A New Pseudo-random Sequence Generator Based on a Discrete Hyperchaotic System

Xujiong Ma, Jiawu Yu(✉), and Yinghong Cao

School of Information Science and Engineering, Dalian Polytechnic University,
Dalian 116034, China
yujiawu_dlpu@sina.com

Abstract. In this paper, the dynamic characteristics of four-dimensional discrete hyperchaotic mapping are analyzed by phase diagram, bifurcation diagram, Lyapunov exponential spectrum and permutation entropy complexity. On this basis, a new hyperchaotic pseudo-random sequence generator is designed by using the four-dimensional discrete hyperchaotic sequence and multi-quantization algorithm. The performance of the hyperchaotic pseudo-random sequence generator is tested by NIST SP800-22 and sequence correlation. The test results can indicate whether the sequence generated by the chaotic pseudo-random sequence generator has good randomness and correlation. The research results in this paper will provide theoretical basis and experimental basis for the application of chaotic pseudo-random sequences in information security fields such as secure communication.

Keywords: Hyperchaotic system · Pseudo-random sequence · Dynamical characteristic · NIST test

1 Introduction

Pseudo-random sequences are deterministic sequences with some random characteristics. Due to their excellent randomness and statistical properties close to white noise, pseudo-random sequences are widely used in many scientific and engineering fields in modern science. For example, it can be applied to satellites, spacecraft orbits, radar technology, secure communications, digital information processing systems, and spread spectrum communications [1–3]. The use of computer systems can not produce random sequences in the true sense, only pseudo-random sequences can be produced [3–5]. The commonly used pseudo-random sequence generated by traditional pseudo-random sequence generation methods such as m-sequence [6, 7] and Gold-sequence [8, 9] based on linear congruence theory has low complexity and has hidden dangers in information security. At the same time, the speed of password generation in cryptography design is also limited [10]. In order to design a pseudo-random sequence with excellent performance, it is a research hotspot to find a new pseudo-random sequence production method.

Chaos is a seemingly random but deterministic dynamic behavior. It is a unique nonlinear dynamic phenomenon. Its extreme sensitivity to initial values and parameters and long-term unpredictability of orbits enable chaotic systems to generate

J. Jin et al. (Eds.): GreeNets 2019, LNICST 282, pp. 193–203, 2019.
https://doi.org/10.1007/978-3-030-21730-3_21

pseudo-random sequence that seemingly unpredictable, so the study of pseudo-random sequence generator based on chaotic system is a hot topic in the research of pseudo-random sequence generation scheme [11–21].

Chaotic systems are divided into continuous chaotic systems and discrete chaotic systems. The dynamic behaviors of different kinds of chaotic systems are not the same, so the randomness of chaotic pseudo-random sequences generated by them is also different. Therefore, the choice of chaotic systems is very important for the generation of pseudo-random sequences [22]. For continuous chaotic systems, many pseudo-random sequences based on chaotic systems have proved that they have good statistical properties, however, the fixed-step integration method often used in continuous chaotic systems to solve differential equations can easily lead chaotic dynamic behavior to degradation, and the complexity of the sequence will not change much because of the increase in the number of scrolls in the attractor [23]. For discrete chaotic systems, it is a common method to generate pseudo-random sequences by using low-dimensional chaotic systems or low-dimensional chaotic systems based on them. The advantage of this method is that the time is short and the form is simple, and the dynamical property of the chaotic system will not degrade when solving. The disadvantage is that the complexity is not high and the difficulty of deciphering is small. Hyperchaotic systems have two or more positive Lyapunov exponents [24–29], usually its sequence randomness is better than the general low-dimensional chaotic system. Therefore, one of the effective ways to solve these problems is to use a hyperchaotic system to generate pseudo-random sequences, which can effectively improve the security of pseudo-random sequences. For the above reasons, the best way to design a pseudo-random sequence generator is to use a high-dimensional discrete hyperchaotic system.

This paper intends to use a four-dimensional discrete hyperchaotic mapping system based on the modified Marotto theorem. Firstly, by analyzing the dynamic characteristics of the system, the appropriate system parameters are selected, so that the chaotic pseudo-random sequence generated by the pseudo-random sequence generator has the best random performance in theory. Secondly, a pseudo-random sequence generator is designed by using a quantization algorithm; Finally, the performance of the generated pseudo-random sequence is tested.

