A novel algorithm to analyze the dynamics of digital chaotic maps in finite-precision domain

Chunlei Fan(范春雷)† and Qun Ding(丁群)

Electrical Engineering College, Heilongjiang University, Harbin 150080, *China*

(Received 2 January 2022; revised manuscript received 12 June 2022; accepted manuscript online 14 June 2022)

Chaotic maps are widely used to design pseudo-random sequence generators, chaotic ciphers, and secure communication systems. Nevertheless, the dynamic characteristics of digital chaos in finite-precision domain must be degraded in varying degrees due to the limited calculation accuracy of hardware equipment. To assess the dynamic properties of digital chaos, we design a periodic cycle location algorithm (PCLA) from a new perspective to analyze the dynamic degradation of digital chaos. The PCLA can divide the state-mapping graph of digital chaos into several connected subgraphs for the purpose of locating all fixed points and periodic limit cycles contained in a digital chaotic map. To test the versatility and availability of our proposed algorithm, the periodic distribution and security of 1-D logistic maps and 2-D Baker maps are analyzed in detail. Moreover, this algorithm is helpful to the design of anti-degradation algorithms for digital chaotic dynamics. These related studies can promote the application of chaos in engineering practice.

Keywords: digital chaos, dynamic degradation, state-mapping graph, periodicity analysis

PACS: 05.45.Ac, 05.45.Gg, 05.45.Mt **DOI:** 10.1088/1674-1056/ac785c

1. Introduction

As we all know, Lorenz's outstanding contribution opened the way for the study of chaos theory in 1963.[1] After more than half a century, scholars from various countries have also made many distinguished achievements in chaos theory and applied research,[2,3] which undoubtedly deepened people's understanding of chaotic systems. Some basic characteristics of chaos are also revealed, such as long-term unpredictability, positive Lyapunov exponent, intrinsic randomness, topological transfer, high sensitivity to initial conditions, and boundedness. These good characteristics of chaotic systems are highly consistent with the basic principles of confusion and diffusion in cryptography, which makes chaotic systems widely used in chaotic secure communication.

In recent years, scientific research achievements of chaos in engineering applications emerge one after another, such as a true random sequence generator,[4–6] multimedia data encryption,[7,8] digital watermarking,[9,10] a chaotic pseudo-random sequence generator and chaos-based masking technology.[11,12] However, while chaotic systems play an active role in secure communication and cryptography, the dynamic degradation of digital chaos has also become prominent. According to the mathematical definition of chaos such as Li–Yorke or Devaney, the classical chaos theory is defined in the continuous domain.[13] Nevertheless, when the chaotic system is implemented in a hardware processor (e.g., FPGA, DSP) with limited computational accuracy, it is not chaos in the strict mathematical sense. Due to the influence of truncation error and rounding error, the dynamic characteristics of digital chaos will undergo a series of degradation phenomena.[14,15] For example, the original non-periodic chaotic sequence will have a short-period phenomenon, and its high sensitivity to initial conditions, intrinsic randomness and ergodicity will also be greatly reduced or even disappear.[16] These dynamic degradation phenomena of digital chaos will undoubtedly have a negative impact on the security of chaotic secure communication and chaotic cryptography. Therefore, it is very crucial to analyze the dynamic degradation of digital chaos, especially to estimate the number of fixed points and periodic limit cycles accurately.

Actually, as early as 1988, Grebogi *et al.* found that a chaotic system that was numerically simulated on a computer would be affected by the rounding error of hardware equipment, and its chaotic orbit would become periodic.[17] In 2003, Li *et al.* analyzed the degree of dynamic degradation of the digital one-dimensional piecewise linear chaotic map (PWLCM) in fixed-point arithmetic domain.[18] They designed a set of dynamic indicators, which can quantitatively describe the dynamic degradation of the PWLCM to a certain extent. This method can promote the designs of chaotic pseudo-random generators with good performance and reduce the difficulty of cryptanalysis of chaotic encryption systems based on PWLCMs. In 2011, Miyazaki *et al.* found that different rounding methods have different effects on the transient branch length and cycle length of the digital logistic map.[19] The properties of discrete sequences generated by the digital logistic map depend heavily on the rounding method. In Ref. [20], based on strict statistical tests, a new algorithm is designed to analyze the weak keys of digital chaos. When analyzing the security of chaotic ciphers, it is found that the

†Corresponding author. E-mail: 2020021@hlju.edu.cn

© 2023 Chinese Physical Society and IOP Publishing Ltd

short periodicity of the digital chaotic orbit is the essential factor that causes many weak keys in chaotic ciphers. In addition, compared to floating-point operations, chaotic systems implemented by fixed-point operations have a longer average period of chaotic sequences. In 2016, Yoshioka and Kawano analyzed the periodic properties of Chebyshev polynomial sequences over the residue ring $Z/2^kZ$.[21] The analysis results show that a recently proposed public-key algorithm based on the polynomial is insecure. In Ref. [22], for different finite calculation precisions, Persohn and Povinelli conducted a detailed analysis of the periodicity of logistic chaotic sequences generated by floating-point operations. Due to the low efficiency of the calculation method, they used the Condor cluster supercomputer to perform large-scale parallel calculations, and statistically analyzed the transient length and period length of these sequences. The results show that the performance of the logistic sequence generator is not ideal. In 2018, when Frahm *et al.* analyzed the dynamic characteristics of the Chirikov standard map and the Arnold map, they found that there is a certain internal relationship between the dynamic system and the complex network.[23] In recent years, scholars at home and abroad have made outstanding contributions to the study of the dynamic characteristics of digital chaos.[24–27] Nevertheless, these algorithms have several limitations. First, most conventional methods have high time complexity. Therefore, it is bound to use high-performance supercomputers or graphics processing unit (GPU) for parallel computing to improve the execution speed of programs, which undoubtedly increases the consumption of hardware resources and the cost of experiments. Second, some proposed schemes lack a certain degree of versatility, that is, these methods are only suitable for analyzing the dynamic characteristics of one or several digital chaotic systems. Third, most schemes only calculate a general performance index, and cannot accurately locate all periodic cycles and fixed points contained in a digital chaotic map.

