Random Sequence Generation Algorithm for Multi-chaotic Systems

Xiaodi Chen and Hong Wu(✉)

College of Electronic Engineering, Heilongjiang University,
150080 Harbin, China
2002060@hlju.edu.cn

Abstract. The characteristics of chaotic signals, such as pseudorandom and non long term predictability, make it suitable for application to information encryption, digital watermarking and so on. Nevertheless, since the chaotic system is often characterized by its characteristics, attackers can take advantage of these known features to reduce the difficulty of attacks. In contrast, the characteristics of multi-chaotic systems are not uniform, and the complexity of generating sequences is higher than that of single-chaos systems. Hence, the multi-chaotic system increases the security of the sequence to some extent. Therefore, we design a random sequence generation algorithm consisting of multiple chaotic systems that is a chaotic sequence generation algorithm combining Logistic map and Cubic map. And we analyze the sequence of new generation whose the performance, so we can conclude that the new algorithm has better randomness.

Keywords: Multi-chaos system · Logistic map · Cubic map
Chaotic sequence · Randomness

1 Introduction

The ideal chaotic sequence is not periodic, but in the actual application, as the computer or digital signal processor is through finite word length adder, multiplying unit to realize chaotic iteration [1], and all the data are stored in a finite word length unit, resulting in error. And it triggers the simulated chaotic orbit to deviate from the real chaotic orbit, thus resulting in the short-period phenomenon of chaotic sequence. This short-period phenomenon is more than apparent in the system using rarely single chaos mapping [2]. Therefore, we use double-precision floating-point arithmetic and compound chaotic system to improve the dynamic characteristics of chaotic system caused by finite precision. That is to say that we use a chaotic sequence generation algorithm which combines logistic map and cubic map. This paper first analyzes the characteristics of cubic mapping and logistic mapping through the comparison of histogram, correlation and balance, and subsequently analyzing whether the improved algorithm is more cyclical than that of logistic sequence from theoretical and experimental standpoints.

L. Meng and Y. Zhang (Eds.): MLICOM 2018, LNICST 251, pp. 136–143, 2018.
https://doi.org/10.1007/978-3-030-00557-3_14

2 Performance Analysis of Chaotic System

The classical one dimensional chaotic logistic mapping which is widely studied and applied for its simple form and the ability to produce the complex structure of the random sequence. Cubic mapping has the same advantages as logistic mapping, but little attention which has been paid. The following comparison of the logistic mapping and the cubic mapping which reveals that the cubic mapping can be widely used in the domain of encryption.

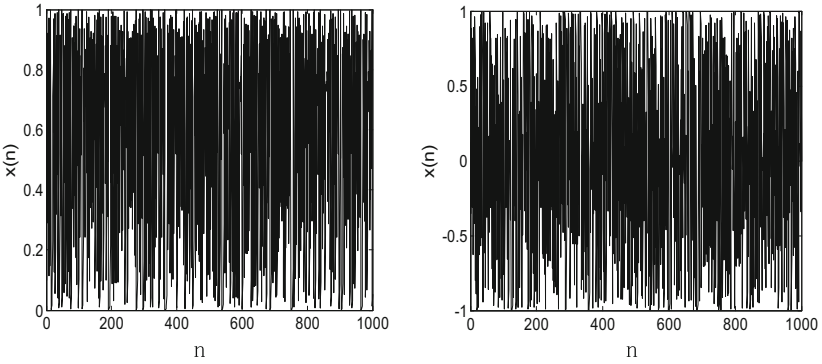
The logistic mapping is defined as $x_{k+1} = \mu x_k(1 - x_k)$, the range of x_k is 0 to 1, and the range of the bifurcation parameter μ is 3.56994 to 4 [3].

The definition of the cubic mapping is that $x_{k+1} = ax_k^3 - bx_k$, the range of b is 2.3 to 3, and when a is 4, the range of x_k is -1 to 1 [4].

