Hindawi
Complexity
Volume 2019, Article ID 3510985, 10 pages
https://doi.org/10.1155/2019/3510985

Research Article

Effects of Limited Computational Precision on the Discrete Chaotic Sequences and the Design of Related Solutions

Chunlei Fan and Qun Ding

Electrical Engineering College, Heilongjiang University, Harbin 150080, China

Correspondence should be addressed to Qun Ding; qunding@aliyun.com

Received 26 August 2018; Accepted 9 December 2018; Published 1 January 2019

Guest Editor: Amir Anees

In this paper, we analyzed the periodicity of discrete Logistic and Tent sequences with different computational precision in detail. Further, we found that the process of iterations of the Logistic and Tent mapping is composed of transient and periodic stages. Surprisingly, for the different initial iterative values, we first discovered that all periodic stages have the same periodic limit cycles. This phenomenon has seriously affected the security of chaotic cipher. To solve this problem, we designed a novel discrete chaotic sequence generator based on m-sequence and discrete chaotic mapping. The experimental results indicated that the chaotic sequence generator can generate pseudorandom chaotic sequences with large periodicity and good performance under the condition of limited computational precision.

1. Introduction

Chaos is a new interdisciplinary theory of physics, mathematics, nonlinear dynamics, and so on. The ergodic character of chaotic system satisfies the diffusion principle of cryptosystem. The initial value sensitivity of chaos can generate a large key space. Compared with traditional cipher, chaotic cipher has the advantages of simple structure, easy implementation, and high security. Therefore, in recent years, chaos theory has been widely applied in the field of cryptography and secret communication [1–4]. For instance, Yadav et al. [5] proposed a chaotic system-based data hiding scheme that provides high payload and imperceptibility. Murillo-Escobar et al. [6] put forward a novel pseudorandom number generator based on pseudorandomly enhanced Logistic map. Li et al. [7] came up with an image encryption scheme based on chaotic Tent map. Hasimoto-Beltran [8] designed a high-performance multimedia encryption system based on chaos to ensure multimedia information security. Chaotic mapping theoretically generates discrete sequences that are not periodic for any given initial iterative value. However, for the digital chaotic sequence generator, performance of the discrete chaotic sequence is seriously affected by the limited computational precision of processor, which will cause the quantized the chaotic binary sequences to have short periodicity and cannot meet the requirements of cryptography [9, 10].

Aiming at this problem, Du et al. [11] proposed a novel chaotic key sequence generator based on double K-L (Karhunen-Loeve) transform. It can effectively improve the complexity and period length of Logistic chaotic sequence. Nagaraj et al. [12] proposed a pseudorandom number generator based on chaotic switching between robust chaos maps in order to increase average period lengths. Cernak [13] proposed to increase the period of discrete chaotic sequences by using programmable combinational circuits and perturbing chaotic parameters. Chen et al. [14] designed a new chaotic sequence generator based on the novel interacting neural networks and the multiple chaotic systems with the purpose of enhancing the performance of chaotic sequences. In order to increase the period of the generated chaotic orbits, Heidari-Bateni et al. [15] proposed a new chaotic sequence generator by cascading two Logistic maps with different bifurcation parameters. Further, Hu et al. [16] proposed an error compensation method to counteract the dynamical degradation of digital chaos. Deng et al. [17] designed an analogue-digital mixed method for enhancing the performance of chaotic sequences. Cao et al. [18] came up with a new perturbation method based on Lyapunov exponent to improve random distribution of chaotic sequences.

However, these schemes do not consider the effect of chaotic initial value on chaotic sequence and key space. These literatures do not accurately analyze the short-period behavior of chaotic systems. Moreover, some of the schemes are too complex to be implemented in hardware circuits and engineering applications. In view of the above problems, we focus on the effect of limited computational precision on discrete chaotic mapping. The periodicity of discrete chaotic sequence and the scope of key space are analyzed accurately. For the discrete Logistic and Tent sequences with different initial values, we found that all periodic stages have the same periodic limit cycles. This phenomenon has seriously affected the key space of chaotic stream ciphers. Based on this situation, we present an effective approach to increase the period and key space of the chaotic sequence by using m-sequences with a simple structure. The experimental results show that the period of chaotic sequence can be determined by the order of the m-sequence. When the computational precision is limited, we can increase the order of the m-sequence to obtain a good performance discrete chaotic sequence. Compared with other proposed schemes, the key advantages of our method include the following several aspects: (i) In comparison with the general perturbation method under same calculation precision and perturbation source, the digital chaotic sequence generated by our scheme has considerable period length. (ii) The method consumes less hardware resources and is easy to implement in engineering. (iii) Compared with the analogue-digital mixed method, our scheme has better stability. Because chaos is extremely sensitive to initial values, components of the analogue circuit are susceptible to environmental temperature and humidity so that the parameters of the chaotic system are difficult to maintain a constant value.

The rest of this paper is organized as follows: Section 2 analyzes in detail the influence of limited computational precision on digital chaotic system. Section 3 describes a novel discrete chaotic sequence generator with the purpose of avoiding short periods of chaotic sequences. Section 4 gives the comparative analysis of performance of discrete chaotic sequences, including key space, autocorrelation test and PE analysis. Section 5 summarizes the discussions of this paper.