In this work, aiming at the limitations of the current schemes, we design a periodic cycle location algorithm (PCLA) from a new perspective to analyze the dynamic degradation of digital chaos. The PCLA can divide the state-mapping graph of digital chaos into several connected subgraphs with the purpose of locating all fixed points and periodic limit cycles contained in a digital chaotic map. In addition, this algorithm can also used to calculate the total number of state variables contained in each connected subgraph. Furthermore, in order to test the versatility and performability of our proposed algorithm, the periodic distribution and security of several typical digital chaotic maps (i.e., logistic map and Baker map) are analyzed in detail. Numerical simulation results show that these digital chaotic maps have obvious short period and multi period phenomena. This algorithm can clearly describe the internal mapping structure of the digital chaotic system under different calculation accuracies, thereby promoting the effective resistance and accurate evaluation of dynamic degradation of digital chaotic maps. In addition, a full understanding of the periodic distribution of digital Baker map is also helpful to design more excellent digital watermarking and image encryption schemes.

The rest of this paper is organized as follows: Section 2 describes digitization of chaotic maps in finite-precision domain. Section 3 puts forward a periodic cycle location algorithm. The performance of two chaotic maps, i.e., logistic and Baker, in finite-precision domains is analyzed in Section 4, and Section 5 concludes the paper.

2. Digitization of chaotic maps in finite-precision domain

In the classical chaos theory, all chaotic maps are defined in the continuous domain, and their dynamic characteristics are meaningful only in the continuous space with positive Lebesgue measure. However, when chaotic maps are implemented on hardware devices (e.g., FPGA and DSP) with limited computational accuracy, these chaotic maps will go through the process of digitization. In this section, let us assume that the iterative formula of a chaotic map can be defined as

$$x_{n+1} = f(x_n, \mu), \quad 0 \le x_n < 1, \tag{1}$$

where μ denotes the control parameter. In binary representation, x_n can be written as

$$x_n = (0.b_1 b_2 b_3 \cdots)_2 = \sum_{i=1}^{\infty} b_i 2^{-i}, \quad b_i \in \{0, 1\}, \tag{2}$$

where $(\cdot)_2$ means the contained digits in binary format. Assuming that m denotes limited computational accuracy, the binary representation of x_n can be approximated as

$$x_n \approx \hat{x}_n = (0.b_1 b_2 \cdots b_m)_2 = \sum_{i=1}^{m} b_i 2^{-i}. \tag{3}$$

In order to convert decimal fractions to integer representation, we introduce a new variable, i.e., y_n, which is defined as

$$y_n = 2^m \hat{x}_n. \tag{4}$$

Based on Eq. (4), the binary representation of y_n can be given by

$$y_n = (b_1 b_2 \cdots b_m)_2, \tag{5}$$

where y_n denotes the bits stored in the memory of hardware devices with the limited computational accuracy m. Substituting y_n into Eq. (1), we obtain

$$\frac{y_{n+1}}{2^m} = f\left(\frac{y_n}{2^m}, \mu\right), \quad 0 \le \frac{y_n}{2^m} < 1. \tag{6}$$

Multiplying both sides of Eq. (6) by 2^m, we obtain

$$y_{n+1} = \left\lfloor 2^m f\left(\frac{y_n}{2^m}, \mu\right) \right\rfloor, \quad y_n \in \{0,1,2,\ldots,2^m-1\}, \tag{7}$$

where $\lfloor\cdot\rfloor$ represents the integer part of a number. Now, Eq. (7) can be easily implemented on a hardware device for any given calculation accuracy m, as long as the hardware device can accurately store m-bit integers. As an example, the classical logistic map can be expressed as

$$x_{n+1} = f(x_n, \mu) = \mu x_n(1-x_n). \tag{8}$$

Furthermore, Eq. (8) can be re-expressed by substituting for the function $f(\cdot)$ from Eq. (8) into Eq. (7) to obtain

$$y_{n+1} = f(y_n) = \left\lfloor \mu y_n\left(1-\frac{y_n}{2^m}\right) \right\rfloor, \quad y_n \in \{0,1,2,\ldots,2^m-1\}, \tag{9}$$

where μ is generally set as 4. Based on Eq. (9), we can analyze the dynamic characteristics of the digital logistic map under different limited calculation accuracy.

3. Periodic cycle location algorithm for digital chaotic maps

In this section, in order to effectively analyze the dynamic degradation and internal structure of digital chaotic maps under different finite calculation precision, we develop a periodic cycle location algorithm (PCLA) that is based on a state-mapping graph. This algorithm has strong universality and can accurately calculate all periodic cycles and fixed points contained in a digital chaotic map. Due to the finite calculation accuracy of microprocessors, the value range of the digital logistic map will be limited to a finite state set $\Omega_m = \{0,1,\ldots,2^m-1\}$. Based on Eq. (9), we plot the state-mapping graph of the digital logistic map with limited calculation accuracy $m = 4$, as shown in Fig. 1. It is obvious that the state-mapping graph is composed of three connected subgraphs, among which the connection subgraph 1 containing the most state variables is called the maximal connection subgraph. Undoubtedly, if any two state variables are in the same connected subgraph, the two state variables must converge to the same fixed point or periodic cycle after several iterations. The core idea of the periodic cycle location algorithm is to divide the state-mapping graphs of digital chaotic maps with different calculation accuracies into multiple connected subgraphs and extract the unique periodic cycle or fixed point contained in each connected subgraph. In addition, this algorithm can also be used to calculate the number of state variables contained in each connected subgraph.

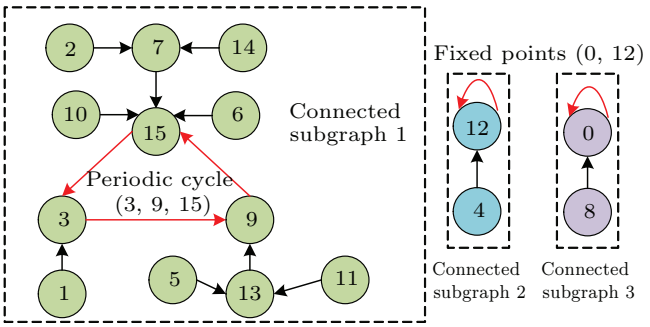


Fig. 1. State-mapping graph of the digital logistic map with limited calculation accuracy $m = 4$.