The parameter range of logistic mapping is about 0.43, and the parameter of cubic mapping whose the range is about 0.7. In contrast, we can see that the parameter range of cubic mapping is larger. The maximum Lyapunov exponent of the logistic mapping is 0.6920, while the cubic mapping whose the maximum Lyapunov exponent is 1.0980 [5], and there is a stronger chaotic characteristic compared with the logistic mapping. The logistic mapping parameter μ is 4, and the cubic mapping parameter a is 4 and b is 3, and the initial values of the two mappings are all 0.1. After the comparison of histogram, correlation and balance, so the cubic mapping and logistic mapping whose the characteristics are analyzed.

2.1 Histogram Characteristics

Figure 1 is the state diagrams of logistic mapping and cubic mapping. As can be seen from the figure, the state values of cubic mapping which are approximately random and have no apparent periodicity. In Fig. 1(a) and (b), the horizontal axis which represents the frequency and the vertical axis which represents the sequence value.



(a) The state diagram of logistic mapping. (b) The state diagram of cubic mapping.

Fig. 1. The state diagrams of logistic sequence and cubic sequence.

2.2 Sequence Correlation Analysis

The autocorrelation of sequences reflects the degree of correlation between the sequences generated by the same function at different moments and which is defined as [6]:

$$R_{XX}(m) = \frac{1}{N}\lim_{N\to\infty}\sum_{i=0}^{N-1} x_i x_{i+m} - \bar{x}^2. \tag{1}$$

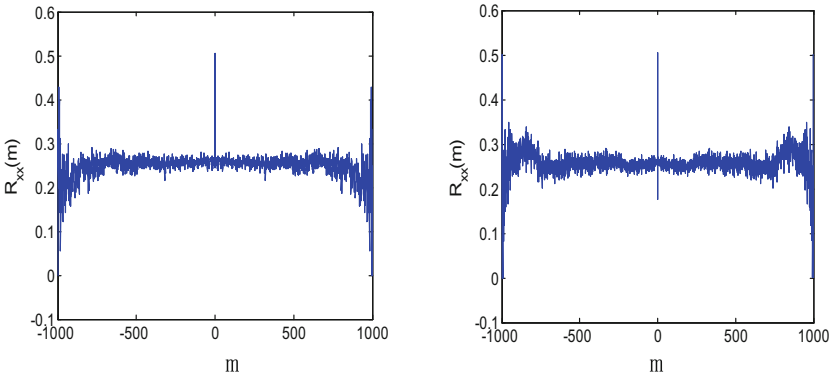
The mean value of the ideal cubic mapping sequences which is 0, so 0 is taken as the threshold, and the cubic real value sequences which are digitized into the 0/1 sequences according to the binary decision method [7]:

$$d_k = \begin{cases} 0 & x_k \le 0 \\ 1 & x_k > 0 \end{cases}. \tag{2}$$

Similarly, the mean 1/2 of the logistic mapping sequences which is used as threshold, and subsequently the logistic real value sequences are digitized into 0/1 sequences:

$$d_k = \begin{cases} 0 & x_k \le 1/2 \\ 1 & x_k > 1/2 \end{cases}. \tag{3}$$

According to the formula (1), the autocorrelation coefficients of the logistic mapping and the cubic mapping are calculated respectively, and the results of MATLAB simulation are shown in Fig. 2. It can be seen that the cubic mapping has the same good autocorrelation with the logistic mapping. The transverse axis of the (a) and (b) of Fig. 2 is the correlation interval, and the longitudinal axis is the correlation coefficient value.



(a) Autocorrelation function of logistic sequence. (b) Autocorrelation function of cubic sequence.

Fig. 2. Autocorrelation function figures of logistic sequence and cubic sequence.

2.3 Analysis of Balancing Characteristics

Another criterion for the randomness of the testing sequence which is the balance test, that is whether the number of 0 in the statistical series is balanced by the number of 1 [8]. The statistical results show Table 1.