2. Influence of Computational Precision on Discrete Chaotic Sequences

2.1. Logistic Mapping. In this section, we take Logistic mapping [19] as an example to illustrate the effect of computational precision on discrete chaotic sequences. The mathematical equation of Logistic mapping can be described as follows:

$$x_{n+1} = \mu x_n \left(1 - x_n\right), \quad \mu \in (0, 4], \; x_n \in [0, 1] \tag{1}$$

where μ is called branch parameter; when the value range of μ is $[3.5699456, 4]$, Logistic mapping is in a chaotic state and displays the complex dynamic characteristics. Further, let us rewrite x_n in its binary representation:

$$x_n = \left(0.\varepsilon_1\varepsilon_2\varepsilon_3\cdots\right)_2 = \sum_{i=1}^{\infty}\varepsilon_i 2^{-i} \quad \varepsilon_i \in \{0, 1\} \tag{2}$$

where $(\cdot)_2$ denotes the enclosed number is in binary format. Let us assume that L represents computational precision. $\hat{x}_n$ denotes approximate value of x_n, defined by

$$\hat{x}_n = \left(0.\varepsilon_1\varepsilon_2\cdots\varepsilon_L\right)_2 = \sum_{i=1}^{L}\varepsilon_i 2^{-i} \approx x_n \tag{3}$$

For computing convenience, we introduce a new variable z_n:

$$z_n = 2^L \hat{x}_n = \left(\varepsilon_1\varepsilon_2\cdots\varepsilon_L\right)_2 \tag{4}$$

where z_n is an integer and $z_n \in [0, 2^L - 1]$. Further, (1) can be rewritten as the follows:

$$z_{n+1} = \mu z_n \left(1 - \frac{z_n}{2^L}\right) \quad z_n \in \left[0, 2^L - 1\right] \tag{5}$$

According to (5), we generated a series of discrete chaotic sequences with different computational precision, including $L = 8$, 12, 16, and 24. In order to test the effect of computation precision on discrete chaotic sequences, we performed autocorrelation test, permutation entropy test, and statistical analysis of sequence periodicity for the above chaotic sequences.

2.2. Autocorrelation Test. Autocorrelation test can clearly reflect the dependence relationship of a signal between two different moments, which is a significant method with the purpose of evaluating the randomness and periodicity of discrete chaotic sequences [20]. Autocorrelation function is defined as follows:

$$R_z(m) = \frac{1}{N}\sum_{n=0}^{N-1} z_n z_{n+m} \tag{6}$$

where $R_z(m)$ and N denote autocorrelation function and the length of discrete chaotic sequence, respectively. Based on the above theoretical basis, autocorrelation test can be performed with discrete Logistic sequences of different computational precision. MATLAB simulation results are shown in Figure 1. As can be seen from the figure, the smaller the computational precision is, the denser the peak the line of the autocorrelation function is. The distance between each two peak lines can be approximately expressed as the period length of the discrete chaotic sequences. Therefore, we can conclude that if the calculation precision is small, the discrete chaotic sequences will emerge some short periodic phenomena.

2.3. Permutation Entropy. Permutation entropy (PE) [21–23] is widely applied in the measurement of discrete time sequence complexity because of its high robustness and fast algorithm characteristics, which can be described as follows.

