An Iteration-Time Combination Method to Reduce the Dynamic Degradation of Digital Chaotic Maps

Yao Wu and Lingfeng Liu

School of Software, Nanchang University, Nanchang, Jiangxi 330031, China

Correspondence should be addressed to Lingfeng Liu; vatanoilcy@163.com

Received 19 May 2020; Revised 12 August 2020; Accepted 18 September 2020; Published 6 October 2020

A new and improved method based on the number of iterations is proposed to reduce the dynamical degradation of the digital chaotic map in this study. We construct a control function by introducing iteration time instead of external systems, thereby replacing the control parameters in the original chaotic map. Experimental results show that the chaotic map based on the iteration-time combination method is more complicated and effective. The period is extended without completely destroying the phase space, which indicates that our method is effective and can compete with other proposed techniques. A type of pseudorandom bit generator based on the iteration-time combination method is proposed to demonstrate its simple application.

1. Introduction

Chaos is a deterministic, pseudorandom process that appears in nonlinear dynamical systems. The irregularity of the process, sensitivity to the initial state, and good ergodicity of the range make this phenomenon compatible with modern cryptography, which requires the principle of confusion and diffusion.

However, due to the accuracy limitations of devices, most chaotic maps cannot reach their ideal state [1]. Thus, dynamic degradation occurs where a chaotic system falls into a loop in a limited phase space, which decreases the dynamic performance of the chaotic system and not meet the demand in many cases.

Many methods have been proposed for the phenomenon of dynamic degradation. These methods can be mainly divided into two categories. The first category does not need to introduce an external system [2, 3], and the second category needs to introduce an external system [4–15]. A detailed classification of the currently popular methods can be divided into the following five types. (1) The simplest approach is to use a high-precision equipment [3] because the original problem is caused by precision limitation. The phase state will increase with the improvement of precision. However, using the high-precision device can only extend the average period length of all pseudotracks but not the period length of each pseudotrack [16]. (2) Some methods extend the period of digital chaotic maps by cascading multiple chaotic maps [6, 7, 12]. The method can avoid the chaotic system entering the loop prematurely. However, it is difficult to control the dynamic complexity of cascading multiple chaotic systems. (3) Several methods by switching multiple chaotic maps [8, 9] among different dynamic systems on the basis of the specified switching policy. For example, if a sequential switching strategy is adopted, then the first dynamic system is iterated once, as well as the second dynamic system. Subsequently, the strategy goes back to the first one and then loops, which can extend the cycle effectively. Therefore, setting appropriate switching rules is important in this case. (4) Some methods introduce a pseudorandom perturbation source [5, 10–13] to improve dynamical degradation. In [5], specifying the lower limit of the length of the extended period and maintaining the original good statistical properties of chaotic dynamics were theoretically possible. This scenario will inevitably increase the implementation cost to a certain extent. In this method, the external pseudorandom perturbation source will determine the random performance of the chaotic map. (5) The analog–digital mixed control
method [14, 15] can also be effectively used to improve the dynamic degradation of chaotic maps by hybrid control of analogy chaotic systems and digital chaotic maps. However, in this approach, the phase space will be absolutely destroyed. The type of system cannot be regarded as a digital chaotic system. In addition to the method of utilizing high precision, another new method that does not require the introduction of an external system is the delay-introducing method [2]. This method improves the dynamic degradation by introducing the last iteration state. However, although a certain effect on improving dynamic degradation was achieved [2], the method remains limited and requires further improvement.

Therefore, in this study, we propose a new approach to improve dynamic degradation by introducing iteration times. In our model, we use a function that combines the number of iterations to replace the control parameters in the original digital chaotic map. Therefore, the control parameters are in a state of constant change, such that the chaotic system will not easily fall into a loop, and dynamic degradation phenomenon will not appear. Different from many other techniques [9, 16], our proposed method does not destroy the phase space of the original chaotic map while improving the dynamic degradation phenomenon. Thus, it is sufficiently competitive against other methods. The uppermost advantages of our proposed method are as follows:

(i) The method is simple to implement without introducing other external systems. It only introduces the iteration times, which are constantly changing. Thus, the method improves the dynamic degradation phenomenon while controlling the cost.

(ii) The method is universal and can be flexibly applied to various chaotic maps.

(iii) The method has been proven effective in improving dynamic degradation.