Table 1. Comparison of balancing characteristics.

The name of the sequence	The statistics of balance	Sequence length N		
		2000	5000	10000
Logistic chaotic sequence	The number of 0	1007	2527	5102
	Ratio	0.5035	0.5054	0.5102
	The number of 1	993	2473	4898
	Ratio	0.4965	0.4946	0.4898
Cubic chaotic sequence	The number of 0	1002	2528	5011
	Ratio	0.5010	0.5056	0.5011
	The number of 1	998	2472	4989
	Ratio	0.4990	0.4944	0.4999

From the analysis of the table, it can be seen that the numbers of 0 and 1 of the cubic chaotic sequence are nearly equivalent to the numbers of 0 and 1 of the logistic chaotic sequence. Although both sequences which are well balanced, the cubic mapping that is slightly more balanced.

Based on the above analysis, it can be found that cubic mapping has the same characteristics as logistic mapping, and which is superior to logistic mapping relating to balance. Consequently, it is of research value to apply cubic mapping to the field of information encryption.

3 Design of Chaotic Sequence Algorithm

From the above analysis, we know that due to the limitation of computer accuracy, accordingly the randomness of chaotic system can not achieve ideal conditions, and there will be the minor-cycle phenomenon. Consequently, we propose a hypothesis that multiple chaotic systems are combined and the parameters of the system are mutually restricted to form a compound chaotic system with variable parameters. Thus, the complexity of the sequence which is increased and the minor-cycle phenomenon is improved. Since cubic mapping which has the same good features as logistic mapping, so we can select cubic mapping and logistic mapping to generate random sequences. At the same time, it provides theoretical support for the improved composite chaotic system due to the superposition of chaotic system [9].

(1) The initial values and parameters of the logistic mapping are given, and the first layer of chaotic sequences which is generated by the iteration of the logistic mapping: $\{x_{k0} | k = 0, 1, 2, \ldots, M\}$.

(2) Each x_{k0} which is used as the initial value of the cubic mapping to iterate out a sequence of length N. A total of M x_{k0} generated M chaotic sequences, and which were connected in series to get the sequence of the second layer:$\{x_{ki} | k = 0, 1, 2, \ldots, M; i = 0, 1, 2, \ldots, N\}$.

(3) In accordance with the value of x_{k0} and the value of x_{kN} which is iterated out as initial value, the parameter μ of logistic mapping and the parameter a of cubic mapping which are dynamically transformed according to the following method to form a mutual control chaotic system.

$$\mu = \begin{cases} 3.9 & x_{kN} \geq 0 \\ 4 & x_{kN} < 0 \end{cases}. \tag{4}$$

$$a = \begin{cases} 1 & x_{k0} \geq 0.5 \\ 4 & x_{k0} < 0.5 \end{cases}. \tag{5}$$

(4) Discard the antecedent sequence of each subsystem iteration to ensure that the system enters chaos state.

(5) Give the system a different initial value y_{00} and repeat the above steps to generate a compound sequence $\{y_{ki}\}$.

(6) Select 0 as the threshold, according to the binary decision method to chaotic sequence $\{x_{ki}\}$, $\{y_{ki}\}$ to obtain a binary sequence $\{X_{ki}\}$ and $\{Y_{ki}\}$.

(7) Exclusive-OR of $\{X_{ki}\}$ and $\{Y_{ki}\}$ which yields a random sequence for encryption $\{Z_{ki}\}$.

