TELKOMNIKA, Vol.11, No.2, June 2013, pp. 409~416
ISSN: 1693-6930
accredited by DGHE (DIKTI), Decree No: 51/Dikti/Kep/2010

A Bidirectional Generalized Synchronization Theorem - Based Chaotic Pseudorandom Number Generator

Han Shuangshuang[1, 3], Min Lequan[1, 2]
[1]Schools of Automation and Electrical Engineering, University of Science and Technology Beijing, China;
[2]Schools of Mathematics and Physics, University of Science and Technology Beijing, China
[3]Beijing Command College of Chinese People's Armed Police Force, China
e-mail: shuangert1@126.com[3]; minlequan@sina.com[2]

Abstrak

paper ini memperkenalkan suatu sistem baru yaitu 5-dimensional bidirectional generalized chaos synchronization system (BGCSDS), untuk mendesain suatu pembangkit nilai pseudorandom yang baik, dengan menggunakan teorema sinkronisasi tergeneralisasi dua arah (bidirectional generalized synchronization) untuk suatu sistem chaotic. Purwarupa dari sistem ini yang berupa sistem chaotic baru. Simulasi numerik menunjukkan bahwa dua pasangan variabel dari BGCSDS mencapai sikronisasi acak tergeneralisasi melalui suatu transformasi H. Sebuah pembangkit nilai acak yaitu chaos-based pseudorandom number generator (CPNG) didesain dengan BGCSDS yang baru. Pengujian dengan menggunakan FIPS-140-2 tests yang diterbitkan oleh National Institute of Standard and Technology (NIST) dipilih untuk membuktikan tingkat keacakan (randomness) dari urutan 1000 buah bilangan biner yang dibangkitkan dengan CPNG dan algoritma RC4. Hasil yang diperoleh menunjukan bahwa semua urutan yang diuji telah lulus tes FIPS-140-2. Analisis confidence interval menunjukkan bahwa sifat statistik dari keacakan urutan yang dibangkitkan dengan CPNG dan algoritma RC4 algorithm tidak memiliki perbedaan yang signifikan. Jadi, CPNG sesuai untuk digunakan di bidang sekuriti.

Keywords*: sinkronisasi tergeneralisasi; urutan acak semu (pseudo-random sequence), tes FIPS-140-2, sistem diskret dua arah*

Abstract

In order to design good pseudorandom number generator, using a bidirectional generalized synchronization theorem for discrete chaos system, this paper introduces a new 5-dimensional bidirectional generalized chaos synchronization system (BGCSDS), whose prototype is a novel chaotic system. Numerical simulation showed that two pair variables of the BGCSDS achieve generalized chaos synchronization via a transform H. A chaos-based pseudorandom number generator (CPNG) was designed by the new BGCSDS. Using the FIPS-140-2 tests issued by the National Institute of Standard and Technology (NIST) verified the randomness of the 1000 binary number sequences generated via the CPNG and the RC4 algorithm respectively. The results showed all the tested sequences passed the FIPS-140-2 tests. The confidence interval analysis showed the statistical properties of the randomness of the sequences generated via the CPNG and the RC4 algorithm do not have significant differences. So, the CPNG is suitable to be used in the information security filed.

Keywords*: generalized synchronization; pseudo-random sequence, FIPS-140-2 tests, bidirectional discrete system*

1. Introduction

As a nonlinear dynamics phenomenon, chaos has many properties to be worthwhile use, such as pseudo-random characteristics, the unpredictability of the orbit, and the extreme sensitivity of the initial state and so on [1]. The feature of chaotic systems which makes them suitable for generating pseudo-random sequence is important. One way is to use a single chaotic map, such as Tent map [2], Henon map [3] and so on [4]-[5]. Another way is to extend or compound some common chaotic maps, such as Logistic map [6]-[7], Henon map [8]. By summarizing the literatures, it is found that the extension methods are simple addition, improved and coupled mostly. Using the existing chaotic theorem to extend the chaotic maps is still in some sense.

Since the earlier work of Pecora and Carroll [9], chaos synchronization (CS) based on cryptography communication research has attracted much attention [10]-[12]. Generalized

Received January 30, 2013; Revised March 9, 2013; Accepted March 25, 2013

chaotic synchronization (GCS) is one of the focal research topics in CS, which provides a new tool for constructing secure communication systems [13]-[14].