Specifically, the periodic cycle location algorithm (PCLA) is proposed as follows:

Step 1 Define an array of 1-D variables $\varepsilon = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_i, \ldots, \varepsilon_L\}$, where $L = 2^{md} - 1$ and d denotes the dimension of digital chaos in finite-precision domains. Please note that if the dimension of a digital chaotic map exceeds 1, dimensionality reduction is required before executing this algorithm. Then, the 1-D array ε can be initialized as

$$\varepsilon_i = i, \quad i \in \{0,1,2,\ldots,L\}. \tag{10}$$

Algorithm 1 State variable union algorithm (SVUA)

1. **SVUA begin**
2. Define two temporary variables sv_1 and sv_2
3. $sv_1 \leftarrow \varepsilon_{A_{0,r}}$; // the elements $A_{0,r}$ and $A_{1,r}$ in the matrix A
4. $sv_2 \leftarrow \varepsilon_{A_{1,r}}$;
5. **if** $sv_1 == sv_2$ **then** // Judging whether $A_{0,r}$ and $A_{1,r}$ are in the same connected subgraph
6. **return**;
7. **end if**
8. **for** t from 0 to L **do**
9. **if** $\varepsilon_t == sv_1$ **then**
10. $\varepsilon_t \leftarrow sv_2$;
11. **end if**
12. **end for**
13. **SVUA end**

Step 2 We can define a 2×2^L matrix A, which is given by

$$A = \begin{bmatrix} A_{0,0} & A_{0,1} & \ldots & A_{0,r} & \ldots & A_{0,L} \\ A_{1,0} & A_{1,1} & \ldots & A_{1,r} & \ldots & A_{1,L} \end{bmatrix}, \quad \begin{cases} A_{0,r} = r, \\ A_{1,r} = f(A_{0,r}), \end{cases} \tag{11}$$

where $r \in \{0,1,2,\ldots,L\}$, and the function $f(\cdot)$ denotes the iterative equation of digital chaos. Subsequently, variables $[A_{0,r},\ A_{1,r}]^{\mathrm{T}}$ in each column are separately used as a formal parameter of the state variable union algorithm (SVUA). Then, the SVUA with different formal parameters is executed one by one from variable $[A_{0,0},\ A_{1,0}]^{\mathrm{T}}$ to $[A_{0,L},\ A_{1,L}]^{\mathrm{T}}$. Furthermore, the state variable union algorithm is presented in algorithm 1 as a pseudocode. This algorithm can filter out state variables that are connected to each other, that is, it can split the state-mapping graph of digital chaos into several connected subgraphs.

Step 3 After Step 2 is carried out, the corresponding elements in the 1-D array ε are also updated. Moreover, we define a $1 \times L$ array γ, which can be initialized as

$$\gamma_j = 0,\ j \in \{0,1,2,\ldots,L\}. \tag{12}$$

Then, the element γ_{ε_i} in the array γ is incremented by 1 and let i range from 0 to L. Based on the above operation, the updated array γ contains the structural information of the digital chaotic map. Here, we can search for all non-zero elements in the array γ and define C as the set of all non-zero elements. The sum of all elements in set C is equal to 2^m. If $\gamma_j > 0$, the state variable j will be a fixed point or a node in a periodic cycle for digital chaos. In addition, the total number of nodes in the connected subgraph containing the state variable j is equal to γ_j. Moreover, if $j > 0$ and $j = f(j)$, the state variable j will be a fixed point of digital chaos in finite-precision domains. If $j > 0$ and $j \neq f(j)$, the state variable j will be a node in a limit cycle. The core idea of this algorithm is to assume that each node (i.e., state variable) of the digital chaotic map is isolated. Then, SVUA is used to determine which nodes are connected by the state-mapping relationship of the digital chaotic system. Those interconnected nodes are constructed into a connected subgraph. The above-mentioned periodic cycle location algorithm can precisely locate the fixed point and periodic distribution of digital chaos, which is of great significance for analyzing the degree of dynamic degradation of digital chaotic systems. It is worth noting that this algorithm is limited by storage bottlenecks when the computational accuracy m is greater than 32. This can make the program difficult to run. Therefore, when the finite calculation accuracy is relatively high, we can use Floyd's cycle-finding algorithm to calculate the cycle length of a single chaotic orbit, which occupies almost no memory (only a few variables' storage space). Furthermore, in order to speed up the running efficiency of the program, the CUDA platform can be used for large-scale parallel computing.

Furthermore, to assess the effectiveness and practicality of the PCLA, we take the case of the digitized logistic map with finite calculation accuracy $m = 3$ as an example. Based on the execution steps of the PCLA, we first define an array of 1-D variables $\varepsilon = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_i, \ldots, \varepsilon_L\}$. Because the dimension of the digital logistic map is 1 and the calculation accuracy m is 3, the variable L is equal to 7. Therefore, the array ε can be initialized as $\varepsilon = \{0,1,2,\ldots,7\}$. Next, according to the iterative formula of the digitized chaotic map, the matrix A is given by

$$A = \begin{bmatrix} 0 & 1 & 2 & 3 & \cdots & 7 \\ 0 & 3 & 6 & 7 & \cdots & 3 \end{bmatrix}. \tag{13}$$

According to the column order of matrix A, the periodic cycle location algorithm is performed from element $[0,0]^{\mathrm{T}}$ to $[7,3]^{\mathrm{T}}$. The update process of each element ε_i in the array ε is shown in Fig. 2. First, we can regard all state variables as multiple sets (i.e., connected subgraphs), and the nodes in each connected subgraph are connected. As shown in Fig. 2, based on the iterative relationship of the digital logistic map, these isolated state variables are continuously connected and eventually construct multiple connected subgraphs.