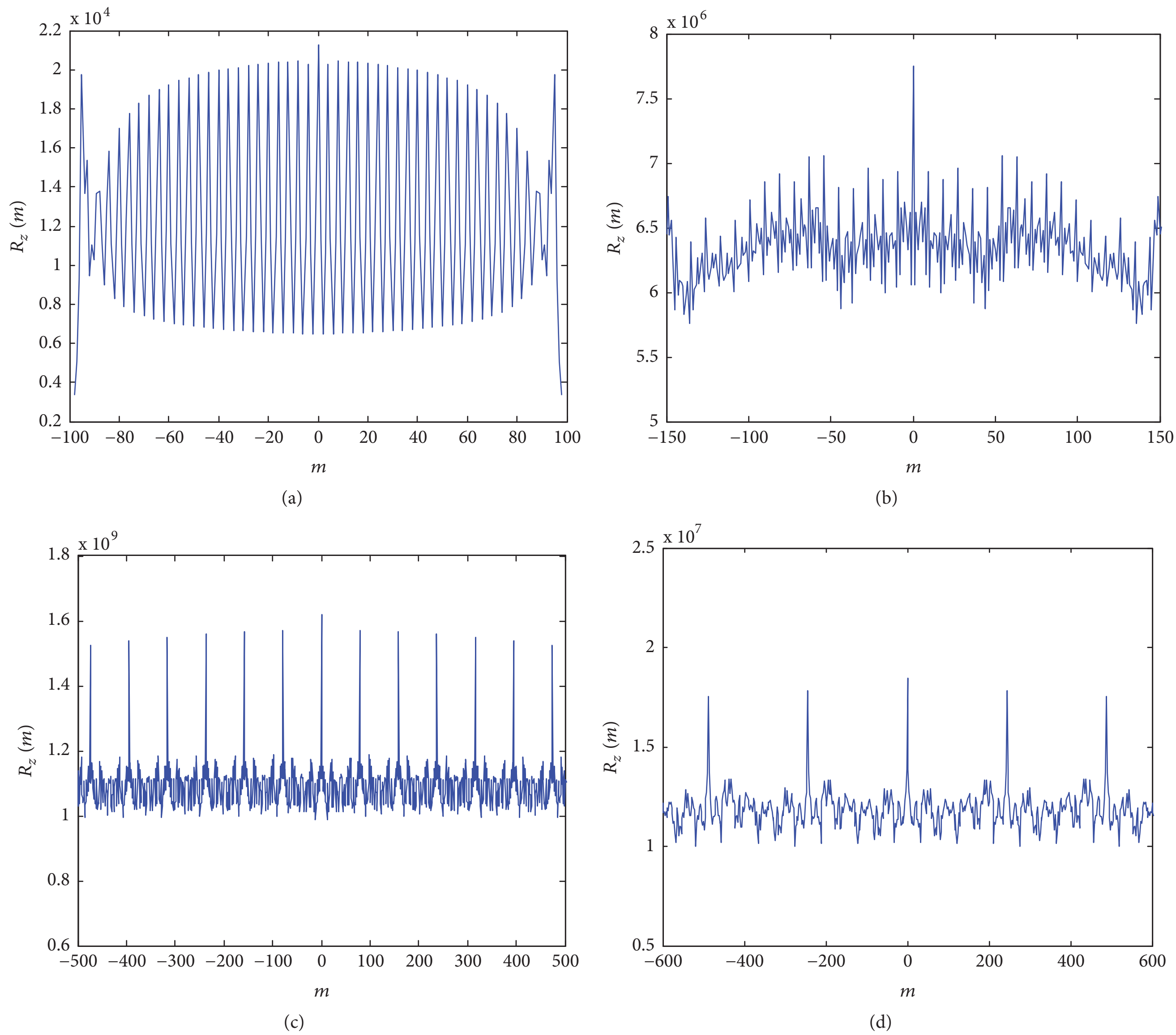

Figure 1: Autocorrelation test of Logistic chaotic sequences with different computational precision. (a) $L = 8$; (b) $L = 12$; (c) $L = 16$; (d) $L = 24$.

Step 1. For a discrete time sequence $X_N = \{X_1, X_2, \cdots X_N\}$, where m and τ represent the embedding dimension and a delay factor, respectively, the sequence X_N can be reconstructed as

$$X(n), X(n+\tau), \ldots, X(n+(m-1)\tau) \quad 1 \le n \le N - m + 1 \tag{7}$$

Step 2. Each sequence of (7) is placed depending on an ascending order.

$$X(n+(k_1-1)\tau) \le X(n+(k_2-1)\tau) \le \cdots \le X(n+(k_m-1)\tau) \tag{8}$$

Step 3. Further, $\pi_n = \{k_1, k_2, \cdots, k_m\}$ displays the original position index of each element, which is one of the possible order types of all $m!$ permutations. Suppose P_g is a symbol permutation and $\sum_{g=1}^{w} P_g = 1$, where $g = 1, 2, \cdots, w$, $w \le m!$. Then, PE H_p is defined as

$$H_p = -\sum_{g=1}^{w} P_g \ln P_g \tag{9}$$

When $H_p = 1/m!$, then H_p obtains the maximum value $\ln(m!)$. Further, the normalized PE h_p is defined as $h_p = H_p / \ln(m!)$.

PE test can be performed with discrete Logistic sequences of different computational precision. On the basis of a large number of experimental analysis, we set $m = 6$ and $\tau = 1$ with the purpose of obtaining more accurate PE values. The experimental results are shown in Table 1. As can be seen from

Table 1: The PE value of discrete Logistic sequences with different computational precision.

computational precision	PE value
8	0.22066
12	0.39636
16	0.57908
24	0.63111

the table, with the improvement of calculation precision, the PE value of the discrete chaotic sequence is larger. That is to say, the discrete chaotic sequences with high computational precision have higher complexity.

2.4. Statistical Analysis of Sequence Periodicity. In this section, we analyzed the periodicity of discrete Logistic sequences with different computational precision in detail. The experimental results are shown in Table 2, where p and r represent the period length of discrete Logistic sequences and the number of p-period, respectively. Under the same calculation precision L, we generated 2^L discrete Logistic sequences with different initial values z_1 and analyzed the periodicity of each chaotic sequence. It can be seen from the table that the limited computational precision will lead to a variety of short-period phenomena in discrete Logistic sequences. For instance, when computational precision =12, it offers periods 1, 3, 8, and 9. If such a chaotic sequence is used as a key stream for the stream cipher, it will seriously affect the security of the stream cipher privacy communication.

Moreover, we have done a more detailed analysis for the periodicity of the discrete Logistic sequences. On the basis of (5), we can generate a series of discrete Logistic sequences with different initial values. For arbitrary initial value z_0 and $z_0 \in [0, 2^L - 1]$, when two iterative values z_α and z_β in the sequence are equal ($z_\alpha = z_\beta$, $\alpha \neq \beta$), it can be concluded that the period length of the sequence is p ($p = \beta - \alpha$) and the set of periodic elements is $\Omega_p = \{z_\alpha, z_{\alpha+1}, \cdots, z_{\beta-1}\}$. Correspondingly, for another discrete Logistic sequence of p-period with initial value z_1, we assume that z_γ is an arbitrary iterative value on the periodic limit cycle of this sequence. If $z_\gamma \in \Omega_p$, then the initial value z_0 and z_1 will converge into the same periodic limit cycles. According to the above theoretical analysis, we can conduct corresponding statistical analysis experiments on all discrete Logistic sequences.

We take the calculation precision $L = 8$ as an example to give a detailed explanation. When calculation precision $L = 8$, the discrete Logistic sequences were generated with initial values 1, 2 and 3. The illustrations of iterations of the Logistic mapping with different initial values z_1 are shown in Figure 2. As can be seen from the figure, the process of iterations of the Logistic mapping is composed of transient and periodic stages. However, for the discrete Logistic sequences with different initial values, all sequences of 4-period have the same periodic limit cycles (11, 42, 140, 253). We did the same test for other initial values with $L = 8$, and the results showed the same periodic limit cycles.