Based on a bidirectional generalized synchronization theorem for discrete chaos system in [15], a novel BGCSDS was introduced. By a transformation from the real set to the integer set, a chaos-based pseudo-random number generator (CPNG) was designed. The key set was initial condition and system parameters of the BGCSDS.

Let the key set be perturbed randomly by $|\Delta|$ for 1000 times where $10^{-16} < |\Delta| < 10^{-5}$. We verify the randomness of the binary number sequences by the FIPS 140-2 tests, and compare the correlation coefficients and the percentages of the different bits between two different key steams. The outputs of the CPNG are passed the tests. Comparing with the confidence intervals between the CPNG and the RC4 algorithm, it shows that the randomness of the sequences generated via the two ways do not have significant differences.

2. Algorithm

To design the CPNG based on GCS for bidirectional discrete system, some basic concepts are introduced.

Definition 1: Consider two discrete systems

$$X(k+1) = F(X(k), Y(k)) \tag{1}$$

$$Y(k+1) = G(Y(k), X(k)) \tag{2}$$

where $X(k) = (x_1(k),...,x_n(k))^T \in R^n$, $Y(k) = (y_1(k),...,y_m(k))^T \in R^m$,
$F(X(k), Y(k)) = (f_1(X(k), Y(k)),...,f_n(X(k), Y(k)))^T$, $G(Y(k), X(k)) = (g_1(Y(k), X(k)),..,g_m(Y(k), X(k)))^T$.

If there exists a transformation $H : R^n \to R^m$ and a subset $B = B_X \times B_Y \subset R^n \times R^m$ such that all trajectories of (1), (2) with intial conditions $(X(0), Y(0)) \in B$ satisfies $\lim_{k \to +\infty} || H(X(k)) - Y(k) || = 0$, then the systems in (1) and (2) are said to be in GS with respect to the transformation H.

Theorem 1 [15]**:** If two bidirectional discret sysems (1) and (2) are in GS with respect to the transformation H given by Definition 1. Then the $G(Y(k), X(k))$ in (2) has form

$$G(Y, X) = H(F(X, Y) - Q(X, Y)) \tag{3}$$

where $F(X) = (f_1(X,Y), f_2(X,Y),...,f_m(X,Y))^T$ and $Q(X,Y) = (Q_1(X,Y), Q_2(X,Y),...,Q_m(X,Y))^T$ makes the zero solution of the error equation

$$e(k+1) = H(X(k+1)) - Y(k+1)) = Q(X, Y) \tag{4}$$

be asymptotically stable.

3. Research Method

In this section, a novel discrete chaotic system could be constructed using the Theorem 1, and then a new CPNG based on the BGCSDS is designed. The last procedure is to verify the randomness of binary sequence generated via the CPNG. All the simulations are implemented using Matlab 7.0.

3.1. A New BGCS Discrete System

Suppose the discrete chaotic system has the form[16]:

$$\begin{cases} x_1(k+1) = a_{11}x_1(k) + a_{12}x_2(k) \bmod 1 \\ x_2(k+1) = a_{21}x_1(k) + a_{22}x_3(k) \bmod 1 \\ x_3(k+1) = a_{31}x_2(k) \bmod 1 \end{cases} \quad (5)$$

Its largest Lyapunov exponent is 0.964763, which shows the system is chaotic.

Let the chaotic system (5) be amended as follow:

$$\begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \end{pmatrix} = (\begin{pmatrix} a_{11}x_1(k) + a_{12}x_2(k) \\ a_{21}x_1(k) + a_{22}x_3(k) \\ a_{31}x_2(k) \end{pmatrix} + A(Y(k))x_3(k)) \bmod 1 \quad (6)$$

where $A(Y(k)) = \left(a_1, a_2 y_1(k), a_3 y_2(k)\right)^T$.

Based on the Theorem 1, the system (5) is extended to 5-dimensional system, where $\left(y_1(k), y_2(k)\right)^T$ can be gotten by the GCS of the variables $\left(x_1(k), x_2(k), x_3(k)\right)^T$ and $\left(y_1(k), y_2(k)\right)^T$. Denote the transform $H : R^3 \to R^2$ have the following form:

$$H(X(k)) = \Lambda X(i) = \Lambda\left(x_1(k), x_2(k), x_3(k)\right)^T \quad (7)$$

where $\Lambda = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix}$

Let $e(k+1) = 0.5e(k)$, and then $Q(X,Y) = 0.5(Y(k) - H(X(k)))$ makes the error equation (4) zero asymptotically stable.