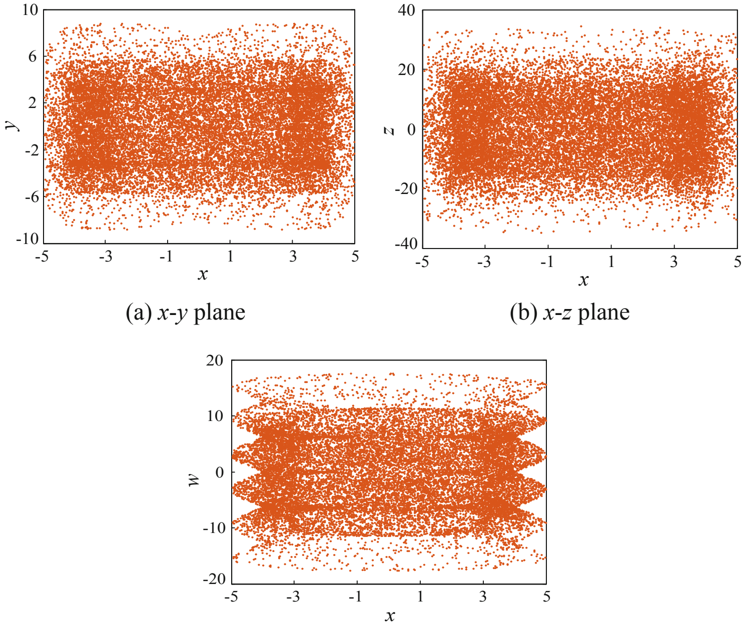
2 Four-Dimensional Discrete Hyperchaotic Mapping System and Its Dynamics Analysis

2.1 Four-Dimensional Discrete Hyperchaotic Mapping System

The mathematical model of the four-dimensional discrete hyperchaotic mapping system is:

$$\begin{cases} x_{n+1} = \sin(x_n)\sin(y_n) - a\sin(w_n) \\ y_{n+1} = b\sin(x_n)\cos(y_n) - x_n \\ z_{n+1} = cy_n + t\sin(z_n) \\ w_{n+1} = dy_n \end{cases}. \tag{1}$$

Take $a = 4$, $b = 4$, $c = 3.5$, $d = 2$, $t = 4$, the initial value of the system $[x_0, y_0, z_0, w_0] = [0.7, 0.8, 1.5, 0.8]$, the simulation step size is 0.0001. At this time, the Lyapunov exponents of the system are [0.8665, 0.6941, 0.6248, 0.1993], so the system is hyperchaotic. The corresponding chaotic attractor phase diagram is shown in Fig. 1.