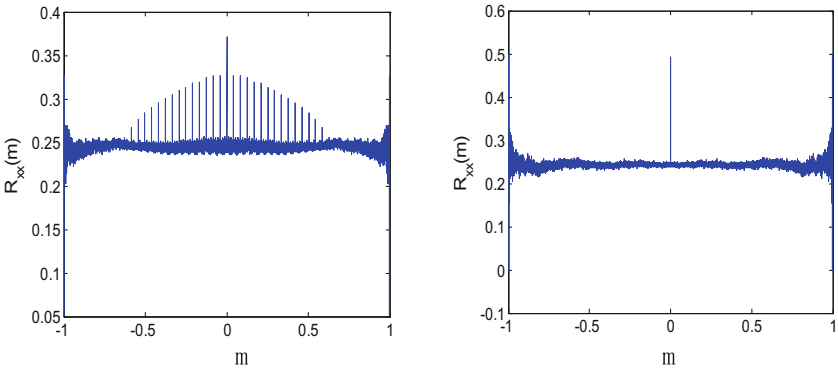
4 Performance Analysis and Comparison of Algorithms

4.1 Periodicity Analysis

From the theoretical and experimental point of view, we will analyze whether the hybrid sequence generated by the improved algorithm is more periodic than the logistic sequence.

(1) Theoretical analysis

The improved algorithm is compounded by two chaotic systems with different initial values by XOR generated mixed sequence, and each of the composite chaotic system is composed of several different initial cubic subsystems, the period of the chaotic sequence produced by each compound system must be larger than the period of each subsystem generation sequence, and two composite systems by XOR the operation once again expand the cycle, due to the XOR operation is to add operation, the two systems are independent of each other, the number of states experienced from a certain state to recovering this state can only be the least common multiple of two composite system periods [10].



(a) Logistic sequence (b) Advanced sequence

Fig. 3. Autocorrelation function figures of logistic sequence and advanced sequence

(2) Experimental analysis

Provided that a sequence is periodic, so its autocorrelation function which is also cyclical and has the same period as the sequence, so we can use the autocorrelation function to test the periodicity of the improved sequence. When the accuracy is 10^{-8}, logistic sequence and mixed chaotic sequence with length of 10^4 are respectively calculated whose the autocorrelation according to formula (1), and Fig. 3 is the relation graph between correlation interval and autocorrelation function. The horizontal axis of (a) and (b) of Fig. 3 is related interval, and whose the vertical axis is all autocorrelation function value. Logistic sequences have apparent short-period phenomena under low-precision conditions. Nevertheless, the autocorrelation function of the sequence generated by the improved algorithm in this paper is closer to the δ function, which avoids the short-period phenomenon and the randomness of the sequences is better [11].

4.2 Key Space Analysis

In this algorithm, the key is the initial value x_{00} and y_{00} of two systems, and the value range of x_{00} and y_{00} is 1 to 2, and the key space is 1032 when the computing precision is 10^{-16}. As a result $\log_2 10^{32} \approx 106$, a 106 bits key is sufficient to resist the exhaustive attack.

4.3 Randomness Test

There are many relevant theories and methods for testing the randomness of sequences, such as the Menezes test [12], the NIST test, the Helsinki test [13] and so on. Among the test methods, the NIST test is universally accepted [14]. NIST test by the United States National Institute of Standards and Technology research and development of randomness test system, due to the perfect function, it has been widely used. It includes approximate entropy, block frequency, cumulative sums, spectrum test (FFT), frequency test, linear complexity, longest run, nonoverlapping template, overlapping

template, random excursions, random excursions variant, binary matrix rank test rank, run, serial, universal, and a total of 15 tests. Test results return P-value, the value range of the significant level of α is 0.001 to 0.01, if so P-value $\geq \alpha$, through the test, and conversely, if P-value $< \alpha$, subsequently did not pass the test, generally take $\alpha = 0.01$ [15].

NIST tests which are carried out on the single logistic chaotic sequence and the chaotic sequence generated by the improved algorithm, and the results show Table 2.

Table 2. NIST test results of logistic sequences and complex sequences.