The remainder of this paper is organized as follows. Section 2 provides a preliminary introduction to the proposed approach. In Sections 3 and 4, we combine our proposed method with the one-dimensional logistic map and two-dimensional baker map, respectively, to compare our methods with the original digital maps. Then, the effectiveness of our method is evaluated through numerous experimental results. A pseudorandom bit generator (PRBG) based on our proposed method is presented in Section 5. Finally, Section 6 summarizes the study.

2. Iteration-Time Combination Method

A chaotic map, which is implemented on precision limited equipment, can be expressed as follows:

\[ x_{i+1} = \text{Pre}(f(a,x_i),p), \]

where \( x_i \) is the state variable after \( i \) times of iteration, and \( a \) is the control parameter of map \( f \) when \( a \in \mathbb{R} \); hence, map \( f \) will be chaotic. \( \text{Pre} \) denotes the precision function, and \( p \) is the current precision. So, \( \text{Pre}(f,p) \) means that when implemented on a computing device with precision \( p \), the output of the chaotic system \( f \) will be limited to a set of \( 2^p \) elements. Given the limited precision of the computer, the number of bits it can represent is certain. Thus, the phase space is finite, which leads to the chaotic map finally falling into the loop with the fixed control parameters. Specifically, \( x_p = x_q(p \neq q) \) is bound to happen after a couple of iteration times. At this time, if other parameters still remain unchanged, then the chaotic system will fall into the loop, and the period length is \( q - p \).

To improve the situation, we propose the iteration-time combination method to make the control parameter \( a \) change continuously as follows:

\[ x_{i+1} = \text{Pre}(f(h(i),x_i),p), \]

where \( h(i) \) is the control parameter function, and \( i \) is the number of iterations. The iteration-time combination method replaces the original control parameter \( a \) with a control parameter function \( h(i) \). The range of \( h(i) \) should be a subset of \( a \) (the range of \( a \)) to ensure that the mapping is still chaotic. Therefore, \( x_{i+1} \) is jointly determined by \( x_i \) and \( i \).

As the iteration continues, the number of iterations increases, that is, \( i \) continuously changes, so that the value of the control parameter function \( h(i) \) constantly changes, thereupon, when \( x_p = x_q \) but \( p \neq q \), and \( x_{p+1} \neq x_{q+1} \). At this time, the chaotic system will not fall into a cycle, and the period will be extended. The number of iterations \( i \) does not require additional computing resources, thereby resulting in a considerable cost reduction.

On the basis of different chaotic maps, we can construct different functions as follows:

\[ h(i) = b_1|\sin(g(i))| + b_2, \]

where \( g(i) \in (-\infty, +\infty) \) is a function related to \( i \); \( |\sin(g(i))| \in [0, 1] \); and parameters \( b_1 \) and \( b_2 \) are used to adjust the range of \( h(i) \) in \( a \).

The function \( g(i) \) is not fixed and can be flexibly changed as required, under the premise of meeting the relevant evaluation indicators. It can be a linear or nonlinear function about \( i \). We recommend that simple functions should be constructed as much as possible to reduce implementation costs. The output of \( g(i) \) is used as the input to the sine trigonometric function. The range of the trigonometric function is \([-1, 1]\), and the range of \( h(i) \) must satisfy the corresponding conditions on the basis of different chaotic maps to keep the chaotic state. Thus, the absolute value which belongs to \([0, 1]\) is taken to adjust the range easily. Then, parameters \( b_1 \) and \( b_2 \) are adjusted in accordance with the requirements of the specific chaotic system on control parameters.

In the proposed model, we only modify the control parameters of the chaotic system, whereas the control parameters still meet the original range requirements. Hence, the phase space will not be destroyed. Thus, the method can be regarded as a remedy, instead of generating a new random source. Control parameters also exist in each chaotic system. Thus, our proposed method can be used universally.
The one-dimensional logistic chaotic map and the two-dimensional baker chaotic map will be introduced in the following sections.

3. Example 1: Logistic Map

The logistic map on precision limited equipment is defined as

\[ x_{i+1} = \text{Pre}(a \cdot x_i \cdot (1 - x_i), p), \]

where \( a \) is the control parameter, and \( a \in (3.5699, 4) \) to make sure that the map is chaotic. In this section, for the sake of improving dynamical degradation efficiently, we construct \( g(i) = i \) to illustrate the practicality of this iteration-time combination method. Thus, our model is defined as

\[ h(i) = b|\sin(i)| + 4 - b, \]

where \( b \) is an adjustment parameter, and since the range of \( h(i) \) is \((3.5699, 4)\), \( b \in (0.4301, 4) \). Thus, the iteration-time combined logistic map can be expressed as

\[ x_{i+1} = \text{Pre}((b|\sin(i)| + 4 - b) \cdot x_i \cdot (1 - x_i), p). \]

Next, we verify the efficiency of our method by comparing relevant features with the original logistic map and other improved methods.

