx_6}{dt} = 5 * x_4 - 12 * x_6 \end{cases} \quad (5)$$

Using (5), the Lyapunov exponents of this system are -0.3824, 0.1283, 0.1596, -0.3995, -1.3580, -0.5473 respectively. There are two positive values in these Lyapunov exponents ,which means that this system is hyperchaotic system. The step-size parameter *h* can be chosen freely to a small value, which we set at 0.005. The initial value of x_i (where $i = 1, 2...6$) can be set to arbitrary values, each with any number of digits (up to machine precision). The initial state is the seed that starts the generation of chaotic sequence from the evolution of x_i. As long as the parameters given in (4) is used. As an example, when the initial state is set as $x_1(0) = 0.1, x_2(0) = x_3(0) = x_4(0) = x_5(0) = x_6(0) = 0.2$; the *CNN* generates chaotic attractors as shown in Figure 1. In the actual application, the above seven parameters (x_i ($i = 1, 2...6$) and h) can be set to any digit length value, it can greatly increases the key space.

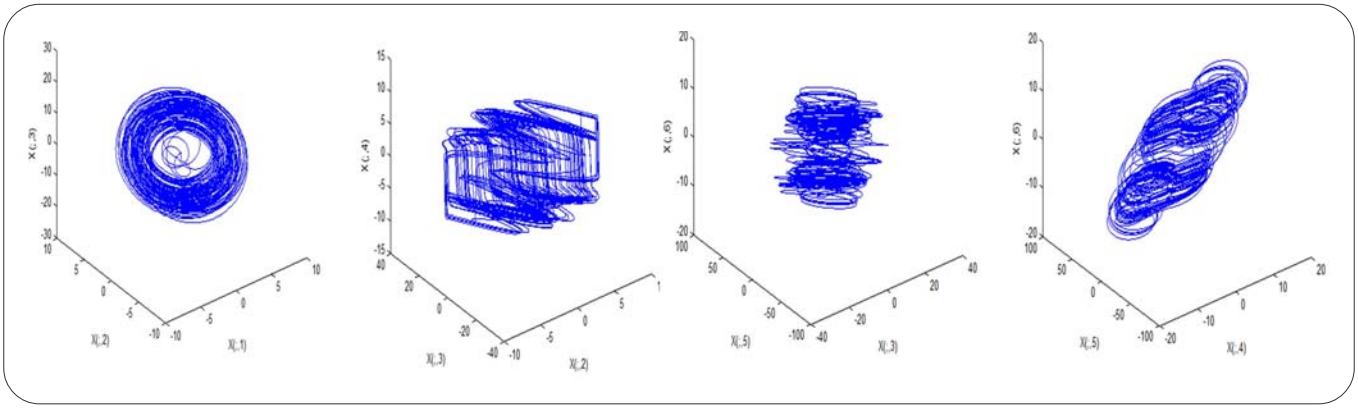


Figure 1. Some chaotic attractors generated by the 6D CNN

The Figure 1 shows that the CNN system can generate chaotic system with the appropriate parameters. These chaotic systems had the characteristic such as ergodicity, boundedness and strong randomness. Which can be used for the secrecy communication.

3. The Method of Generating Pseudo Random Number

Because the Cellular Neural Networks has good performance of chaotic characteristics, the pseudorandom number which is generated by the Cellular Neural Networks depends on the key $x_i\,(i = 1, 2...6)$ and step size h. In order to avoid the chaos degradation caused by the finite precision, the six output data from the iteration set as the feedback for the new input values each time to obtain the pseudo random number with good performance. The main steps to generate pseudorandom numbers are as follows.

1. set the constant coefficient value of the Cellular Neural Networks system, step size and other initial parameters values (x_i). These seven parameters (x_i and h) are also being as the key of the Cellular Neural Networks system, they can be set as any number of arbitrary digits.

2. After iterate the formula (5) several times to eliminate the initial effect. The formula (5) iterated once again, which can obtain six output values. These six values are taken as the values of the first sequence. $\{x_1(k), x_2(k), x_3(k), x_4(k), x_5(k), x_6(k) \mid k = 0, 1, 2, ...\}$.

3. Take the above six output values set as the new input value $x_i\,(i = 1, 2...6)$ for the Cellular Neural Networks system, and then iterate again.