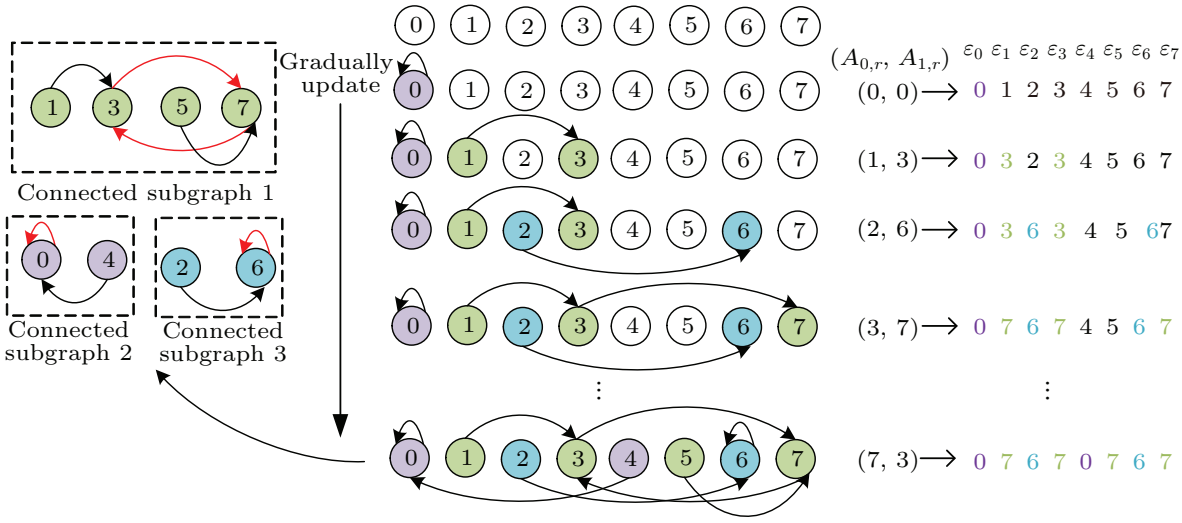


Fig. 2. Update process of each element ε_i in the array ε.

Moreover, the general structure diagram of the connected subgraph is illustrated in Fig. 3, which is composed of branch nodes and cyclic nodes. All branch nodes will eventually point to a cyclic node and fall into a limit cycle. Specifically, if the length p of a limit cycle is equal to 1, the cyclic node in the limit cycle will be a fixed point. Based on the above analysis, we find that if the subscript i of ε_i is equal to a branch node of the connected subgraph, the final value of the updated ε_i will equal the value of a cyclic node. As an example, the variable ε_1 is continuously updated from initial value 1 to 7. Note that, for the state-mapping graph of the digital logistic map with the precision $m = 3$, all branch nodes (1, 5) and partial cyclic nodes 3 of the connected subgraph 1 will eventually point to a cyclic node 7 in the limit cycle (3, 7).

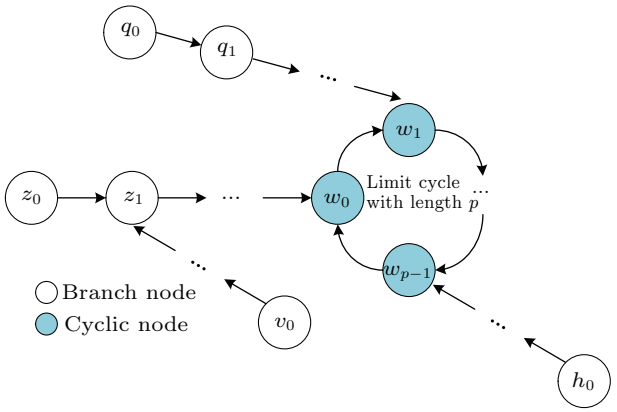


Fig. 3. General structure diagram of the connected subgraph.

Next, after the array ε is updated, we can calculate the $1 \times L$ array $\gamma = \{2,0,0,0,0,0,2,4\}$. Sequentially, we can search for all non-zero elements (i.e., γ_0, γ_6 and γ_7) in the array γ, the set C of all non-zero elements is $\{2,2,4\}$. Since $0 = f(0)$, $6 = f(6)$ and $7 \neq f(7) = 3$, we can conclude that the digitized logistic map with the precision $m = 3$ contains two fixed points (0, 6) and one limit cycle (3, 7).

4. Performance analysis of chaotic maps in finite-precision domains

4.1. Analyzing the dynamic degradation of the digital logistic map

4.1.1. Short-period and multi-period phenomena

In cryptography, the confidentiality of sequence ciphers depends on the performance of key stream generator. For chaotic cryptography, the key stream is usually generated by chaotic pseudo-random sequence generators. In order to improve the security of the encryption algorithm as much as possible, the generated key stream needs to have certain characteristics of a random sequence. An extremely large period can effectively increase the anti-attack ability of the cryptographic algorithm. Generally speaking, since the data rate of modern cipher machines is as high as 10^8 b/s, the period length of the key stream should not be less than 3×10^{16}. Chaotic time series in the continuous domain have the characteristics of non-periodicity and good randomness. Nevertheless, due to the limited calculation accuracy of hardware equipment, chaotic maps in finite-precision domains emerge many short-period and multi-period phenomena. In this section, for the digital logistic map, we perform the periodic cycle location algorithm for different calculation accuracy m, and the experimental results are listed in Table 1. Here, N_{cs} and N_{sv} represent the number of connected subgraphs and the total number of state variables contained in each connected subgraph. The variable node_{cn} denotes the cyclic node located by the PCLA, and p is the period length of the limit cycle contained in a certain connected subgraph. Note that if $p = 1$, the variable node_{cn} will be a fixed point.

Table 1. Periodicities of the digital logistic map with various calculation precisions.