3.1. Trajectories and Phase Diagrams. The same parameters should be used for clear and accurate comparison. We set the precision to be \( 2^{-16} \), and the initial values are randomly selected as \( x_0 = 0.14, a = 3.9, \) and \( b = 0.1 \). We performed experiments on different sets of initial values. The experimental results are similar, so we randomly select the results of one set of initial values as a representative. Figures 1(a) and 1(b) show the trajectories of the original digital logistic map and the digital logistic map of the proposed method, respectively. Figure 1(a) shows that the original digital logistic map falls into a loop quickly, and its cycle length is 58. By contrast, Figure 1(b) is still random. Thus, the iteration-time combined digital logistic method can effectively change the phenomenon of falling into the cycle.

The original digital logistic map has a limited range of values due to the trapped period, and its phase diagram is an intermittent curve, as shown in Figure 2(a). However, the points on the phase diagram of the iteration-time combined digital logistic map are denser (Figure 2(b)). The following comparison shows that the improved chaotic map does not change the phase space of the original chaotic map but is supplemented on the basis of the original phase space to expand its range.

3.2. Auto-Correlation Analysis. The auto-correlation function is one of the important metrics in assessing whether a sequence is random and independent. For a qualified random sequence, the auto-correlation function should be a delta function. When the precision is still set as \( 2^{-16} \), the images of the auto-correlation function of the original digital logistic map and the iteration-time combined digital logistic map are shown in Figures 3(a) and 3(b), respectively. It can be seen from Figure 3(a) that as the time interval increases, the auto-correlation of the sequence does not immediately approach zero but will have obvious sidelobes; hence, the sequence generated by the original digital logistic map has a certain correlation. While the image shown in Figure 3(b) is highly delta-like, which indicates that the sequence has weak autocorrelation. This shows that the iteration-time combined digital logistic map has a better chaotic property to some extent.

3.3. Period Analysis. Period analysis is an essential factor wherein the sequence generated by the digital chaotic map falls into the cycle faster than the ideal. Therefore, analysing the periodicity of the sequence is necessary. The initial value and the value of the control parameter remain the same as before. Table 1 details the comparison results when the precision is the same. Contrast whether the sequence generated by the original chaotic map and the improved chaotic map have a period and its length. The iteration-time combined digital logistic map changes the dynamic degradation of the chaotic system due to the limited accuracy of the device. Hence, it cannot detect the period when the precision is larger than \( 2^{-12} \). However, in [4], the precision needs to be as large as \( 2^{-18} \). Thus, our method is superior to that presented in the previous study in the case of cycle improvement.

3.4. Complexity Analysis

3.4.1. Approximate Entropy (ApEn) Analysis. ApEn is a nonlinear parameter of the complexity and statistical quantification of a metric sequence proposed by Pincus in 1991 [17]. The larger the ApEn is, the lower the self-similarity of the sequence will be, and the sequence will be more complex. Conversely, the sequence self-similarity will be higher. ApEn is weakly dependent on the sequence length. Only a short amount of data is required to obtain a robust entropy value. In this section, we calculate the values of the two mappings at various precisions separately. The ApEn has considerably increased, as shown in Figure 4. The value obtained by the iteration-time combined digital logistic map is always above the value of the original digital logistic map. This result shows that our approach can also increase the complexity of the digital logistic map. Furthermore, the ApEn of our method is also slightly higher than that of [4], which is an improved method by bi-coupling digital chaotic maps that needs to introduce an external system.

3.4.2. Permutation Entropy (PE) Analysis. PE is a method for entropy calculation based on the permutation model, which is mainly used to analyse the characteristics of nonlinear chaotic systems. Similar to ApEn, PE is another important factor used to evaluate the dynamical characteristics of a chaotic sequence. In comparison with other analysis methods, its calculation process is simpler, of strong
antinoise ability, and only needs a shorter sequence to estimate a more stable system eigenvalue.