4. According to the length of the pseudorandom sequences in practical application, repeat the above step 3 to get the final pseudo random sequences.

4. Security Analysis

4.1 The Key Space Analysis

With the purpose of resisting the enumerated attack, the key space for generating the pseudo random sequence should belarge enough. Our method used the different initial values (x_i and h) to obtain the different pseudo random sequences. In this algorithm, the seven parameters (x_i and h) can be set as any number of arbitrary digits. Its key space depends on the actual precision of the computer. Suppose that a 64 bit computer is used, the key space can be reached to 7×2^{64}.The key space are very large, which can effectively to resist exhaustive attack.

4.2 The Randomness Analysis

According to the randomness testing method which is proposed by the NIST800-22[11]. The pseudo random sequence generated by this algorithm is tested for comprehensive way. Every test will get one P_value. When the test result to satisfy $P\_value \geq 0.01$, it is considered that the sequence is random in the test. When the test result to satisfy$P_value < 0.01$, the sequence is considered as nonrandom in the test. We used the **sts-2.1.1** software for testing these six groups chaotic sequences' randomness which was generated by this algorithm. The test results are shown in Table 1.

From the test results of Table 1, it shows that in each test result, the conditions are satisfied ($P\_value \geq 0.01$), the sequences generated by this algorithm can satisfy the NIST completely , which means that this sequence is randomness.

4.2 Analysis the Effect of Image Encryption

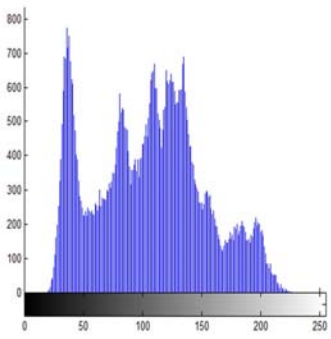
The pseudo random sequence is widely used in secure communication. We use the pseudo random sequence which was generated by this algorithm for image encryption, the encrypted method used the image pixel XOR and position scrambling. The test 8bit gray image is the Lena and Cameraman image. The cipher image and the histogram of the cipher image are shown in Figure 2.

The pseudo random sequence generated by this algorithm is applied to image encryption, and compared with other algorithms. The number of pixel changed ratio (NPCR) and the information entropy (IE) is shown in Table 2.

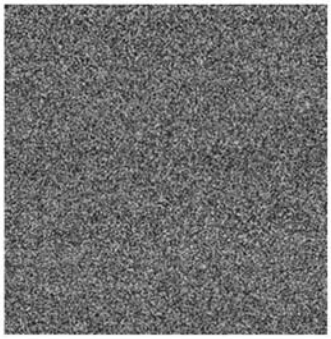
Test Type	Testvalues (group 1)	Testvalues (group 2)	Testvalues (group 3)	Testvalues (group 4)	Testvalues (group 5)	Testvalues (group 6)
Frequency	0.7058	0.6140	0.7973	0.5761	0.8713	0.4654
Block Frequency	0.8876	0.7723	0.9755	0.5001	0.8857	0.2108
Cumulative Sums	0.6782	0.5861	0.7132	0.6045	0.6878	0.3328
Runs	0.6023	0.6023	0.6023	0.6023	0.6023	0.6023
Rank	0.4019	0.2453	0.4019	0.2453	0.4019	0.2453
Discrete Fourier Transform	0.1742	0.1654	0.0565	0.2036	0.4132	0.1655
Overlapping Template Matching	0.3061	0.2101	0.2101	0.3061	0.2101	0.2101
Universal Statistical	0.5046	0.4578	0.3451	0.1979	0.2451	0.0824
Approximate Entropy	0.2804	0.2021	0.3328	0.1051	0.3670	0.3206
Random Excursions Variant	0.2825	0.3032	0.3216	0.2344	0.3542	0.2043
Serial	0.5088	0.4508	0.4960	0.3898	0.3445	0.3034
Linear Complexity	0.6125	0.5215	0.2074	0.4637	0.5032	0.2188