In addition, when calculation precision $L = 12$, all discrete Logistic sequences of 3-period will converge into the same periodic limit cycles (771, 2503, 3893). Similarly, all sequences of 8-period and 9-period will also converge separately into the corresponding cycles (217, 822, 2628, 3767, 1210, 3410, 2284, 4041) and (3786, 1146, 3301, 2562, 3837, 970, 2961, 3281, 2611). When calculation precision $L = 16$ and 24, for every sequence of period $p (p > 1)$, all periodic stages display the same periodic limit cycles with period length p. This phenomenon has seriously affected the key space of chaotic stream ciphers.

In addition, we did the same experiment for Tent mapping with the purpose of analyzing statistical analysis of Tent sequence periodicity. The mathematical equation of Tent mapping can be described as follows:

$$x_{n+1} = \begin{cases} \dfrac{x_n}{a} & 0 \leq x_n < a \\ \dfrac{(1 - x_n)}{(1 - a)} & a \leq x_n \leq 1 \end{cases} \quad (10)$$

when $a = 0.5$, the above Tent mapping is a standard Tent mapping. Further generalization, we can get a kind of piecewise linear Tent mapping.

$$x_{n+1} = \begin{cases} \dfrac{x_n}{w} & 0 \leq x_n < w \\ \dfrac{(x_n - w)}{(0.5 - w)} & w \leq x_n < 0.5 \\ \dfrac{(1 - x_n - w)}{(0.5 - w)} & 0.5 \leq x_n < (1 - w) \\ \dfrac{(1 - x_n)}{w} & (1 - w) \leq x_n \leq 1 \end{cases} \quad (11)$$

When $w = 0.25$, $\hat{x}_n = (0.\varepsilon_1 \varepsilon_2 \cdots \varepsilon_L)_2 \approx x_n$, $R = 2^L$, $z_{n+1} = \hat{x}_{n+1} R$, and $z_n = \hat{x}_n R$, (11) is transformed into

$$z_{n+1} = \begin{cases} 4z_n & 0 \leq z_n < 0.25R \\ 4z_n - R & 0.25R \leq z_n < 0.5R \\ 3R - 4z_n & 0.5R \leq z_n < 0.75R \\ 4R - 4z_n & 0.75R \leq z_n \leq R \end{cases} \quad (12)$$

where L represent computational precision and $\hat{x}_n$ denotes approximate value of x_n. The value ranges of z_n and z_{n+1} are $[0, 2^L - 1]$. Equation (12) can get two stable zero solutions, which are 0 and R, respectively. If (12) appears $z_n = 0$ or $z_n = R$ in the iteration process, all subsequent iterations z_{n+1} will be zero value. In order to avoid this phenomenon, we improved (12) as follows:

$$z_{n+1} = \begin{cases} 4z_n + 1 & (0 \leq z_n < 0.25R) \cap (z_n = 2k - 1) \\ 4z_n - 1 & (0 \leq z_n < 0.25R) \cap (z_n = 2k) \\ 4z_n - R & 0.25R \leq z_n < 0.5R \\ 3R - 4z_n - 1 & 0.5R \leq z_n < 0.75R \\ 4R - 4z_n + 1 & (0.75R \leq z_n \leq R) \cap (z_n = 2k - 1) \\ 4R - 4z_n - 1 & (0.75R \leq z_n \leq R) \cap (z_n = 2k) \end{cases} \quad k \in N^* \quad (13)$$

Table 2: The statistical analysis of Logistic sequence periodicity with different computational precision.

computational precision L	The range of initial values $[0, 2^L - 1]$	Period length p	Number r	Percent $r/2^L$
8	$[0, 255]$	1	4	1.56%
		4	252	98.44%
12	$[0, 4095]$	1	10	0.24%
		3	8	0.195%
		8	98	2.39%
		9	3980	97.17%
16	$[0, 65535]$	1	4	0.006%
		7	112	0.17%
		18	1574	2.4%
		79	43998	67.14%
		119	19848	30.29%
24	$[0, 16777215]$	1	4	0.000%
		2	2556	0.003%
		5	22	0.000%
		8	8760	0.052%
		16	224	0.001%
		272	10553704	62.9%
		716	3047268	18.16%
		993	3164678	18.86%