On the basis of equations (4) and (6), the PE results are obtained, as shown in Figure 5. The yellow line is always above the blue line when at the same precision. Thus, the PE of the sequence generated by equation (6) is larger than equation (4). Therefore, the iteration-time combined digital logistic method has a better complex performance that the original method.

4. Example 2: Baker Map

We also test and analyse the two-dimensional baker map, which is another popular chaotic map, to further illustrate the effectiveness of the proposed method of introducing iteration times.

The baker map on precision limited equipment can be expressed as follows:

\[
B(x_{i+1}, y_{i+1}) = \begin{cases} 
\text{Pre}\left(\frac{x_i}{a}, ay_i\right), & 0 < x \leq a, \\
\text{Pre}\left(\frac{x_i - a}{1-a}, (1-a)y_i + a\right), & a < x \leq 1, 
\end{cases}
\]

where \(a\) is the control parameter in the interval of \((0, 1)\) to generate a chaotic map. Following equation (3), we attempt to represent the control parameters as functions related to the number of iterations. In this test, we define \(g(x)\) as follows:

\[
g(x) = \tan\left(\hat{x}\right).
\]
Figure 3: Auto-correlation function of two maps. (a) Digital logistic sequence; (b) iteration-time combined digital logistic sequence.

Table 1: Period analysis of two maps (U denotes undetected).

| Precision | Original digital logistic map | Iteration-time combined digital logistic map |
|-----------|------------------------------|---------------------------------------------|
| $2^{-8}$  | 12                           | 355                                         |
| $2^{-10}$ | 13                           | 312689                                      |
| $2^{-12}$ | 8                            | U                                           |
| $2^{-14}$ | 74                           | U                                           |
| $2^{-16}$ | 58                           | U                                           |
| $2^{-18}$ | 201                          | U                                           |
| $2^{-20}$ | 898                          | U                                           |
| $2^{-22}$ | 1397                         | U                                           |
| $2^{-24}$ | 3111                         | U                                           |
| $2^{-26}$ | 734                          | U                                           |
| $2^{-28}$ | 10739                        | U                                           |
| $2^{-30}$ | 6042                         | U                                           |
| $2^{-32}$ | 2996                         | U                                           |

Figure 4: The ApEn of the digital logistic map, iteration-time combined digital logistic map, and coupled digital logistic map.

Figure 5: The PE of the digital logistic map and iteration-time combined digital logistic map.
Thus, 
\[ h(i) = b|\sin(\tan(i))| + 1 - b, \] (9)

where \( b \in (0, 1) \) is the adjustment parameter. Thus, the iteration-time combined digital baker map can be expressed as in the following equation.

\[
B(x_{i+1}, y_{i+1}) = \begin{cases} 
\text{Pre} \left( \frac{x_i}{b|\sin(\tan(i))| + 1 - b}, b|\sin(\tan(i))| + 1 - by_i, p \right), & 0 < x \leq b|\sin(\tan(i))| + 1 - b, \\
\text{Pre} \left( \frac{x_i - b|\sin(\tan(i))| + 1 - b}{b - b|\sin(\tan(i))|} \cdot \left( \left| \frac{y_i + b|\sin(\tan(i))|}{b|\sin(\tan(i))| + 1 - b} \right| \right), p, \right), & b|\sin(\tan(i))| + 1 - b < x \leq 1.
\end{cases}
\] (10)

Experiments are performed according to the above formula, and the control parameters in the improved digital baker map are completely random. Due to the special nature of the Baker map itself, here, avoiding the situation that the chaotic map falls into a certain point and cannot jump out on account of that the control parameters tend to zero \((a \to 0)\) is necessary. Hence, we need to add a step to the algorithm to prevent such situation. We add the judgment step, the pseudocode of which is shown as follows:

```plaintext
if \text{pre}(x(i) - b, p) == 0, \\
a = \text{Pre}((b * \text{abs}(\sin(g(i)))) + 1 - b)p.
```

When the control parameter function \( h(i) = 0 \), that is, \( a = 0 \), the judgment condition is true. Replace \( a \) with another expression. \( g(i) \) can be replaced by many other expressions, and we set \( g(i) = \tan(i) \) in this study. In a word, the most important thing is to avoid making the control parameter \( a = h(i) = 0 \). \text{abs} indicates the absolute value function.