Calculation precision m	N_{cs}	node_{cn}	N_{sv}	Period length p
3	3	0	2	1
		6	2	1
		7	4	2
4	3	0	2	1
		12	2	1
		15	12	3
5	2	0	30	1
		24	2	1
6	3	0	2	1
		48	2	1
		63	60	4
8	3	0	2	1
		192	2	1
		253	252	4
10	6	0	150	1
		768	2	1
		926	24	2
		973	424	3
		993	62	3
		1018	362	6
16	6	0	2	1
		49152	2	1
		64367	112	7
		64586	1574	18
		65482	19848	119
		65535	43998	79

As an example, the state-mapping graph of the digital logistic map with limited calculation accuracy $m = 6$ is divided into three connected subgraphs, as shown in Fig. 4. The variables $\text{node}_{cn} = 0, 48, 63$ are located as the cyclic nodes. Based on the corresponding period length p, we can draw conclusions that the digital logistic map has two fixed point (0, 48) and one limit cycle (63, 3, 11, 36). Since the largest N_{sv} is equal to 60, the maximal connection subgraph has sixty state variables. Undoubtedly, if the sixty state variables are used as initial values of the digital logistic map, all discrete chaotic

sequences generated by them will eventually fall into the periodic limit cycle (63, 3, 11, 36). From the table, as the calculation accuracy m increases, the maximum value of the period length p also becomes longer. However, the period length is far less than 3×10^{16}. The experimental results show that the digital chaotic map has obvious short-period and multi-period phenomena, which cannot guarantee the security of chaotic sequence ciphers.

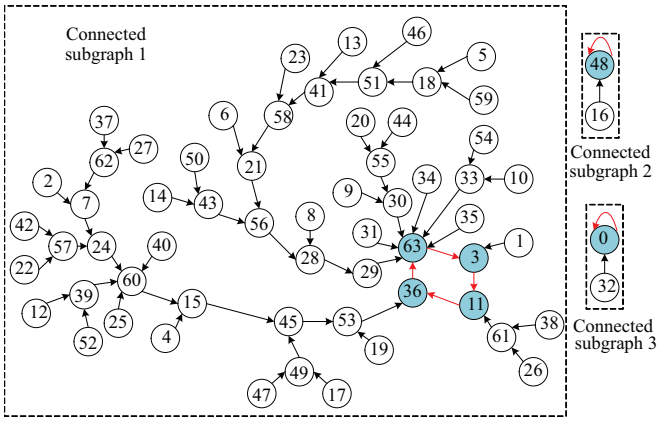


Fig. 4. State-mapping graph of the digital logistic map with limited calculation accuracy $m = 6$.

4.1.2. Cross-correlation of discrete chaotic sequences

Chaotic systems have strong initial value sensitivity. When the initial conditions change slightly, the difference between the two chaotic trajectories is not obvious in a short time. However, as time goes on, the chaotic trajectories under different initial conditions will occur huge deviation. The initial value sensitivity of chaos reduces the correlation between different discrete chaotic sequences. This characteristic makes the chaotic encryption algorithm have a large key space. However, for digital chaotic maps, the initial sensitivity is severely degraded due to the negative influence of limited calculation accuracy. As an example, we set the calculation accuracy $m = 7$ and generate three discrete logistic sequences with initial values 7, 23 and 39. Furthermore, we analyze the cross correlation between different discrete logistic sequences, as given in Fig. 5. The result of cross-correlation operation reflects the measure of similarity between two signals. Here, we assume that $\{x(n)\}$ and $\{y(n)\}$ denote two different logistic sequences. The cross-correlation function is defined as

$$R_{xy}(k) = \begin{cases} \frac{1}{N-k}\sum_{n=0}^{N-k-1} x(n+k)y(n), & k \geq 0, \\ R_{yx}(-k), & k < 0, \end{cases} \tag{14}$$

where $R_{xy}(k)$ and N represent the cross-correlation function and the length of digital logistic sequence. As shown in Fig. 5(a), the cross correlation of two logistic sequences with the initial values 7 and 39 shows dense peak lines, which implies strong correlation. When the initial values are equal to 7 and 23, it can be seen from Fig. 5(b) that the cross correlation of the two sequences is significantly reduced.

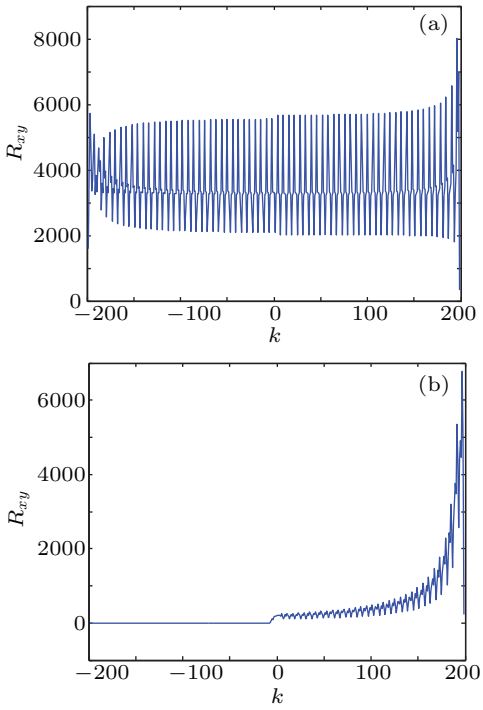


Fig. 5. Cross correlation of discrete logistic sequences with different initial values of (a) 7, 39 and (b) 7, 23.

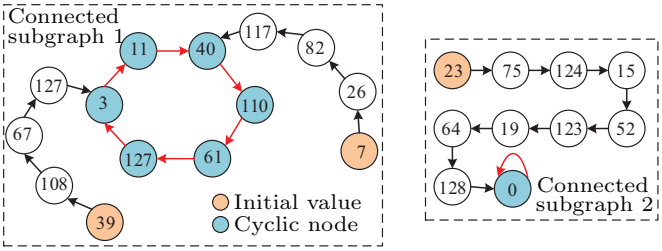


Fig. 6. Partial state-mapping graph of the digital logistic map with calculation accuracy $m = 7$.

Moreover, the reason for this phenomenon is that the three initial values are in different connected subgraphs. Partial state-mapping graph of the digital logistic map with calculation accuracy $m = 7$ is shown in Fig. 6. According to the figure, the initial values 7 and 39 are in the same connected subgraph, and the initial values 7 and 23 are in different connected subgraphs. This phenomenon implies that the discrete chaotic sequences generated by these initial values in the same connected subgraph are approximately equal to each other and differ only in the transient state. Based on the PCLA, we can obtain that the digital logistic map with the precision $m = 7$ has two fixed point (0, 96) and one limit cycle (11, 40, 110, 61, 127, 3). This phenomenon is common for the digital logistic map, which will reduce the effective key space of chaotic ciphers. From the above analysis, it can be concluded that the sensitivity of initial value and long-term unpredictability of digital chaotic maps are degraded due to the influence of calculation accuracy, and this undesirable phenomenon has caused

a non-negligible effect on the security of the chaotic pseudo-random sequence generator.