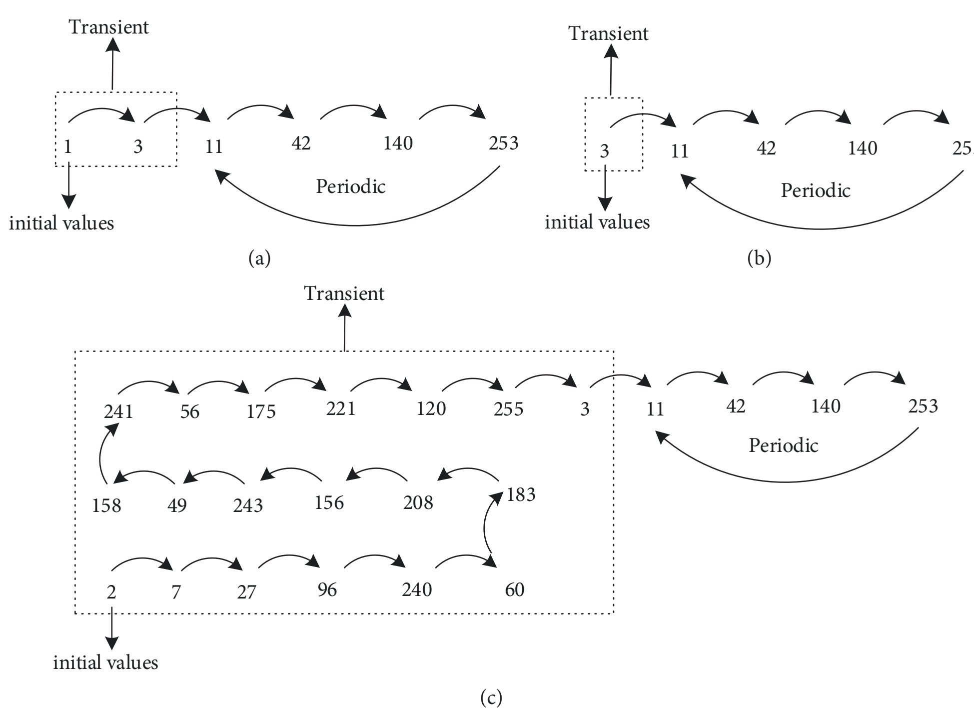

Figure 2: The illustration of iterations of the Logistic mapping with different initial values. (a) $z_1 = 1$; (b) $z_1 = 3$; (c) $z_1 = 2$.

where N^* is the set of positive integers. On the basis of (13), we did some experiments to analyze the periodicity of piecewise linear Tent sequences with different computational precision. The experimental results are shown in Table 3. It can be seen from the table that the limited computational precision can lead to a variety of short-period phenomena for discrete Tent sequences.

We still take the calculation precision $L = 8$ as an example to analyze the periodicity of the discrete Tent sequence in detail. When calculation precision $L = 8$, the Tent sequences

Table 3: The statistical analysis of Tent sequence periodicity with different computational precision.

computational precision L	The range of initial values $[0, 2^L - 1]$	Period length p	Number r	Percent $r/2^L$
8	$[0, 255]$	1	6	2.34%
		2	1	0.39%
		3	1	0.39%
		5	52	20.3125%
		7	1	0.39%
		12	195	76.172%
12	$[0, 4095]$	1	8	0.1953%
		2	1	0.0244%
		5	911	22.2412%
		7	118	2.881%
		8	219	5.34668%
		10	152	3.7109%
		11	1	0.0244%
		14	201	4.9072%
		30	1093	26.6846%
		43	440	10.7422%
		44	951	23.2178%
		240	1	0.0244%

were generated with initial values 2 and 3. The illustration of iterations of the Tent mapping with different initial values z_1 is shown in Figure 3. Obviously, Tent sequences with different initial values z_1 still converge to the same periodic limit cycles. Through a large number of experimental analysis, for every sequence of period p, we found that all periodic stages display the same periodic limit cycles with period length p. It shows a similar regularity to the discrete Logistic sequences.

3. A Novel Discrete Chaotic Sequence Generator

Based on the above experimental results and theoretical analysis, we found that a large number of short-period phenomena occur in discrete chaotic sequences under the influence of limited computational precision. In addition, the chaotic sequences with different initial values will converge to the same periodic limit cycles. These phenomena will seriously affect the security of chaotic ciphers and key space. To avoid the above problems, we designed a novel discrete chaotic sequence generator based on Logistic and Tent mapping, which is shown in Figure 4. Where z_1^{Lo} and z_1^{Te} represent the initial value of Logistic and Tent mapping. The $C = c_0, c_1, \cdots, c_{q-1}$ and $M = m_1, m_2, \cdots$ are the initial state and bit stream of q-order m-sequence, and b is the number of bits that are passed into the Logistic or Tent system every time. Moreover, the structure schematic diagram of the function $g(\cdot)$ is shown in Figure 5. The $\wedge$, $\oplus$, and $\vee$ represent the bitwise logical AND, XOR and OR operator, respectively. The $<<<$ is bit cycle left shift operator, and L is equal to the value of the calculation precision, which represent the number of bits for input and output data.

The generation process of the novel discrete chaotic sequences is given as follows.

Step 1. The initialized m-sequence generator outputs the b bits sequence stream $m_1, m_2, \cdots m_b$, and then $m_1, m_2, \cdots m_b$ is represented as a decimal form:

$$T = \sum_{i=1}^{b} m_i 2^{i-1} \tag{14}$$

where the choice of parameter b should correspond to the average period length of the digital chaotic system. For example, if the average period length of the digital chaotic sequence is 32 under a certain computational precision, the value of b should be roughly equal to 5 ($2^5 = 32$). Based on the above parameter selection, the iterative value will approximately fall into the periodic cycle after T iterations. At the same time, the iterative value should jump to another digital chaotic system to prevent continuous loop in a certain periodic limit cycle.

Step 2. Logistic mapping passes the last iteration value into function $g(\cdot)$ after T iterations. Next, the output result of the function $g(\cdot)$ is used as the initial iteration value of Tent mapping. Similarly, the Tent mapping also passes the last iteration value into function $g(\cdot)$ after the T iteration. The new output result of the function $g(\cdot)$ serves as the initial iteration value of Logistic mapping.

Step 3. The m-sequence generator outputs the b bits new sequence stream $m_{1+b}, m_{2+b}, \cdots m_{2b}$, and the binary sequence is also converted to decimal number T.