Similarly, we perform an experiment as the iteration-time combined digital logistic map in Section 3 to assess the performance of the improved digital baker map. The results of the \( y \)-dimensional variables are basically consistent with the results of the \( x \)-dimensional variables. Thus, we only demonstrate the results of the \( x \)-dimensional variables. We set \( x_0 = 0.1237, y_0 = 0.6187, a = 0.49, \) and \( b = 0.49 \). First, we set the precision to be \( 2^{-12} \). Figure 6(a) shows that the original digital baker map quickly enters the cycle after approximately 220 iterations. However, Figure 6(b) is still in a random state. Figure 7 shows the phase diagrams of the digital baker map and the digital iteration-time combined baker map after iterating the same number of times. The phase space of the two digital baker maps is distributed in the space \((0, 1) \times (0, 1)\). The points of the phase space in Figure 7(b) are significantly denser. Thus, the proposed method can effectively extend the cycle and improve the dynamic degradation phenomenon.

According to equations (7) and (10), we perform an auto-correlation analysis on the obtained \( x \)-dimensional sequences to obtain a comparison result, as shown in Figure 8. The sequence generated by our method is an ideal delta function. Nevertheless, the sequence generated by the results of the Figure 8. kQhe sequence generated by our method is an ideal dynamic degradation phenomenon.

The period of the original digital baker map and the improved digital iteration-time combined baker map at various precisions is statistically analysed, as shown in Table 2. In the test data, the original baker map can always detect cycles; however, the sequences generated by our method cannot detect the period under the same precision. The effectiveness of our approach for improving the dynamic degradation is demonstrated.

Finally, we evaluate the complexity of the sequence. Figures 9 and 10 show the results for ApEn and PE of different maps at various precisions. The ApEn of the original digital baker map is the lowest (Figure 9). The iteration-time combined digital baker map and coupled baker map in [4] are considerably higher than the original one, whereas the iteration-time combined digital baker map is slightly better. The PE of the original digital baker map is lower when the precision is lower, whereas the PE of the iteration-time combined digital baker map always maintains a satisfactory result (Figure 10). On this basis, the complexity of the iteration-time combination method is acceptable and outstanding.

In addition, in order to ensure the authenticity of the experiments, we used different sets of initial values to evaluate the experiments. The experimental results are similar to the above, so we will not repeat them here.

5. PRBG Based on the Iteration-Time Combined Digital Chaotic Map

5.1. PRBG. Pseudorandom sequence is the sequence that can be predetermined and can be repeatedly produced and replicated but has the random nature of a random sequence (i.e., statistical properties). Consequently, scientists have proposed many PRBGs. Given the excellent performance of chaotic systems in cryptography, quite a few PRBGs are based on chaotic systems [18–21]. In this section, a type of pseudorandom bit generator based on the iteration-time combined digital baker method is proposed, as shown in equation (10).
The proposed PRBG can be represented as

$$b_i = \begin{cases} \lfloor y_i \cdot 10^6 \mod 256 \rfloor, & \text{if } x_i > 0.5, \\ \lfloor y_i \cdot 10^5 \mod 256 \rfloor, & \text{if } x_i < 0.5, \end{cases}$$

(12)

where $\lfloor N \rfloor$ denotes the round-down function, and only the integer part is reserved. We use the method of integer remainder quantization. First, we generate a series of random numbers on the basis of the two-dimensional digital baker map. Next, the iteratively generated number that belongs to $(0, 1)$ is converted to a number between $(0, 255)$, which is then converted to an 8-bit binary number. The specific process is shown in Figure 11.

A series of qualified pseudorandom sequences should be able to pass various statistical tests that evaluate the randomness of the sequence. We adopt the NIST statistical test, key space analysis, key sensitivity analysis, and linear complexity analysis. The values for the experiment are set as follows: $x_0 = 0.1237$, $y_0 = 0.6187$, and $b = 0.49$, and the precision is set as $2^{-12}$.