Hence the system (2) has the form:

$$Y(k+1) = \begin{pmatrix} y_1(k+1) \\ y_2(k+1) \end{pmatrix} = \Lambda X(i+1) - 0.5(H(x(k)) - Y(k)) \quad (8)$$

3.2. Chaotic Pseudo-random Number Generator

In order to transform the streams of the BGCSDS into key streams with integers $\{0,1,\cdots,255\}$, a transformation T is introduced. Denote $X(k) = k_1 x_1(k) y_2(k) + k_1 x_3(k) y_1(k)$, where $k_1 = \sqrt{3}, k_2 = \sqrt{5}$. Let the transform T be defined by:

$$T(X(k)) = \mathrm{mod}(round(\frac{\sqrt{2} \times 10^5 \times 255(X(k) - \min(X))}{(\max(X) - \min(X))}), 256) \quad (9)$$

where $\min(X) = \min\{X(k) | k=1,2,\cdots N\}$, $\max(X) = \max\{X(k) | k=1,2,\cdots N\}$.

Then the binary sequence $s(k)$ can be obtained by transferring $T(X(k))$ into binary codes:

$$s(k) = binary(T(X(k))), k = 1,2,\cdots N \quad (10)$$

Hence, we obtain a chaotic pseudo-random number generator (CPNG).

4. Results and Discussion

The chaotic trajectories of the BGCSDS and the characteristics of the pseudorandom sequence generated via the formula (10) are simulated and analyzed in this section.

4.1. Chaotic trajectories of The BGCSDS

In system (6), we select the following parameters and initial conditions $X(0)=(0.5,0.5,0.5)^T$, $Y(0)=H(X(0))$, $[a_1,a_2,a_3]=[0,1,-1]$ and $[a_{11},a_{12},a_{13},a_{21},a_{22},a_{23}]=[1,2,1,0,1,1]$. By calculating the Lyapunov exponents of the 5-dimensional system, two positive Lyapunov exponents 0.69507 and 0.48318 can be obtained. It shows the system (6) is chaotic. Then the trajectories of system (6) and (8) are shown in Figure 1. From (d), it can be seen that the two pair of variables are in GCS with respect to H, so it is in line with expectations.

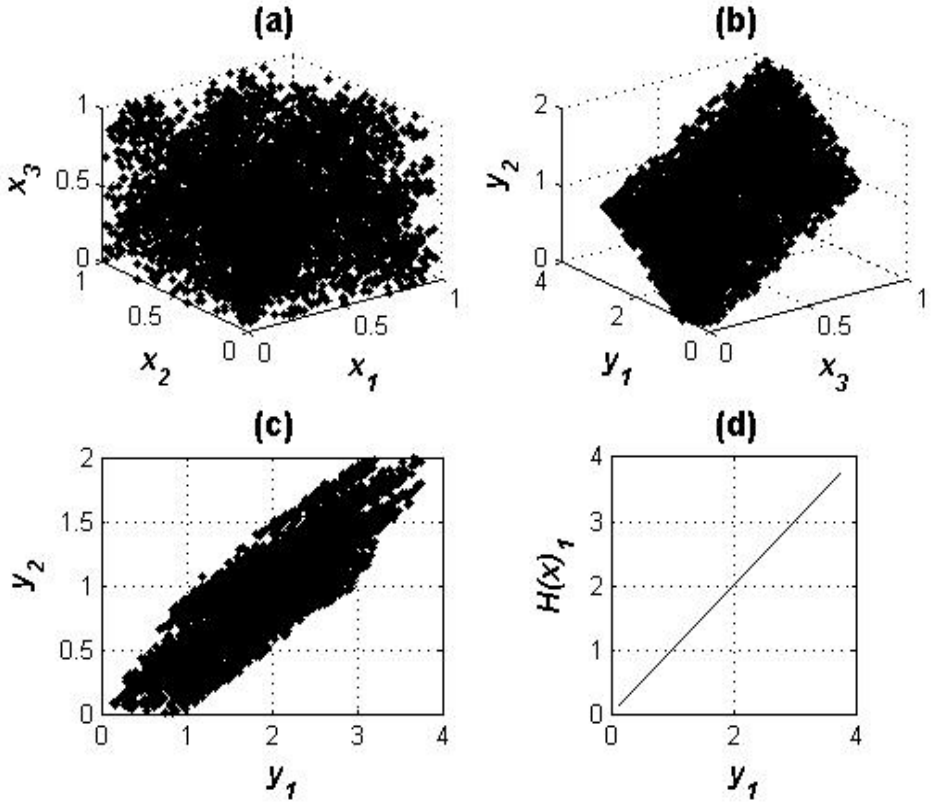

Figure 1. Chaotic trajectories: (a) $x_1-x_2-x_3$; (b) $y_1-y_2-y_3$; (c) y_1-y_2; (d) $y_1-H(x)_1$