4.1.3. Ergodic property of the digital logistic map

In the classical chaos theory, the chaotic system has good ergodicity in its attraction domain. However, the digitized logistic map is affected by limited calculation accuracy, and its dynamic characteristics are severely degraded. It is difficult to achieve complete coverage of state variables in the range of state space. Therefore, in order to evaluate the degradation degree of ergodicity of the digital logistic map, under the same calculation accuracy, 2^m discrete logistic sequences are generated with different initial values. Furthermore, a set of discrete data can be obtained by calculating the state-space utilization of each logistic sequence. Based on the box-whisker plot, these data are statistically analyzed. The simulation results can be shown in Fig. 7. The box-whisker plot can describe the distribution of data in a relatively stable manner without being affected by outliers. As presented in Fig. 7, with the calculation accuracy increases, the state-space utilization of the digital logistic map gradually tends to 0.

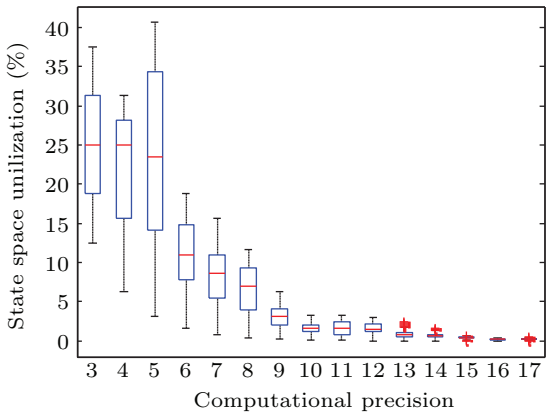


Fig. 7. State-space utilizations of the digital logistic map with various computational precisions.

4.1.4. Low permutation entropy

In 2002, Bandt *et al.* proposed a mensuration to analyze the complexity of discrete-time sequences, that is, permutation entropy (PE).[28] This method has many advantages, such as its robustness, fast-computing speed, and invariance to nonlinear monotonic transformations. The range of permutation entropy is between 0 and 1. The larger the PE value, the better the randomness and the higher the complexity of the discrete-time sequence. In this section, we calculate the permutation entropy of digital logistic sequences with various limited calculation precisions. The parameters of PE include embedding dimension θ and time delay τ, which are set as 6 and 1, respectively. For different digital logistic sequences, the results are listed in Table 2. From the table, as the calculation accuracy m increases, the PE value of the discrete logistic sequence also increases. However, when the calculation accuracy reaches 20, the PE value is only 0.62507, which cannot still meet the requirements of chaotic ciphers.

Table 2. PEs of digital logistic sequences with various calculation precisions.

Calculation precision m	PE value
4	0.16802
8	0.2286
16	0.58842
18	0.62252
20	0.62507

4.2. Analyzing the periodicity of the 2-D digital Baker map

Baker map is widely used in the field of multimedia data encryption, which is often responsible for scrambling digital images. It is called Baker map because the folding and stretching effect of this chaotic map is like that of a baker kneading dough. In this section, we briefly introduce the digitization of the 2-D Baker map. First, we assume that T_c is the iterative equation of the Baker map, which is based on the mapping relationship from a unit square to itself. Furthermore, the unit square is divided into k vertical bars (i.e., $[N_{i-1}, N_i] \times [0,1]$) along the x-axis, where $i \in \{1,2,\ldots,k\}$ and N_i is defined by

$$N_i = \begin{cases} P_1 + P_2 + \cdots + P_i, & 0 < i \le k, \\ 0, & i = 0, \end{cases} \tag{15}$$

where P_i represents the width of the above vertical bar and $P_1 + P_2 + \cdots + P_i = 1$. Each vertical bar is stretched along the x-axis direction and then compressed along the y-axis direction, and the schematic diagram of the Baker map is shown in Fig. 8. This process can also be expressed by a mathematical formula as

$$T_c(x,y) = \left(\frac{1}{P_i}(x - N_i), P_i y + N_i \right), \tag{16}$$

where $(x,y) \in [N_{i-1}, N_{i-1} + P_i] \times [0,1]$ and $i \in \{1,2,\ldots,k\}$. In this section, we consider the case of $k = 2$, and the mathematical equation of the digital 2-D Baker map can be given by

$$T_c \begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{cases} \begin{bmatrix} 2x_n + y_n \bmod 2 \\ \frac{1}{2}(y_n - (y_n \bmod 2)) \end{bmatrix}, & 0 \le x_n < 2^{m-1}, \\ \begin{bmatrix} 2x_n + y_n \bmod 2 - 2^m \\ \frac{1}{2}(y_n - (y_n \bmod 2)) + 2^{m-1} \end{bmatrix}, & 2^{m-1} \le x_n < 2^m, \end{cases} \tag{17}$$

where m denotes the limited computational precision, and $x_n, y_n \in \{0, 1, 2, \ldots, 2^m - 1\}$. Furthermore, we reduce the dimension of the 2-D digital Baker map, which is define as

$$\begin{cases} c_n = x_n \cdot 2^m + y_n, \\ c_{n+1} = \varphi(c_n) = x_{n+1} \cdot 2^m + y_{n+1}, \end{cases} \tag{18}$$

where c_n is an integer, and $c_n \in \{0, 1, \ldots, 2^{2m} - 1\}$. Based on Eq. (18), numerical conversion can be realized between c_n and (x_n, y_n).

Furthermore, based on the periodic cycle location algorithm, the period distribution of the digital Baker map under different calculation accuracies is analyzed in detail, and the experimental results are listed in Table 3. From the table, we can see that the digital Baker map has two fixed points and many short periodic limit cycles. When the calculation accuracy $m = 8$, it has 4116 connected subgraphs.