5.2. Statistical Tests. To prove that the pseudorandom number generator generated by the proposed method is secure and reliable, it must be statistically tested. At present, the most popular statistical tests for PRBG are as follows: (1) NIST suite of statistical tests [22, 23], (2) Donald Knuth’s statistical tests [24], (3) Crypt-XS suite of statistical tests [25], and (4) DIEHARD suite of statistical tests [26]. These test suites can explain the randomness of the sequence to some extent. Among them, the NIST statistical test suite contains various independent statistical tests, which can be relatively comprehensive in statistical analysis. Thus, in this study, we select the NIST statistical test suite.
Table 2: Period analysis of two maps ($U$ denotes undetected).

| Precision | Original digital baker map | Iteration-time combined digital baker map |
|-----------|---------------------------|-------------------------------------------|
| $2^{-8}$  | 19                        | 3371                                       |
| $2^{-10}$ | 39                        | 45615                                      |
| $2^{-12}$ | 124                       | $U$                                       |
| $2^{-14}$ | 193                       | $U$                                       |
| $2^{-16}$ | 691                       | $U$                                       |
| $2^{-18}$ | 146                       | $U$                                       |
| $2^{-20}$ | 700                       | $U$                                       |
| $2^{-22}$ | 88                        | $U$                                       |
| $2^{-24}$ | 1154                      | $U$                                       |
| $2^{-26}$ | 13104                     | $U$                                       |
| $2^{-28}$ | 8202                      | $U$                                       |
| $2^{-30}$ | 21670                     | $U$                                       |
| $2^{-32}$ | 129367                    | $U$                                       |

Figure 8: The Auto-correlation function of two maps. (a) Digital baker map; (b) iteration-time combined digital baker map.

Figure 9: The ApEn of the digital baker map, iteration-time combined digital baker map, and coupled baker map in [4].

Figure 10: The PE of the digital baker map and iteration-time combined digital baker map.
5.2.1. NIST Statistical Tests. The NIST statistical test includes 16 test methods. These test methods can be used to detect the randomness of arbitrary long binary sequences generated by a pseudorandom number generator. They are dedicated to determine the variety of nonrandomness that may exist in a sequence. The test results are shown in Table 3. All P values are larger than 0.01; thus, the sequence is accepted as random. This finding indicates that the pseudorandom sequence generated by our proposed method has passed the NIST statistical test. Thus, the bit sequence has a good stochastic performance.

5.3. Security Test

5.3.1. Key Space. Brute force cracking is the most common and difficult attack method. At present, when the key space is larger than $2^{128}$, the security of the password can be guaranteed. In our method, the control parameters $b_1$ and $b_2$ and the initial values of $x_0$ and $y_0$ can be used as a joint secret key. The largest precision is set to be $10^{-14}$. Given that $0 < b_1, b_2 < 1$ and $0 < x_0, y_0 < 1$, the key space is approximately $2^{190}$, which is considerably larger than the standard $2^{128}$, and thus prove that it can resist brute force cracking. Furthermore, in comparison with other methods, the proposed method is larger than $2^{184}$ in [4] and $2^{146} (9.7 \times 10^{42})$ in [27].

5.3.2. Key Sensitivity. Key sensitivity is an important indicator of evaluation. The PRBG key must be sufficiently sensitive to resist differential attacks. When the key changes slightly, the generated sequence should be different. To test key sensitivity, we change 1 bit in the key to generate a new sequence. As we know, variance is a measure of the difference between two sets of data. Therefore, the degree of difference between the two sequences can be compared by calculating the variance ratio of the two sequences. And conducted multiple experiments. The results in Table 4 show that the variance ratio in each case is close to 50%. Thus, the method shows good key sensitivity and can resist differential attacks effectively.

5.3.3. Linear Complexity. Linear complexity plays an important role as an evaluation criterion for the complexity of random sequences. The number of stages of the shortest linear feedback shift register (LFSR) that generates this sequence is the definition of the linear complexity of a binary sequence. Set $s^i = s_0, s_1, \ldots, s_{n-1}$ is a binary sequence with a period of $2^n$. Then, the linear complexity of $s^i$ is defined as the smallest positive integer $l$ satisfying formulas (4) (2), and for $\forall i \in (l, n)$ are satisfied:

$$-s_i = c_1 s_{i-1} + c_2 s_{i-2} + \cdots + c_l s_{i-l},$$

where $c_0 = 1$, and $c_i (i = 1, 2, \ldots, n) \in \mathbb{C}$.

Mathematically, the polynomial $c(x) = c_0 + c_1 x + \cdots + c_l x^l$ is called the characteristic polynomial that generates this sequence, that is, the feedback polynomial of the shortest linear feedback shifter (LFSR). Among all the feedback polynomials of the sequence $s$, the first polynomial $m_s(x)$ with the smallest degree is called the smallest polynomial of the sequence $s$. The linear complexity of the sequence $s$ is usually defined as the smallest polynomial $m_s(x)$, expressed as $\text{LC}(s)$. A detailed algorithm can be seen in [28].