4.2. Key Space of the CPNG

We choose the system parameters $\{a_1,a_2,a_3,a_{11},a_{12},a_{13},a_{21},a_{22},a_{23}\}$ and the initial condition $(x_1(0),x_2(0),x_3(0),y_1(0),y_2(0))^T$ as the key set of the CPNG. Let the key set be perturbed randomly by $|\Delta|$ for 1000 times where $10^{-16}<|\Delta|<10^{-5}$, and then compare the correlation coefficients and the percentages of the different bits between two different key steams. The comparing results are shown in Table 1. The computed mean of the percentages of the different bits is about 49.9961%, which is very close to the ideal value 50%. While the mean of the correlation coefficients is 0.00569. The above results imply that two different key streams are almost completely independent. Consequently we can assume that the key space of the CPNG is large than $10^{11\times12}>2^{396}$.

Table 1. The percents of the variations and the correlation coefficients among 1000 group key streams

	minimum	maximum	mean
Corrcoef(abs)	2.68×10^{-7}	0.0312	0.00569
Percents (%)	48.4412	51.24	49.9961

4.3. The Equilibrium Analysis

In a randomly generated N-bit sequence, we would expect approximately half of the bits in the sequence to be ones and approximately half to be zeros. Here, we denote the number of 0 and 1 as N_0 and N_1 respectively. The equilibrium analysis checks whether the number of ones in the sequences is significantly different from $N/2$, which also is named frequency test. We choose $¡^2=(N_0-N_1)^2/N$ to test the equilibrium of the sequence. Supposing the significance level is 5%, the sequence passes the test if the number of $¡^2$ is less than 3.84. For the sequence $\{s(k)\}$ generated by (10), we can obtain the N_0=9993 and N_1=10007 through the statistics. So $¡^2=(N_0-N_1)^2/N=(9993-10007)^2/20000=0.0098<3.84$, the sequence passes the frequency test. That is, the sequence generated by (10) has sound equilibrium.

4.4. The Correlation Analysis

The correlation analysis are main analysis of auto-correlation function and cross-correlation function. The auto-correlation function can be calculated by the following formula:

$$R(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(s_i-s_{mean})(s_{i+m}-s_{mean}) \tag{11}$$

which investigates the predictability of the sequence. If the auto-correlation coefficient is 0, the sequence is unpredictable and random. The auto-correlation function of ideal pseudo random sequence is ¢ .

While the cross-correlation function can be defined by:

$$C(m)=\lim_{N\to\infty}\frac{1}{N}\sum_{i=0}^{N-1}(s_i-s_{mean})(s'_{i+m}-s_{mean}) \tag{12}$$

The cross correlation function describes the correlation between the two pseudorandom sequences. The number is more close to 0, the difference degree is greater. In formula (12), $\{s_i\}$ and $\{s_i'\}$ represent two different sequences respectively, while s_{mean} represents the mean of the sequence. Simulating the correlation characteristics of the sequence generated via (10), the results are shown in Figure 2. It can be seen that the auto-correlation is of ¢ -like and the cross correlation is sound.

4.5. FIPS 140-2 Test

At present, there are some representative randomness testing standards, such as FIPS 140-2 test, SP800-22 test, and Marsaglia's Diehard battery test. Generally speaking, the pseudo-random sequences which pass these tests are of good randomness. In this paper, FIPS 140-2 is used to verify the randomness of the binary sequence. The test consists of four sub-tests. Each test needs 20000 binary {0, 1} codes. The test is passed if the tested values are fallen into the required intervals listed in required space in Tables 2 and 3, in which MT, PT and LT represent the Monobit test, Poker test, Longest Run test, respectively; LR stands for the length of the run. Define the significant level ~ =0.00001, and prove the runs of the above 256 binary sequences have the normal distribution property. So the confidence intervals of the runs can be calculated by the following formula.