Step 4. Finally, the novel discrete chaotic sequence generator circulates continuously between step 2 and 3. The iterative

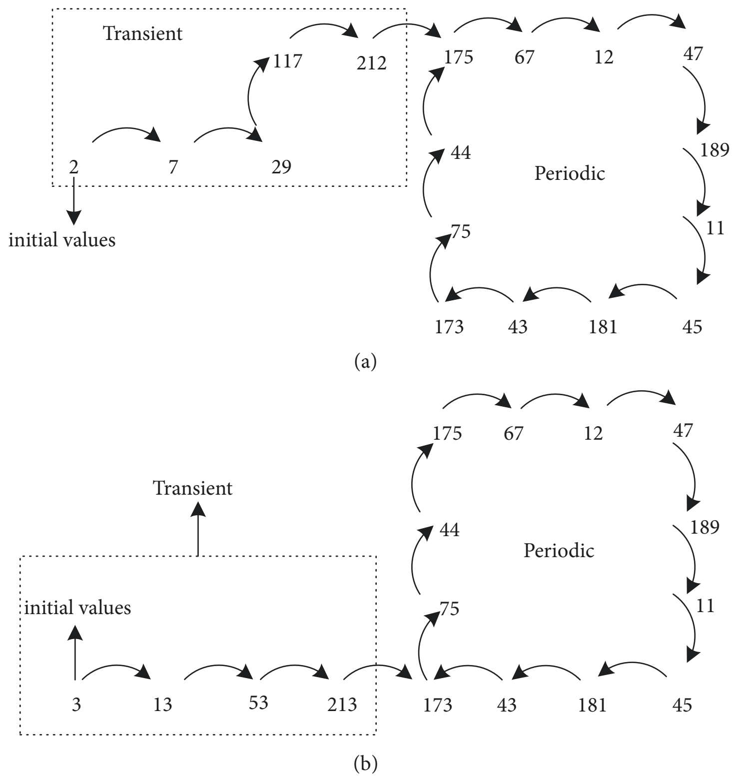

Figure 3: The illustration of iterations of the Tent mapping with different initial values. (a) $z_1 = 2$; (b) $z_1 = 3$.

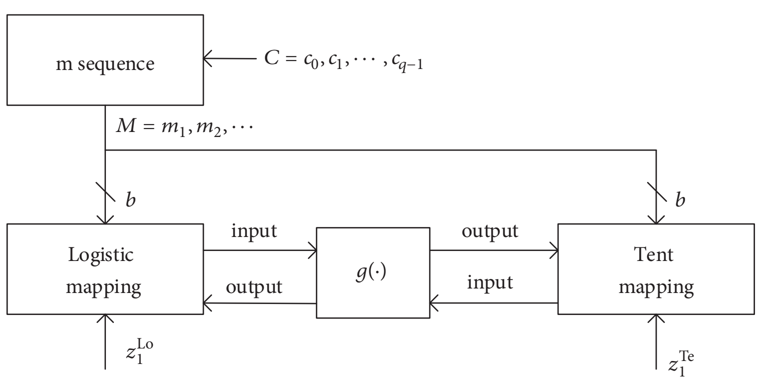

Figure 4: Block diagram of the novel discrete chaotic sequence generator.

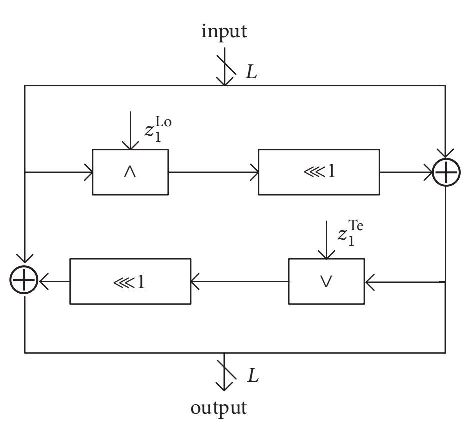

Figure 5: The structure schematic diagram of the function $g(\cdot)$.