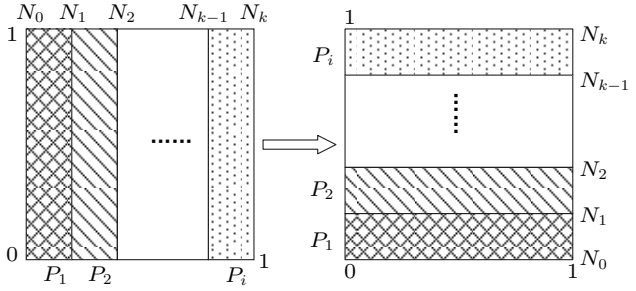


Fig. 8. Schematic diagram of the Baker map.

Table 3. Periodicities of the digital Baker map with various calculation precisions.

Calculation precision m	Fixed points	Number of connected subgraphs	Types of limit cycles length
1	(0 and 3)	3	1, 2
2	(0 and 15)	6	1, 2, 4
3	(0 and 63)	14	1, 2, 3, 6
4	(0 and 255)	36	1, 2, 4, 8
8	(0 and 65535)	4116	1, 2, 4, 8, 16

In order to reflect the internal mapping structure of the digital Baker map more intuitively, state-mapping graphs of the digital Baker map with calculation precisions $m = 2, 3$ are shown in Fig. 9. From the figure, regardless of the calculation accuracy m, all connected subgraphs of the digital 2-D Baker map have only cyclic nodes and no branch nodes. Compared with the digital logistic map, the digital Baker map has a large number of short limit cycles and no transient state. For the calculation accuracy m, the length of the limit cycle contained in the maximal connected subgraph is equal to $2m$.

When using the 2-D digital Baker map to scramble the pixels of a digital image, an important issue is to select the number of iterations. In this section, we consider how to choose an appropriate number of scrambling from the aspect of the period distribution of the Baker map. When the Baker map is used to scramble an image, (x_n, y_n) in Eq. (17) represents the position of the pixel of the digital image, and $2^m \times 2^m$ denotes the size of the digital image. Furthermore, we adopt the Fruits image with a size of 256×256 as the experimental data. Based on the PCLA, we can calculate the period distribution of the digital Baker map with the calculation accuracy $m = 8$, and the results are listed in Table 4. As can be seen from Table 4, there are five types of periodic cycles (i.e., 1, 2, 4, 8, and 16) for the Baker map. Among these limit cycles, there are 4080 periodic cycles with a length of 16, and the proportion of nodes is as high as 99.61%.

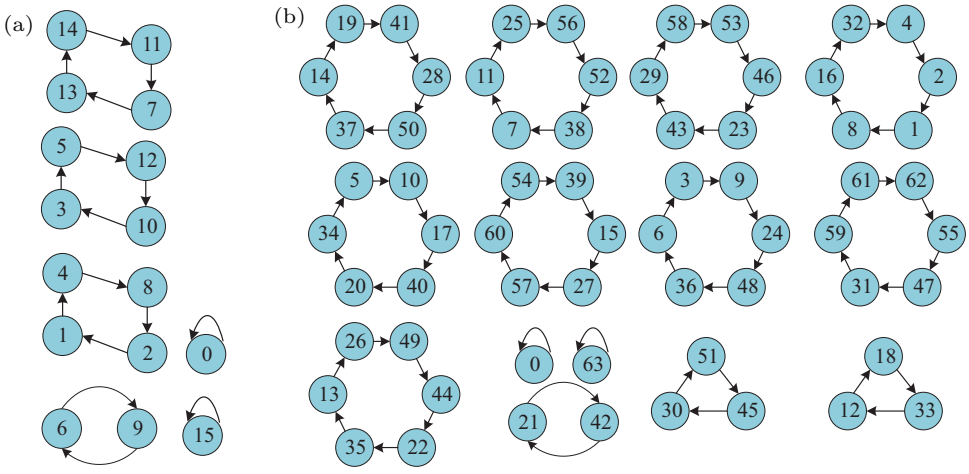


Fig. 9. State-mapping graph of the digital Baker map with different calculation precisions: (a) $m = 2$, and (b) $m = 3$.

Table 4. Period distribution of the digital Baker map in the precision $m = 8$.

Types of limit cycles length	Number of limit cycles	Number of nodes	Percent of nodes (%)
1	2	2	0.00305%
2	1	2	0.00305%
4	3	12	0.0183%
8	30	240	0.3662%
16	4080	65280	99.61%

It is not difficult to find that when the number N_b of iterations of the digital Baker map is an integer multiple of the length of any limit cycle, there must be corresponding pixels that are not scrambled in the digital image. The Fruits image with different scrambling times are shown in Fig. 10. A subjective evaluation method can be used to obtain that the three sub-graphs in Figs. 10(h)–10(j) have better scrambling effects. However, according to the above analysis of the periodicity of the digital Baker map, there are still 256 pixels that are not scrambled in Fig. 10(i). Therefore, based on the periodicity of the digital Baker map and the subjective evaluation method, we believe that the scrambling effect of digital image is the best when the scrambling number N_b is equal to 7 or 9.