(a) x-y plane

(b) x-z plane

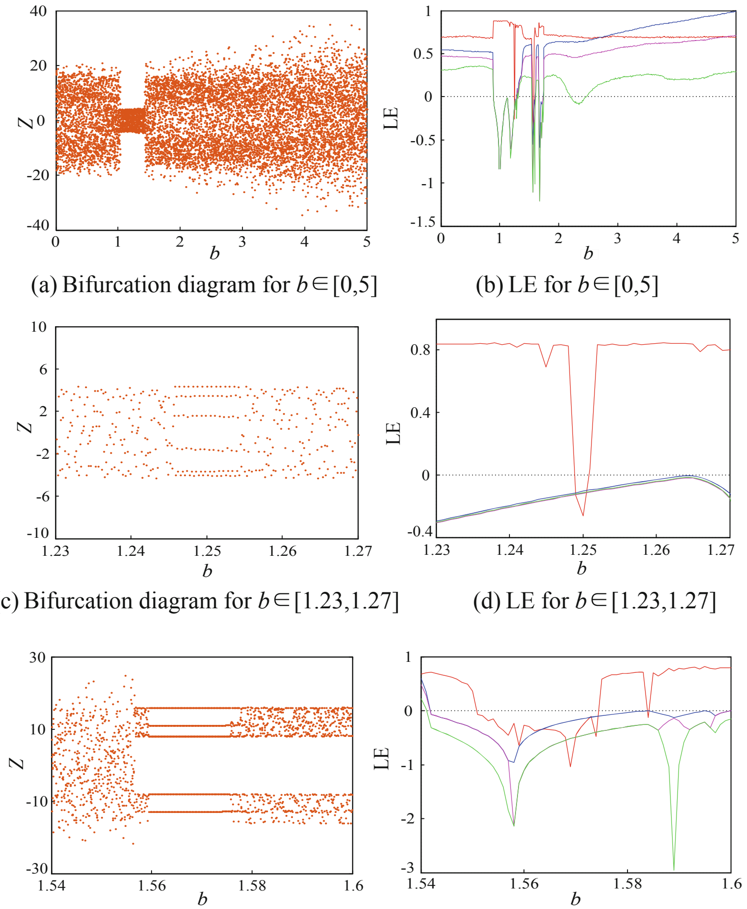
(c) x-w plane

Fig. 1. Phase diagram of four-dimensional discrete hyperchaotic system

2.2 Analysis of Dynamic Characteristics

2.2.1 Bifurcation Diagram and Lyapunov Exponent Spectrum

When the parameter $b \in [0, 5]$, let $a = 4$, $c = 3.5$, $d = 2$, $t = 4$, the initial value of the system $[x_0, y_0, z_0, w_0] = [0.7, 0.8, 1.5, 0.8]$, At this time, the Lyapunov exponent spectrum and the bifurcation diagram of the system are shown in Fig. 2. It can be seen from Fig. 2 that the bifurcation diagram and the Lyapunov exponent spectrum agree well. When $0 \leqslant b \leqslant 0.88$, $1.75 \leqslant b \leqslant 2.19$ $2.47 \leqslant b \leqslant 5$, there are four positive Lyapunov exponents in the system, and the system is in hyperchaotic state. However, when $b \in [1.248, 1.252]$, $b \in [1.556, 1.573]$, there are two obvious periodic windows in the system, so when selecting parameter b, the value of the period window should be avoided.



(a) Bifurcation diagram for $b \in [0,5]$

(b) LE for $b \in [0,5]$

(c) Bifurcation diagram for $b \in [1.23,1.27]$

(d) LE for $b \in [1.23,1.27]$

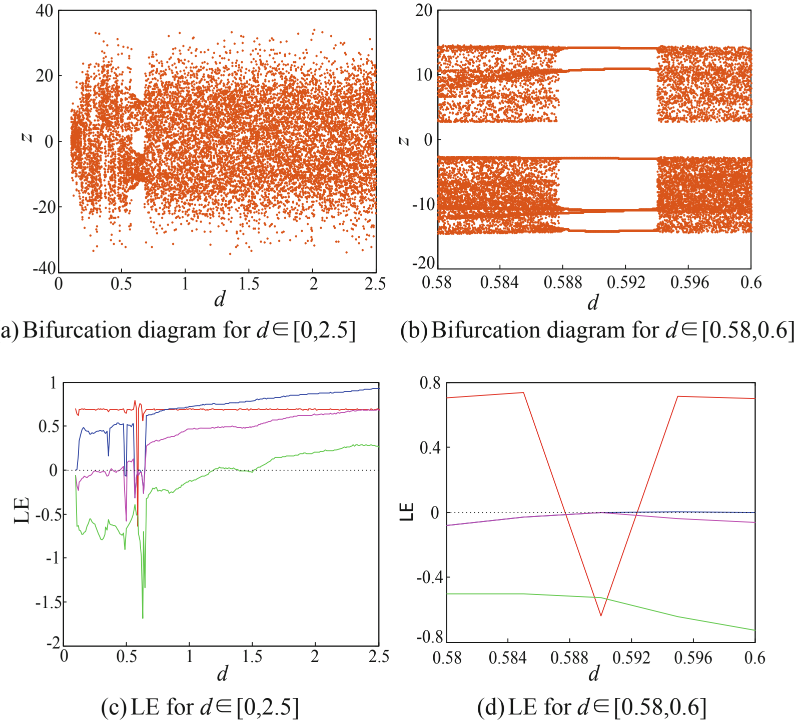
(e) Bifurcation diagram for $b \in [1.54,1.6]$