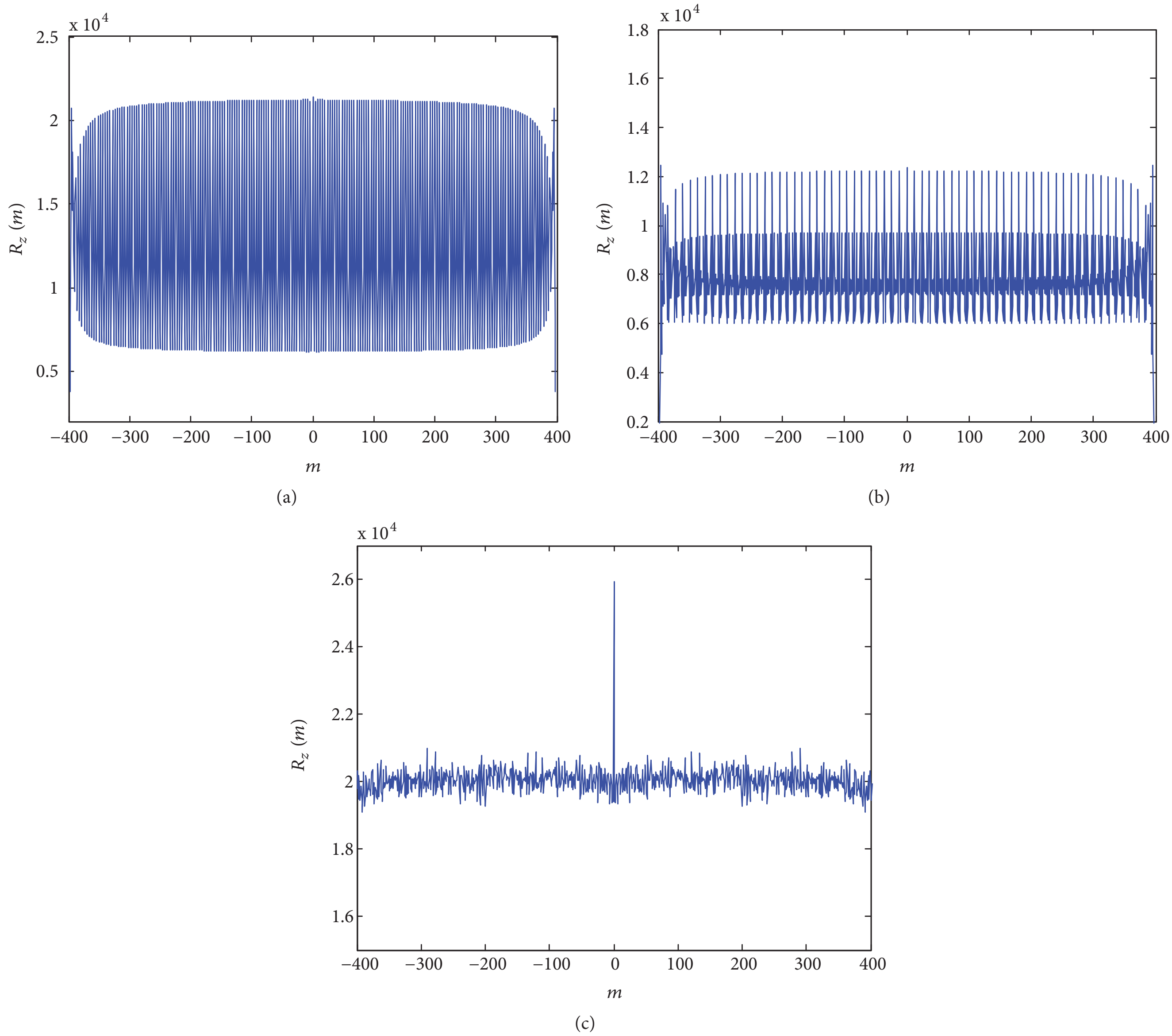

Figure 6: Autocorrelation test of chaotic sequences. (a) Logistic; (b) Tent; (c) improved method.

value of each round of Logistic and Tent mapping constitutes a new discrete chaotic sequence.

The design idea of this chaotic sequence generator is to control the number of iterations of Logistic and Tent mapping through m-sequence. When the iteration value is in periodic limit cycles, it can jump out of the periodic limit cycles in time with the purpose of avoiding the short-period phenomenon of the chaotic sequence. The purpose of function $g(\cdot)$ is to control the initial iteration value of each round of Logistic and Tent mapping in order to increase the complexity of the discrete chaotic sequence.

4. Comparative Analysis of Performance of Discrete Chaotic Sequences

4.1. Key Space. On the basis of these original Logistic and Tent sequence generator, for every sequence of period p, all periodic stages display the same periodic limit cycles with period length p. Therefore, for one-dimensional digital chaotic maps, the original key space 2^L will suffer a large degradation, because different initial values (secret key) will generate the same key stream except for a few iterative values in the transient state. Therefore, there are a large number of weak secret keys in key space 2^L. In contrast, actual key spaces of these generator are much less than 2^L. For instance, when calculation precision $L = 8$, key spaces of Logistic and Tent sequence generator are 2 and 6 (the number of different periodic limit cycles), respectively. However, for the novel discrete chaotic sequence generator, the key space should be 2^{2L+q}, where q is the order number of m-sequence. Further, when $L = 8$ and $q = 7$, the key space is 2^{23}. Hence, the key space of the improved sequence generator has been fully expanded.

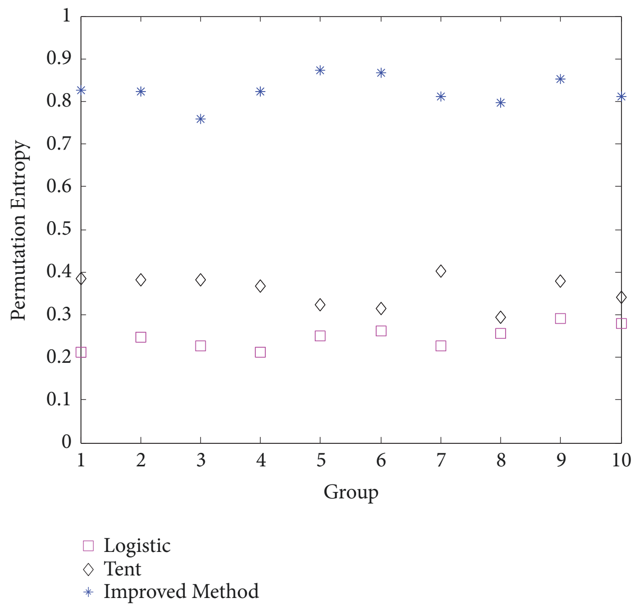

Figure 7: PE analysis with three different chaotic sequences.

4.2. Autocorrelation Test. Autocorrelation is a significant randomness measure. We generated three different discrete chaotic sequences (Logistic, Tent, and improved method) with calculation precision $L = 8$. Moreover, for improved method, we set $q = 7$. Results of autocorrelation test are shown in Figure 6. Obviously, autocorrelation function of the improved method approximates the δ function and shows good randomness. However, autocorrelation functions of original Logistic and Tent generator show a serious short-period phenomenon.

4.3. PE Analysis. In this section, we calculated the PE of chaotic sequences generated by the above three different generators with the purpose of comparing their complexities. The parameters of PE are selected to be the same as that in Section 2.3, and MATLAB simulation results are shown in Figure 7. We generated 10 sets of data to compare the complexity of chaotic sequences. As can be seen from the figure, improved method can significantly increase the complexity of chaotic sequences. The PE of sequence generated by improved method is larger than original Logistic and Tent sequences. Therefore, the method can improve the dynamical degradation of a digital chaotic map obviously.