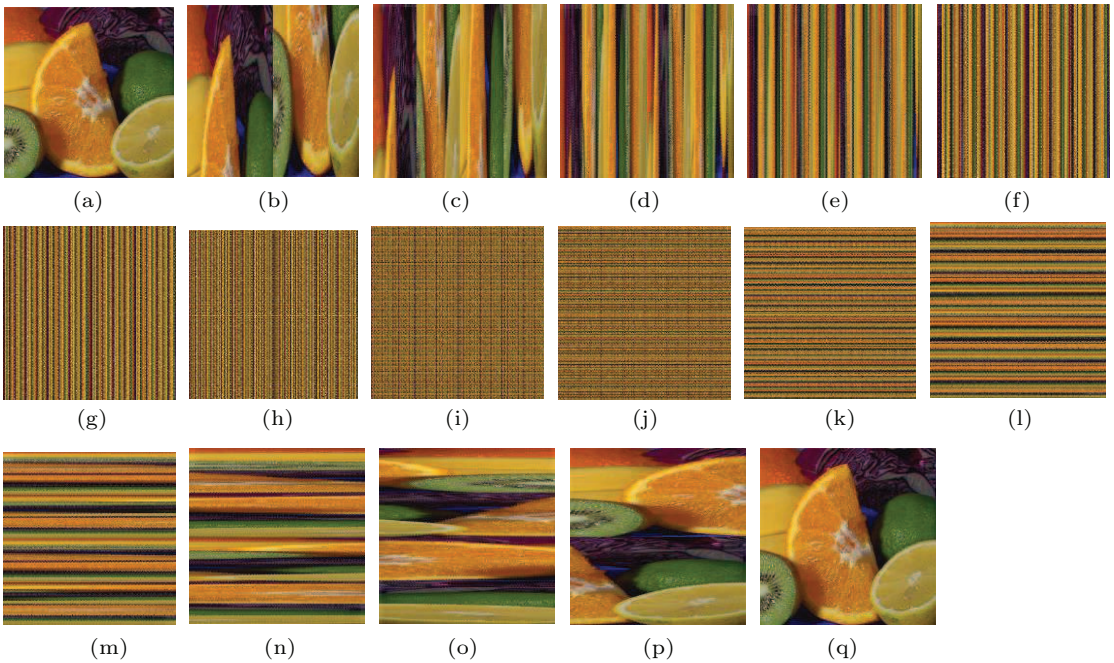


Fig. 10. Fruits image after being scrambled by the digital Baker map with various numbers of scrambling iterations N_b: (a) original image, (b) $N_b = 1$, (c) $N_b = 2$, (d) $N_b = 3$, (e) $N_b = 4$, (f) $N_b = 5$, (g) $N_b = 6$, (h) $N_b = 7$, (i) $N_b = 8$, (g) $N_b = 9$, (k) N_b=10, (l) $N_b = 11$, (m) $N_b = 12$, (n) $N_b = 13$, (o) $N_b = 14$, (p) $N_b = 15$, and (q) $N_b = 16$.

5. Conclusion

In order to facilitate the application of chaos in engineering practice, it is very crucial to effectively evaluate the characteristic degeneration of digital chaotic maps. In this paper, we employ a periodic cycle location algorithm (PCLA) that is based on state-mapping graph of digital chaos. This algorithm can precisely locate all fixed points and limit cycles contained in a digital chaotic map from a new perspective. Related experiments have been performed to verify the versatility and availability of the PCLA in terms of cross correlation of discrete chaotic sequences, period distribution, sequence complexity and state-space utilization. This algorithm can not only analyze the degree of dynamic degeneration of digital chaotic systems, but also effectively improve the security of the multimedia data encryption algorithm and help to understand the internal mapping law of the digital chaos.

Acknowledgements

Project supported by the National Natural Science Foundation of China (Grant No. 62101178) and the Fundamental Research Funds for the Higher Institutions in Heilongjiang Province, China (Grant No. 2020-KYYWF-1033).

References

[1] Lorenz E N 1963 *J. Atmosph. Sci.* **20** 130
[2] Lahmiri S and Bekiros S 2019 *Chaos Solitons & Fractals* **118** 35
[3] Bayani A, Rajagopal K, Khalaf A J M, Jafari S, Leutcho G D and Kengne J 2019 *Phys. Lett. A* **383** 1450
[4] Argyris A, Pikasis E and Syvridis D 2016 *J. Lightw. Technol.* **34** 5325
[5] Yeoh W Z, The J S and Chern H R 2019 *Multimedia Tools and Applications* **78** 15929
[6] Alcin M, Koyuncu I, Tuna M, Varan M and Pehlivan I 2019 *Int. J. Circuit Theory Appl.* **47** 365
[7] Hu G Z and Li B B 2021 *Nonlinear Dyn.* **103** 2819
[8] Chen B J, Yu S M, Zhang Z Q, Li D D U and Lü J H 2021 *Int. J. Bifur. Chaos* **31** 2150045
[9] Wu X Y and Guan Z H 2007 *Phys. Lett. A* **365** 403
[10] Jamal S S, Shah T and Hussain I 2013 *Nonlinear Dyn.* **73** 1469

[11] Hamza R 2017 *J. Inf. Security Appl.* **35** 119
[12] Pan J, Ding Q and Du B X 2012 *Int. J. Bifur. Chaos* **22** 1250125
[13] Li T Y and Yorke J A 1975 *Am. Math. Month.* **82** 985
[14] Luo Y L, Liu Y Q, Liu J X, Tang S B, Harkin J and Cao Y 2021 *Inf. Sci.* **556** 49
[15] Hu H P, Deng Y S and Liu L F 2014 *Commun. Nonlinear Sci. Numer. Simulat.* **19** 1970
[16] Fan C L and Ding Q 2021 *Nonlinear Dyn.* **103** 1081
[17] Grebogi C, Ott E and Yorke J A 1988 *Phys. Rev. A* **38** 3688
[18] Li S J, Chen G R and Mou X Q 2005 *Int. J. Bifur. Chaos* **15** 3119
[19] Miyazaki T, Araki S, Nogami Y and Uehara S 2011 *IEICE Trans. Fund. Electron. Commun. Comput. Sci.* **E94A** 1817
[20] Yin R M, Wang J, Yuan J, Shan X M and Wang X Q 2012 *Sci. China Inf. Sci.* **55** 1162
[21] Yoshioka D and Kawano K 2016 *IEEE Transactions on Circuits and Systems II-Express Briefs* **63** 778
[22] Persohn K J and Povinelli R J 2012 *Chaos Solitons & Fractals* **45** 238
[23] Frahm K M and Shepelyansky D L 2018 *Phys. Rev. E* **98** 032205
[24] Fan C L and Ding Q 2021 *Phys. Scr.* **96** 085212
[25] Zheng J, Hu H P and Xia X 2018 *Nonlinear Dyn.* **94** 1535
[26] Liu Y Q, Luo Y L, Song S X, Cao L C, Liu J X and Harkin J 2017 *Int. J. Bifur. Chaos* **27** 1750033
[27] Fan C L, Ding Q and Tse C K 2022 *Int. J. Bifur. Chaos* **32** 2250075
[28] Bandt C and Pompe B 2002 *Phys. Rev. Lett.* **88** 174102