Table 1. The test results from NIST800-22

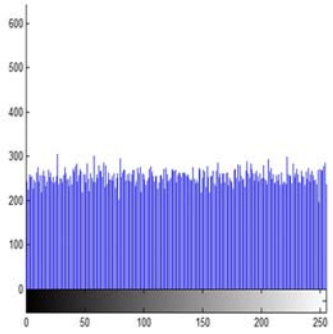
(a) The lena original image



(b) The histogram of original image

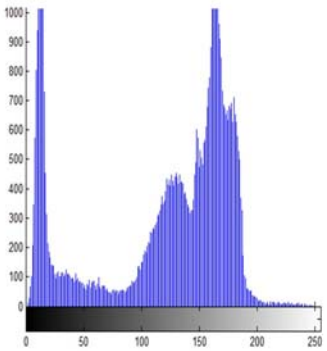


(c) The cipher image

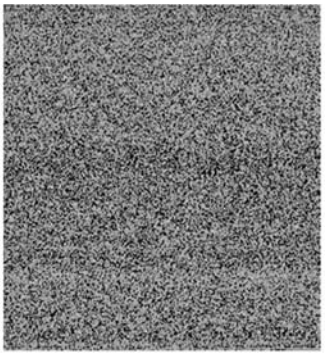


(d) The histogram of cipher image

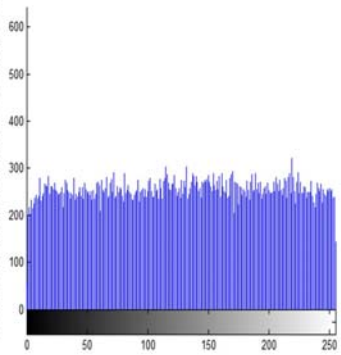
(e) The cameraman original image



(f) The histogram of original image



(g) The cipher image



(h) The histogram of cipher image

Figure 2. The pseudo random sequence generated by this algorithm is used for image encryption effect

	Algorithms	NPCR	IE
Lena (256 × 256)	The Reference [12] method	0.9932	7.989
	The Reference [13] method	0.9953	7.989
	Our method	0.9960	7.991
Cameraman (256 × 256)	The Reference [12] method	0.9938	7.988
	The Reference [12] method	0.9938	7.988
	Our method	0.9961	7.992

Table 2. The image encryption effect by using different algorithms

The Table 2 shows that using our algorithm for image encryption, the number of pixel changed ratio (NPCR)and information entropy (IE) are greater than other algorithms. Which means that the pseudo random sequence obtained from the Cellular Neural Networks has good applicability and can resist statistical attacks well.

5. Conclusion

In this paper, we proposed a new pseudo random number generation method which is designed by using the hyper chaotic system of six dimensional Cellular Neural Networks. It adjusted the initial input value of the Cellular Neural Networks system automatic iterated many times to obtain the pseudo random number. Compared with other algorithm by using the Cellular Neural Network system and Logistic mapping together to generate pseudo random numbers, this algorithm is simple and has the character of low complexity. At the same time, these pseudo random sequences generated by our algorithm shows that it has large key space and perfect randomness. The experiments show that this algorithm can be applied to secure communication very well, and it can meet the needs of network information security and expand the application of chaotic system in cryptography.

Declaration

Funding

This project was supported by the Doctoral Research Foundation of Southwest Forestry University (grant number 111802),it was also supported by the National Natural Science Foundation of China(grant number 31760181 and 61261013).

Conflict of Interest

The authors hereby declare that they have no conflict of interest.

Data Availability

Data Availability statement

The datasets used to support the finding of this study are included with the article.

References

[1] Li Jetc. (2018). Efficient deterministic and non-deterministic pseudo-random number generation, *Mathematics and Computers in Simulation*. 1 (1) 143, 114 - 24.

[2] Bahi, J. M. (2017). An optimization technique on pseudo-random generators based on chaotic iterations, arXiv preprint arXiv, 27 (1) 1706 - 1713.

[3]Hamza, R. (2017). A novel pseudo random sequence generator for image-cryptographic applications, *Journal of Information Security and Applications*. 8 (1) 19-27.

[4] Hue, T. T. (2017). Complexity and properties of a multidimensional Cat-Hadamard map for pseudo random number generation, *The European Physical Journal Special Topics*. 226 (10) 2263-80.

[5] Sen, BAI. (2017). Method to generate the pseudo random sequence based on the statistical properties, *Chinese Journal of Network and Information Security*, 3 (1) 31-38.