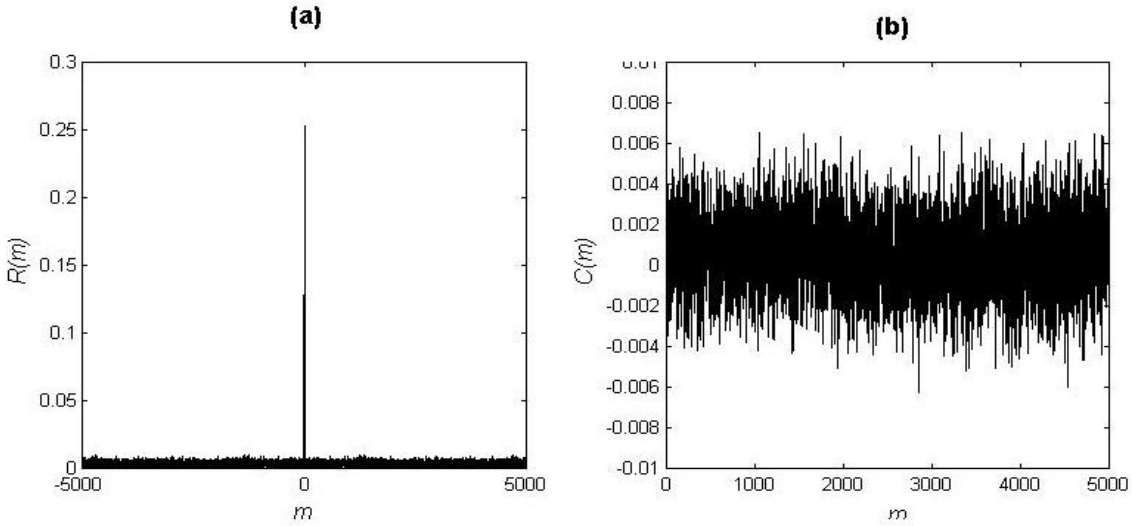

Figure 2. Correlation of the sequence: (a) auto-correlation; (b) cross-correlation

$$[\bar{x} - t_{n-1,1-\sim/2} S/\sqrt{n}, \bar{x} + t_{n-1,1-\sim/2} S/\sqrt{n}] \quad (11)$$

The RC4 algorithm is widely used in popular protocols. Although some defects are found in the key, the binary stream generated by the RC4 has a good random performance. Comparing the confident intervals of 1000 key streams generated by the CPNG and the RC4 algorithm respectively, the results are also shown in Tables 2 and 3. It follows that the confidence interval of the 1000 key streams generated by the two methods are of similar size.

Table 2. The MT, PT and LT results of 1000 key streams generated by *the CPNG and the RC4 algorithm*

Test item	Bits	FIPS 140-2 required interval	Golomb's postulates	CPNG	RC4
MT	0	9725~10275	10000	[9992 10007]	[9992 10012]
	1			[9993 10008]	[9988 10008]
PT	-	2.16~46.17	24.165	[14.5 15.6]	[14.5 15.9]
LT	0	<26	<26	[13.6 13.9]	[13.4 13.9]
	1			[13.47 13.87]	[13.37 13.87]

Based on the above analysis, it can be seen that the randomness of the sequences generated via the CPNG and the RC4 algorithm do not have significant differences. Besides, we compare the results of the statistical tests with the results described in [6]. In [6], a pseudorandom binary sequence generator was proposed based on a combination of two logistic maps. As a result it turned out that over 95% of the sequences passed the test of FIPS 140-2. For the binary number sequences generated via the CPNG, it turned out all the tested sequences passed the test. It shows that the proposed method to extend chaotic maps is effective.