(f) LE for $b \in [1.54,1.6]$

Fig. 2. Bifurcation diagram and Lyapunov exponent spectrum of the system as b changes

When the parameter $d \in [0, 2.5]$, the remaining system parameters remain unchanged, and the Lyapunov exponent spectrum and the bifurcation diagram of the system are shown in Fig. 3. It can be seen from Fig. 3 that the results of the bifurcation diagram and the Lyapunov exponent spectrum also agree. When $1.19 \leqslant d \leqslant 1.38$ and $1.53 \leqslant d \leqslant 5$, the four Lyapunov exponents of the system are positive values, indicating that the system state is hyperchaotic too, but the system obviously has a periodic window when $d \in [0.586, 0.594]$. Therefore, the selection of the parameter d should avoid selecting the value of the period of the periodic window.

When designing a pseudo-random sequence generator using hyperchaotic maps, appropriate parameters can be chosen to ensure that the system has two or more positive Lyapunov exponents. After analyzing the dynamic characteristics of the system, the parameters $a = 4$, $b = 4$, $c = 3.5$, $d = 2$, $t = 4$ are selected to ensure that the system has four positive Lyapunov exponents to design hyperchaotic pseudo-random sequence generator.



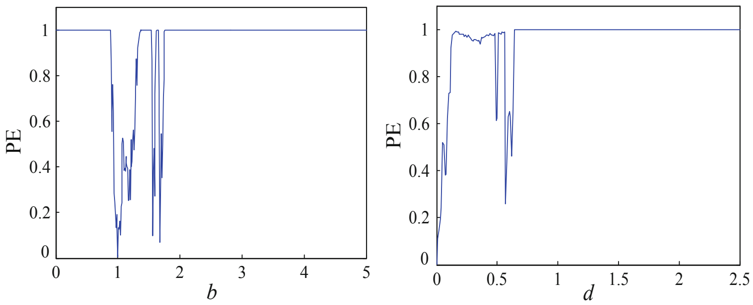
(a) Bifurcation diagram for $d \in [0,2.5]$ (b) Bifurcation diagram for $d \in [0.58,0.6]$

(c) LE for $d \in [0,2.5]$ (d) LE for $d \in [0.58,0.6]$

Fig. 3. Bifurcation diagram and Lyapunov exponent spectrum of the system as d changes

2.2.2 Permutation Entropy Complexity Analysis

In order to measure and calculate the complexity of time series, this paper uses the permutation entropy complexity algorithm for analysis. Compared with other algorithms, the algorithm is simple to calculate, the image is clear and easier to implement. In this analysis, let the dimension $p = 5$, the sequence length is 10000, and other system parameters are unchanged. When the parameters $b \in [0, 5]$ and $d \in [0, 2.5]$, the permutation entropy complexity of the chaotic sequence is obtained as shown in Fig. 4. As can be seen from Fig. 4, when the parameter b and the parameter d change, the trend of the dynamic characteristics of the system is consistent with the bifurcation diagram and the Lyapunov exponents spectrum.



(a) PE($b\in[0,5]$)

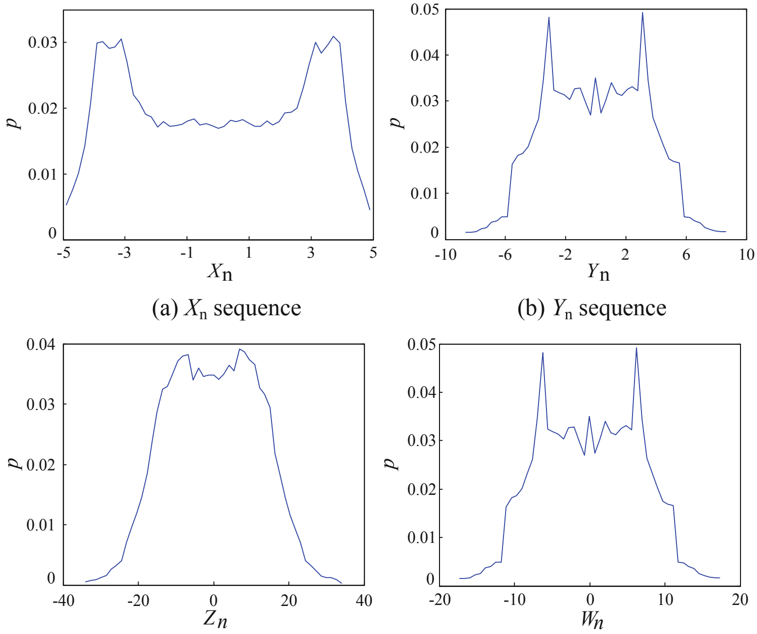
(b) PE($d\in[0,2.5]$)