[6] Li-hua, Dong. (2016). Method for generating pseudo random numbers based on cellular neural network, *Journal of Communications*, 37 (Z1) 85-91.

[7] Shuang-shuang, Han. (2013). Generalized Synchronization theorem based chaotic pseudo random number genetrator and performance analysis, *Applicaition Research of Computers*, 30 (5) 1512-1514.

[8] Wang, X. (2013). Cryptanalysis of a parallel subimage encryption method with high-dimensionalchaos, *Nonlinear Dynamics*, 73 (1-2) 795 -800 .

[9] Qi, Y. B., Sun, K. H., Wang, H. H. (2015). The design and performance analysis of hyper-chaotic pseudo-random sequence generator, *Computer Engineer and Applications*. 53 (4) 135-139.

[10] Chua, L. O., Yang, L. (1988). Cellular neural networks: theory. IEEE Transactions on Circuits & Systems, 35 (10) 1257-1272.

[11] Rukhin, A., Soto, J., Nechvatal, J. (2010). A statistical test suite forrandom and pseudo-random number

generators for cryptographic applications. Andrew Rukhin Juan Soto James Nechvatal Miles SmidElaine, 59 (4) 2289-2297.

[12] WANG, Y. H. (2010). The design and applications of PRNG based on Henonmap with parameter perturbation. *Journal of Chinese Information Processing*, 59 (4) 2289-2297.

[13] HOSSAIN, M. B., RAHMAN, M. T., RAHMAN, B. M. S. (2014). A new approach of image encryption using 3D chaotic map to enhance security of multimedia component. *International conference on Informatics, Electronics & Vision*. 1-6.

[14] OJSE, Assad., Chetto, M. (2017). Design and analysis of two stream ciphers based on chaotic coupling and multiplexing techniques. *Multimedia Tools Applications*. 1 (6) 1–27

[15] Han D, Min L, Hao L).A chaos robustness criterion for 2d piecewise smooth map with applications in pseudorandom number generator and image encryption with avalanche effect. *Mathematical Problems in Engineering* 10 (1) 1–14

[16] Huang, L., Shi, D., Gao, J. (2016). The design and its application in secure communication and image encryption of a new lorenz-like system with varying parameter. *Mathematical Problems in Engineering*, 1–11.

[17] Lin, M., Long, F., Guo, L . (2016). Grayscale image encryption based on latin square and cellular neural network. *In*: Control and Decision Conference (CCDC), 2016, IEEE, 2787–2793

[18] Runhe, Q., Zhu, C., Liu, S. (2015). A chaos image encryption algorithm based on binary sequence and baker mapping, *International Industrial Informatics and Computer Engineering Conference* (IIICEC 2015), Xi'an, China.

Author Biography

Gangyi Hu received the B.E. in Communication Engineering and the M.E. degree in Communication And Information System from Chongqing University of Posts and Telecommunications, Chongqing, China, in 2005 and 2010, respectively. He received the Ph.D. degree in Information Technology at Shinawatra University, Thailand. He research interests are neural networks, image processing and Embedded Systems.

Jian Qu received Ph.D. in information technology with Outstanding Performance award from Japan Advanced Institute of Science and Technology, Japan, in 2013. He received B.B.A in business administration with Summa Cum Laude honors from Institute of International Studies of Ramkhamhaeng University, Thailand, in 2006, and M.S.I.T in Information technology from Sirindhorn International Institute of Technology, Thammast university, Thailand, in 2010. His research interests are natural language processing, artificial intelligence, machine learning, machine translation, information retrieval and image processing.

Sumeth Yuenyong received the B.E. in Electrical Engineering the M.E. degree in Embedded Systems and the Ph.D. degree from Sirindhorn International Institute of Technology, Thailand, in 2004 and 2010, respectively. He received the Ph.D. in Communication and Integrated Systems at Tokyo Institute of Technology. He research interests are signal processing, neural networks and biomedical application of signal processing algorithms.

Weili Kou received the B.E. in Computer Science and Technology, the M.E. degree in Forest Management from Southwest Forestry University, Kunming, China, in 2003 and 2008, respectively. He received the Ph.D.degree in Geographic information system from Kunming University of Science and Technology in 2015. He researched interests are GIS, Remote Sensing and Forest information.