Table 3. The run test results of 1000 key streams generated by the CPNG and the RC4 algorithm

Test item (LR)	Bits	FIPS 140-2 required interval	Golomb's postulates	CPNG	RC4
1	0	2315~2685	2500	[2494.9 2504.6]	[2493.6 2506.9]
	1			[2492.8 2502.3]	[2493.7 2506.6]
2	0	1114~1386	1250	[1246.2 1252.7]	[1244.9 1253.8]
	1			[1245.4 1251.9]	[1242.6 1251.3]
3	0	524~723	625	[620.3 625.3]	[621.5 628]
	1			[623.6 628.4]	[622.4 629.3]
4	0	240~384	313	[310.6 314.1]	[310.1 314.7]
	1			[310.8 314.5]	[311.3 315.7]
5	0	103~209	156	[154.6 157]	[154.8 158.2]
	1			[155.4 157.9]	[154.8 158.2]
6+	0	103~209	156	[156.2 158.6]	[154.3 157.6]
	1			[154.8 157.2]	[154.5 157.93]

5. Conclusion

This paper presents a novel 5-dimensional bidirectional discrete chaotic system with the GS property. The trajectories of the novel BGCSDS has two positive Lyapunov exponets. The simulations show that the dynamics of the BGCSDS appear obviously chaotic characteristics. Based on the new BGCSDS, a CPNG is designed by a transform T. The pseudorandom number sequences generated by the CPNG via different keys are different at mean value 49.9961%, and have mean correlation coefficient 0.00569. The values are very close to the ideal value 50% and 0. The confidence interval analysis of FIPS 140-2 test showed the sequences generated via the CPNG pass the FIPS 140-2 test, and do not have significant differences with the sequences generated via the RC4 algorithm. It can be expected that the CPNG are promising for information security encryption.

Acknowledgments

This project is supported by the National Nature Science Foundations of China (Grant No. 61074192 and No. 61170037),

References

[1] Fang JQ. Manage chaos and develop high-tech, Beijing: Atomic Energy Press. 2002: 31-32.
[2] Addabbo T, Alioto M, Bernardi S, Fort A. *The digital Tent map: performance analysis and optimized design as a source of pseudo-random bits*. Proceedings of the 21st IEEE Instrumentation and Measurement Technology Conference. Como. 2004; 2: 1301-1304.
[3] Madhekar S. Cryptographic pseudorandom sequence from the chaotic Henon map. *Sadhana*. 2009: 34(5): 689-791.
[4] Behnia S, Akhavan A, Akhshani A, Samsudin A. A novel dynamic model of pseudorandom number generator. *Journal of Computational and Applied Mathematics*. 2011; 235(12): 3455-3463.
[5] Zhang Y, Xia JL, Cai P, Chen B. Plaintext related two-level secret key image encryption scheme. *TELKOMNIKA*. 2012; 10(6): 1254-1262.
[6] Kanso A, Smaoui N. Logistic chaotic maps for binary numbers generations. *Chaos, Solitons and Fractals*. 2009; 40(5): 2557-2568.
[7] Zhang XF, Fan JJ. A new piecewise nonlinear chaotic map and its performance. *Acta Physical Sinica*. 2010; 59(4): 2298-2304.
[8] Zheng F, Tian XJ, Song JY, Li XY. Pseudorandom sequence generator based on the generalized Henon map. *The Journal of China Universities of Posts & Telecommunications*. 2008; 15(3): 64-68.
[9] Pecora LM, Carroll TL. Synchronization in chaotic systems. *Physical Review Letters*. 1990; 64(8): 821-824.

[10] Grzybowski JMV, Rafikov M, Balthazar JM. Synchronization of the unified chaotic system and application in secure communication. *Communications in Nonlinear Science and Numerical Simulation*. 2009; 14(6): 2793-2806.
[11] Du YL, Zhang JX. The performance of synchronization algorithm in real-time OFDM-PON system. *TELKOMNIKA*. 2012; 10(7): 1784-1794.
[12] Banerjee S, Mukhopadhyay S, Rondoni L. Multi-image encryption based on synchronization of chaotic lasers and iris authentication. *Optics& Lasers in Engineering*. 2012; 50(7): 950-957.
[13] Moskalenko OI, Koronovskii AA, Hramov AE . Generalized synchronization of chaos for secure communication: Remarkable stability to noise. *Physics Letters.A*. 2010; 374(29): 2925-2931.
[14] Grassi G. Generalized synchronization between different chaotic maps via dead-beat control. *Chinese Physics B*. 2012; 21(5): 104-110.
[15] Min LQ, Chen GR. Generalized synchronization in an array of nonlinear dynamic systems with applications to chaotic CNN. *International Journal of Bifurcation and Chaos*. 2013; 23(1): 1350016.
[16] Cao L, Min LQ, Zang HY. *A chaos-based pseudorandom number generator and performance analysis*. 2009 International Conference on Computational Intelligence and Security. Beijing. 2009; 1: 494-498.