Fig. 4. Permutation entropy complexity

2.2.3 Probability Density

For example, the probability density function of the chaotic sequence generated by the classical Logistic map approximates the Chebyshev type with more ends and less middle, which is not conducive to the efficiency and ability of search [30].

The probability density of four discrete sequences *X*n, *Y*n, *Z*n and *W*n generated by the four-dimensional discrete hyperchaotic mapping system in this paper is shown in Fig. 5, which are similar to the Chebyshev type distribution, and shows that the probability density distribution meets the demand, and the chaotic sequence generated by it has good randomness.



(a) X_n sequence

(b) Y_n sequence

(c) Z_n sequence

(d) W_n sequence

Fig. 5. Probability density test

3 Design of Pseudo-random Sequence Generator

The chaotic pseudo-random sequence is a binary sequence obtained by quantizing the sequence generated by the chaotic system. This binary sequence can reflect the randomness of the chaotic system. In the process of generating pseudo-random sequences, quantization is the most important link. The choice of quantization algorithm will directly affect the randomness, complexity and security of the generated pseudo-random sequence [31]. Therefore, in order to ensure the performance of the pseudo-random sequence generator, an appropriate quantization method must be selected. In this paper, the system parameters are taken as $a = 4$, $b = 4$, $c = 3.5$, $d = 2$, $t = 4$, and the initial value of the system $[x_0, y_0, z_0, w_0] = [0.7, 0.8, 1.5, 0.8]$. The four chaotic sequences generated by the system are quantized by the following quantization algorithm. The specific steps are as follows:

Step 1. After setting the system parameters and initial values, iterate N times to eliminate the transient effect and ensure that the system enters the chaotic state. Continue to iterate the hyperchaotic system to obtain four real values x_n, y_n, z_n, w_n, and obtain four new real values x'_n, y'_n, z'_n, w'_n by Eq. (2).

$$k' = \pi \log k, k = x_n, y_n, z_n, w_n. \tag{2}$$

Step 2. The integer part of the four real values of x'_n, y'_n, z'_n, and w'_n is removed by the Eq. (3), and the fractional part $A = (A_x, A_y, A_z, A_w)$ of the real value is obtained.

$$A = abs\left(k'\right) - floor\left(abs\left(k'\right)\right). \tag{3}$$

Step 3. The rounding method is used to represent the decimal A in binary:

$$A' = a_1 a_2 \cdots a_m. \tag{4}$$

Where $A' = \left(A'_x, A'_y, A'_z, A'_w\right), a_m = 0$ or 1, m is computer precision.

Step 4. XOR the obtained four binary sequences according to Eq. (5) to obtain a new sequence S:

$$S = A'_x \oplus A'_y \oplus A'_z \oplus A'_w. \tag{5}$$

Step 5. Continue to iterate the hyperchaotic system and repeat the above four steps until a hyperchaotic pseudo-random sequence of the desired length is obtained.

In the above algorithm, the sequence x_0, y_0, z_0, w_0 generated by the initial value of the hyperchaotic system, and the number of iterations N can be used as a key. If the precision of the computer is 16, the key space of the algorithm is 10^{64}, so the algorithm has a large key space and is sufficiently resistant to general exhaustive attacks.