5. Conclusion

In this paper, we analyze the Logistic chaotic sequences with different computational precision in detail through autocorrelation function, permutation entropy and statistical analysis of sequence periodicity. Based on the above experimental results, we found that there are a variety of short-period phenomena in chaotic sequences under finite computational precision. Surprisingly, for every sequence of period p, all periodic stages display the same periodic limit cycles with period length p. This phenomenon will seriously affect the key space and security of chaotic stream ciphers. Further, we did the same experiment for Tent mapping with the purpose of analyzing the periodicity of Tent sequence. The experimental results show a similar regularity to the discrete Logistic sequences. In view of this problem, we designed a novel discrete chaotic sequence generator. The experimental results show that the chaotic sequence generator can generate good pseudorandom chaotic sequences. This method has the advantages of simple structure and easy realization in hardware. In the case of finite computational precision, it can overcome the short-period behavior of chaotic sequence and effectively increase the key space. This method provides a feasible way for the application of chaos theory in the field of secure communication.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare no conflicts of interest.

Acknowledgments

This work was supported by the Natural Science Foundation of China (no. 61471158) and the "Modern Sensing Technology" Innovation Team Project of Heilongjiang Province (no. 2012TD007).

References

[1] J. S. A. Eyebe Fouda, J. Y. Effa, and M. Ali, "Highly secured chaotic block cipher for fast image encryption," *Applied Soft Computing*, vol. 25, pp. 435–444, 2014.

[2] N. W. Abderrahim, F. Z. Benmansour, and O. Seddiki, "A chaotic stream cipher based on symbolic dynamic description and synchronization," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 197–207, 2014.

[3] W. S. Sayed, A. G. Radwan, A. A. Rezk, and H. A. H. Fahmy, "Finite precision logistic map between computational efficiency and accuracy with encryption applications," *Complexity*, vol. 2017, Article ID 8692046, 21 pages, 2017.

[4] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Physical Review Letters*, vol. 71, no. 1, pp. 65–68, 1993.

[5] G. S. Yadav and A. Ojha, "Chaotic system-based secure data hiding scheme with high embedding capacity," *Computers and Electrical Engineering*, vol. 69, pp. 447–460, 2018.

[6] M. A. Murillo-Escobar, C. Cruz-Hernandez, L. Cardoza-Avendano, and R. Mendez-Ramirez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.

[7] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[8] R. Hasimoto-Beltran, "High-performance multimedia encryption system based on chaos," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 18, no. 2, Article ID 023110, 2008.

[9] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, “Cryptanalysis of a chaotic encryption system,” *Physics Letters A*, vol. 276, no. 1–4, pp. 191–196, 2000.

[10] P. Bergamo, P. D’Arco, A. De Santis, and L. Kocarev, “Security of public-key cryptosystems based on Chebyshev polynomials,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 52, no. 7, pp. 1382–1393, 2005.

[11] B. Du, X. Geng, F. Chen, J. Pan, and Q. Ding, “Generation and realization of digital chaotic key sequence based on double K-L transform,” *Journal of Electronics*, vol. 22, no. 1, pp. 131–134, 2013.

[12] N. Nagaraj, M. C. Shastry, and P. G. Vaidya, “Increasing average period lengths by switching of robust chaos maps in finite precision,” *The European Physical Journal Special Topics*, vol. 165, no. 1, pp. 73–83, 2008.

[13] J. Cernak, “Digital generators of chaos,” *Physics Letters A*, vol. 214, no. 3-4, pp. 151–160, 1996.

[14] J. G. Liu, Z. M. Ren, Q. Guo, and B. H. Wang, “Node importance ranking of complex networks,” *Acta Physica Sinica*, vol. 62, no. 17, Article ID 178901, 2013.

[15] G. Heidari-bateni and C. D. McGillem, “A chaotic direct-sequence spread-spectrum communication system,” *IEEE Transactions on Communications*, vol. 42, no. 2, pp. 1524–1527, 1994.

[16] H. Hu, Y. Xu, and Z. Zhu, “A method of improving the properties of digital chaotic system,” *Chaos, Solitons & Fractals*, vol. 38, no. 2, pp. 439–446, 2008.

[17] Y. Deng, H. Hu, N. Xiong, W. Xiong, and L. Liu, “A general hybrid model for chaos robust synchronization and degradation reduction,” *Information Sciences*, vol. 305, pp. 146–164, 2015.

[18] L. Cao, Y. Luo, S. Qiu, and J. Liu, “A perturbation method to the tent map based on Lyapunov exponent and its application,” *Chinese Physics B*, vol. 24, no. 10, Article ID 100501, 2015.

[19] R. M. May, “Simple mathematical models with very complicated dynamics,” *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.

[20] C. Fan, Q. Zhang, H. Sun, B. Song, and Q. Ding, “Designing network encryption machine based on Henon chaotic key algorithm,” *Journal of Applied Analysis and Computation*, vol. 6, no. 4, pp. 1126–1134, 2016.

[21] C. Bandt and B. Pompe, “Permutation entropy: a natural complexity measure for time series,” *Physical Review Letters*, vol. 88, no. 17, Article ID 174102, 2002.

[22] L. Liu and S. Miao, “Delay-introducing method to improve the dynamical degradation of a digital chaotic map,” *Information Sciences*, vol. 396, pp. 1–13, 2017.

[23] H. Hu, Y. Deng, and L. Liu, “Counteracting the dynamical degradation of digital chaos via hybrid control,” *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 6, pp. 1970–1984, 2014.