Test item	Logistic sequences P-value	Whether to pass the test	Complex sequences P-value	Whether to pass the test
Frequency	0.173900	Yes	0.726265	Yes
Block frequency	0.547993	Yes	0.649631	Yes
Runs	0.855063	Yes	0.924797	Yes
Approximate entropy	0.552590	Yes	0.691964	Yes
Cumulative sums	0.132336	Yes	0.831463	Yes
Longest run	0.103811	Yes	0.808232	Yes
Rank	0.239974	Yes	0.696357	Yes
FFT	0.036674	Yes	0.353091	Yes
Nonoverlapping template	0.029912	Yes	0.906058	Yes
Overlapping template	0.616504	Yes	0.184802	Yes
Universal	-	No	0.825677	Yes
Linear complexity	0.842133	Yes	0.789689	Yes
Random excursions	-	No	0.184802	Yes
Random excursions Variant	-	No	0.759490	Yes
Serial	0.624629	Yes	0.293907	Yes

5 Summary

In this paper, we study that the digital chaotic system, compare the performance of cubic mapping with logistic mapping, and point out that its superior performance in quite a few aspects is also suitable for the application in the field of encryption. A new improved combinatorial chaotic system is proposed, in which the output of the first level chaotic system is taken as the initial input of the next level chaotic system and the chaotic system parameters which are controlled according to the output iteration value of each stage. Combining with the theory and experiment, the performance of the new algorithm is analyzed. It can be seen that the new algorithm can improve the short-period phenomenon effectively, resist the exhaustive attack and have good stochastic behavior.

References

1. Vattulainen, I., Kankaala, K.: Physical models as tests of randomness. Phys. Rev. E **52**, 3205–3214 (2013)
2. Li, T.Y., Yorke, J.A.: Entropy and chaos. Adv. Math. **3**, 122–128 (2010)
3. Zhang, Y.P., Zuo, F.: A new image encryption algorithm based on multiple chaos system. In: International Symposium on Electronic Commerce and Security, vol. 142, pp. 347–350 (2017)
4. Li, S.J., Cai, Y.L.: Problems with computerized chaos in finite computing precision. Comput. Phys. Commun. **153**, 52–55 (2016)
5. Xue, K.P., Hong, P.L.: Security improvement on an anonymous key agreement protocol based on chaotic maps. Commun. Nonlinear Sci. Number. Simulat. **17**, 2969–2977 (2012)
6. Short, K.M.: Signal extraction from chaotic communications. Int. J. Bifurcat. Chaos **7**, 1579–1997 (2010)
7. Zhai, Y.K., Lin, X.Y.: Improving image encryption using multi-chaotic map. In: Workshop on Power Electronics and Intelligent Transportation System, vol. 106, pp. 143–148 (2015)
8. Habutsu, T., Nishio, Y., Sasase, I., Mori, S.: A secret key cryptosystem by iterating a chaotic map. In: Davies, D.W. (ed.) EUROCRYPT 1991. LNCS, vol. 547, pp. 127–140. Springer, Heidelberg (1991). https://doi.org/10.1007/3-540-46416-6_11
9. Alvarez, G., Pastor, G.: Chaotic cryptosystems. IEEE Secur. Technol. **67**, 332–338 (2012)
10. Diffie, W., Hellman, M.: New directions in cryptography. IEEE Trans. Inf. Theory **22**, 644–654 (2015)
11. Shannon, C.E.: Communication theory of secrecy systems. Bell Syst. Tech. J. **28**, 656–715 (2016)
12. Kocarev, L.: A brief overview. IEEE Circ. Syst. Mag. **1**, 11–21 (2010)
13. Sabery, K.M., Yaghoobi, M.: A new approach for image encryption using chaotic logistic map. In: 2008 International Conference on Advanced Computer Theory and Engineering, vol. 177, pp. 585–590 (2013)
14. Akhavan, A., Samsudin, A.: A symmetric image encryption scheme based on combination of nonlinear chaotic maps. J. Franklin Inst. **348**, 1797–1813 (2011)
15. Lian, S.: Efficient image or video encryption based on spatiotemporal chaos system. Chaos Solitons Fractals **40**, 2509–2519 (2014)