4 Performance Analysis of Pseudo-random Sequences

4.1 NIST SP800-22 Test

There are many standards for detecting pseudo-random number performance, such as the Federal Information Processing Standard FIPS 140-2, the Diehard Battery test by Marsaglia, and the random sequence test standard SP 800-22 developed by the National Institute of Standards and Technology (NIST). This paper adopts the most widely used and authoritative NIST SP 800-22 standard in the world. The standard has a total of 15 test indicators, using the ideal random sequence as a reference, and testing the pseudo-random from different angles in statistical characteristics. The degree of deviation of the sequence is generally considered to be good pseudo-random performance by the sequence that can be detected. Each test of the SP 800-20 standard provides two criteria for determining the pass rate and the uniformity of the *P*-value distribution. All the tests took a significant level of $\alpha = 0.01$, and test sequence has β groups, the confidence interval for defining the pass rate was:

$$\left(1-\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{\beta}},1+\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{\beta}}\right). \tag{6}$$

When the pass rate falls within this confidence interval, it indicates that the sequence passes the test, and if P-value > 0.0001, it indicates that the P-value of the measured sequence is evenly distributed, and the sequence is random.

The test conditions used herein are: significant level $\alpha = 0.01$, test sequence $\beta = 100$ groups, each group is 1000000 bit in length, and the confidence interval is [0.96, 1]. The results obtained after the test are shown in Table 1. It can be seen from the results in Table 1 that the pseudo-random sequence generated by the pseudo-random sequence generator designed in this paper has passed the NIST SP 800-20 test, and compared with the NIST test results of the chaotic pseudo-random sequence generated by the pseudo-random sequence generator designed by Chung-Yi Li based on Logistic chaotic mapping system and Afshin Akhshani using three-dimensional discrete hyperchaotic mapping system, the NIST test results of the chaotic pseudo-random sequence generated by the pseudo-random sequence generator based on the high-dimensional discrete chaotic system designed in this paper have the P-value of 12 indicators larger than the results in the literature [32], and there are 11 indicators of P-value are larger than the result in literature [33]. Therefore, this pseudo-random sequence is more random and more secure and reliable in the field of information security such as secure communication.

Table 1. Test results of NIST SP 800-22

Number	Test name	*P*-value	Pass rate	Times	Result
1	Frequency	0.997 823	1	1	Pass
2	Block frequency	0.383 827	1	1	Pass
3	Cumulative sums[a]	0.534 146	1	2	Pass
4	Runs	0.401 199	0.99	1	Pass
5	Longest run	0.437 274	0.99	1	Pass

(*continued*)

Table 1. (*continued*)

Number	Test name	*P*-value	Pass rate	Times	Result
6	Rank	0.224 821	0.96	1	Pass
7	FFT	0.816 537	0.98	1	Pass
8	Non-overlapping template[a]	0.935 716	0.96	148	Pass
9	Overlapping template	0.816 537	1	1	Pass
10	Universal	0.304 126	0.98	1	Pass
11	Approximate entropy	0.657 933	1	1	Pass
12	Random excursions[a]	0.232 760	0.96	8	Pass
13	Random excursions variant[a]	0.028 181	0.97	18	Pass
14	Serial[a]	0.616 305	0.99	2	Pass
15	Linear complexity	0.834 308	1	1	Pass

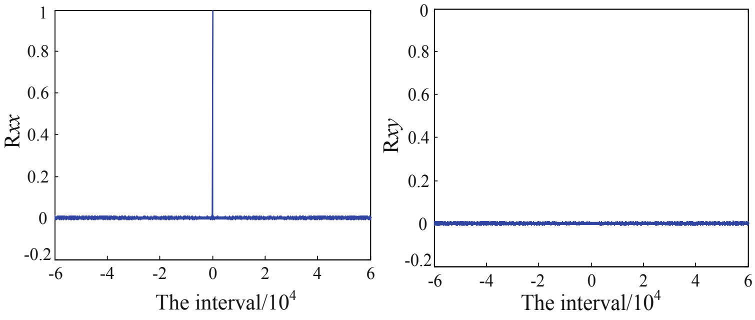
Note: [a]Test contains multiple tests, listed as worst case

4.2 Correlation Analysis

Correlation is an important indicator for testing pseudo-random sequences. Good correlation is an important guarantee for the system to operate reliably. Correlation includes autocorrelation and cross-correlation. The ideal random sequence has an autocorrelation function close to the δ function and its cross-correlation function is close to 0. The δ function is defined as

$$\delta(t) = \begin{cases} \infty & t = 0 \\ 0 & t \neq 0 \end{cases}. \tag{7}$$

Let the system parameters a = 4, b = 4, c = 3.5, d = 2, t = 4, the initial value of the system [x_0, y_0, z_0, w_0] = [0.7, 0.8, 1.5, 0.8], and 60000 values from the A' sequence are selected randomly. Then get the corresponding autocorrelation and cross-correlation results are shown in Fig. 6. The Fig. 6 shows that the autocorrelation of the binary sequences generated by the pseudo-random sequence generator is satisfied with δ function and the cross-correlation is closed to 0. Therefore, the sequence has superior correlation.



(a) autocorrelation

(b) cross-correlation

Fig. 6. Correlation analysis

5 Conclusion

By analyzing the dynamic characteristics of the four-dimensional discrete hyperchaotic mapping system based on the modified Marotto theorem, the parameter range of the system in hyperchaotic state is determined, which provides a theoretical basis for the implementation of pseudo-random sequence generator. Secondly, the pseudo-random sequence generator is designed by combining multiple quantization algorithms. The simulation results show that the pseudo-random sequence generator can quantize the sequence generated by the hyperchaotic system into a hyperchaotic pseudo-random sequence. Then, the quantized hyperchaotic pseudo-random sequence is tested by NIST SP 800-20 test. The test results show that the sequence generated by the designed pseudo-random sequence generator has good randomness. Finally, the autocorrelation and cross-correlation of hyperchaotic pseudo-random sequences are analyzed. The analysis results show that the sequence generated by this generator has an autocorrelation close to the δ function and a cross-correlation close to zero. Therefore, the sequence generated by the chaotic pseudo-random sequence generator can be applied to information security fields such as secure communication.

Acknowledgments. This work supported by Scientific Research Projects in General of Liaoning Province (Grant no. L2015043), and Doctoral Research Startup Fund Guidance Program of Liaoning Province (Grant no. 201601280).

References

1. Tisa, S., Villa, F., Giudice, A.: High-speed quantum random number generation using CMOS photon counting detectors. IEEE J. Sel. Top. Quantum Electron. **21**(3), 1–7 (2015)
2. Sánchez, S., Criado, R., Vega, C.: A generator of pseudo-random numbers sequences with a very long period. IEEE J. Sel. Top. Quantum Electron. **42**(7), 809–816 (2005)
3. Zheng, F., Tian, X., Song, J.: Pseudo-random sequence generator based on the generalized Henon map. J. China Univ. Posts Telecommun. **15**(3), 64–68 (2008)
4. Behnia, S., Akhavan, A., Akhshani, A., et al.: A novel dynamic model of pseudo random number generator[J]. J. Comput. Appl. Math. **235**(12), 3455–3463 (2011)
5. Luo, Q.B.: A new approach to generate chaotic pseudo-random sequence. J. Electron. Inf. Technol. **28**, 1262–1265 (2006)
6. Wang, H., Li, B.: Design and Realize of m-sequence generator. J. Beijing Electron. Sci. Technol. Inst. (2007)
7. Xianyong, W., Zhou, X.: A kind of generating method of m-sequence pseudo-code generator. Meas. Control. Technol. **22**(9), 56–58 (2003)
8. Xinyu, Z.X.Z.: Analysis of m-sequence and Gold-sequence in CDMA system. In: IEEE International Conference on Communication Software and Networks. IEEE (2011)
9. Wang, F., Huang, Z., Zhou, Y.: A new method for m-sequence and Gold-sequence generator polynomial estimation. In: International Symposium on Microwave
10. Kotulski, Z., Szczepański, J., et al.: Application of discrete chaotic dynamical systems in cryptography — DCC method. Int. J. Bifurc. Chaos **9**(06), 1121–1135 (2011)
11. Da, L.H., Guo, F.D.: Composite nonlinare descrete chaotic dynamical systems and stream cipher systems. Acta Electron. Sin. **31**(8), 1209–1212 (2003)

12. Cai, J.P., Li, Z., Song, W.T.: Analysis on the chaotic pseudo-random sequence complexity. Acta Phys. Sin. **52**(8), 1871–1876 (2003)
13. Huang, Y., Zhang, P., Zhao, W.: Novel grid multiwing butterfly chaotic attractors and their circuit design. IEEE Trans. Circuits & Syst. Express Briefs **62**(5), 496–500 (2017)
14. Wang, X.Y., Yang, L.: Design of pseudo-random bit generator based on chaotic maps. Int. J. Mod. Phys. B **26**(32), 1250208 (2012)
15. François, M., Grosges, T., Barchiesi, D., et al.: Pseudo-random number generator based on mixing of three chaotic maps. Commun. Nonlinear Sci. Numer. Simul. **19**(4), 887–895 (2014)
16. Xiang, F., Qiu, S.S.: Analysis on stability of binary chaotic pseudorandom sequence. IEEE Commun. Lett. **12**(5), 337–339 (2008)
17. Hu, H.P., Liu, L.F., Ding, N.D.: Pseudorandom sequence generator based on the Chen chaotic system. Comput. Phys. Commun. **184**(3), 765–768 (2013)
18. Suneel, M.: Cryptographic pseudo-random sequences from the chaotic Hénon map. Sadhana **34**(5), 689–701 (2006)
19. Pellicer-Lostao, C., López-Ruiz, R.: Pseudo-random bit generation based on 2D chaotic maps of logistic type and its applications in chaotic cryptography. In: Gervasi, O., Murgante, B., Laganà, A., Taniar, D., Mun, Y., Gavrilova, M.L. (eds.) ICCSA 2008. LNCS, vol. 5073, pp. 784–796. Springer, Heidelberg (2008). https://doi.org/10.1007/978-3-540-69848-7_62
20. Zelinka, I.: Behaviour of pseudo-random and chaotic sources of stochasticity in nature-inspired optimization methods. Soft. Comput. **18**(4), 619–629 (2014)
21. Li, X., Li, C., Lee, I.K.: Chaotic image encryption using pseudo-random masks and pixel mapping. Signal Process. **125**(C), 48–63 (2016)
22. Dabal, P., Pelka, R.: A study on fast pipelined pseudo-random number generator based on chaotic logistic map. In: International Symposium on Design and Diagnostics of Electronic Circuits and Systems (2014)
23. Qi, W.U., Tan, Z.W., Wan, C.X.: Harmonically coupled chaotic system for a pseudo-random bit generator. J. Chin. Comput. Syst. **32**(4), 639–643 (2011)
24. Chen, C.-H., Sheu, L.J., et al.: A new hyper-chaotic system and its synchronization. Nonlinear Anal. Real World Appl. **10**(4), 2088–2096 (2009)
25. University N, Tianjin: Generation and circuit implementation of a large range hyper-chaotic system. Acta Phys. Sin. **58**(7), 4469–4476 (2009)
26. Liu, H., Wang, X., Kadir, A.: Color image encryption using Choquet fuzzy integral and hyper chaotic system. Opt. Int. J. Light. Electron Opt. **124**(18), 3527–3533 (2013)
27. Kadir, A., Hamdulla, A., Guo, W.Q.: Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Opt. Int. J. Light. Electron Opt. **125**(5), 1671–1675 (2014)
28. Carroll, T.L., Pecora, L.M.: Cascading synchronized chaotic systems. Phys. D Nonlinear Phenom. **67**(1–3), 126–140 (1993)
29. Min, F.H.: Dislocated projective synchronization of Qi hyper-chaotic system and its application to secure communication. Acta Phys. Sin. **59**(11), 509–518 (2010)
30. Flores-Franulič, A., Román-Flores, H.: A Chebyshev type inequality for fuzzy integrals. Inf. Sci. **190**(2), 1178–1184 (2007)
31. Chiang, Y.T., Wang, H.S., Wang, Y.N.: A chaotic-based pseudo-random bit generator for navigation applications. Appl. Mech. Mater. **311**, 99–104 (2013)
32. Li, C.Y., Chen, Y.H., Chang, T.Y., et al.: Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG. IEEE Trans. Very Large Scale Integr. (VLSI) Syst. **20**(2), 385–389 (2012)
33. Akhshani, A., Akhavan, A., Mobaraki, A., et al.: Pseudo random number generator based on quantum chaotic map. Commun. Nonlinear Sci. Numer. Simul. **19**(1), 101–111 (2014)