The linear complexity should be $n/2$ as a qualified random sequence. Figure 12 shows that the linear complexity of the random sequence generated by our proposed method is always maintained at approximately $n/2$, which

![Figure 11: Schematic block diagram of the proposed PRBG.](image-url)

### Table 3: NIST statistical test results.

| Test index                  | $P$ values | Results |
|-----------------------------|------------|---------|
| Approximate entropy         | 0.884121   | Success |
| Block frequency             | 0.667705   | Success |
| Cumulative sums             | 0.823636   | Success |
| FFT                         | 0.295498   | Success |
| Frequency                   | 0.528695   | Success |
| Linear complexity           | 0.808946   | Success |
| Random excursions           | 0.317492   | Success |
| Random excursions variant   | 0.228489   | Success |
| Longest runs of ones        | 0.265755   | Success |
| Overlapping template of all ones | 0.623520 | Success |
| Rank                        | 0.324251   | Success |
| Runs                        | 0.720640   | Success |
| Serial                      | 0.224261   | Success |
| Universal statistical       | 0.368502   | Success |
| Lempel–Ziv compression test | 0.407865   | Success |

### Table 4: Sensitivity analysis.

| Parameter | $H$ (%) |
|-----------|---------|
| $x_0$     | 50.02   |
| $y_0$     | 49.97   |
| $b$       | 50.03   |
indicates good randomness and complexity of our proposed method.

6. Conclusions

In this study, a general method is proposed to improve the dynamic degradation phenomenon of chaotic maps on finite precision devices. In our approach, we introduce the number of iterations to replace the control parameters in the original chaotic map. We combine this number of iterations with the trigonometric function, such that the control parameter functions satisfy the range requirements of the chaotic map. Compared with the delay-introducing method in [2], the improvement effect of the iteration-time combination method in this paper is significantly improved; compared with the bi-coupling method in [4], the improved method is simpler to implement, does not need to introduce external systems, and is of high efficiency. Experimental tests on one- and two-dimensional chaotic maps demonstrate that our proposed method can greatly improve the dynamic degradation phenomenon without introducing other systems. The proposed method is simple and efficient. Finally, we propose a type of PRBG based on the iteration-time combined baker map with finite precision. Through the experiments, all indicators show that the sequences generated according to our method have good statistical properties and security features.

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 that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61862042).

References

[1] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," International Journal of Bifurcation and Chaos, vol. 15, pp. 3119–3151, 2004.
[2] 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.
[3] D. D. Wheeler and R. A. J. Matthews, "Supercomputer investigations of a chaotic encryption algorithm," Cryptologia, vol. 15, no. 2, pp. 140–152, 1991.
[4] L. Liu, B. Liu, H. Hu, and S. Miao, "Reducing the dynamical degradation by bi-coupling digital chaotic maps," International Journal of Bifurcation and Chaos, vol. 28, no. 5, p. 1850059, 2018.
[5] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, and K. To, "Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG," IEEE Transactions on Very Large Scale Integration (VLSI) Systems, vol. 20, no. 2, pp. 385–389, 2012.
[6] A. C. Dascalescu, R. Boriga, and C. Racucia, "A new pseudorandom bit generator using compounded chaotic tent maps," in Proceedings of the 2012 9th International Conference on Communications (COM), pp. 339–342, Bucharest, Romania, June 2012.
[7] Y. Zhou, Z. Hua, C. Pun, and C. L. P. Chen, "Cascade chaotic systems with applications," IEEE Trans Cybernet, vol. 45, no. 9, pp. 2001–2012, 2015.
[8] Y. Wang, K.-W. Wong, X. Liao, T. Xiang, and G. Chen, "A chaos-based image encryption algorithm with variable control parameters," Chaos, Solitons & Fractals, vol. 41, no. 4, pp. 1773–1783, 2009.
[9] 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.
[10] K. J. Persohn and R. J. Povinelli, "Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," Chaos, Solitons & Fractals, vol. 45, no. 3, pp. 238–245, 2012.
[11] S. B. Liu, J. Sun, Z. Q. Xu, and J. S. Liu, "Digital chaotic sequence generator based on coupled chaotic systems," Chinese Physics B, vol. 18, pp. 5219–5227, 2009.
[12] S. Li, X. Mou, and Y. Cai, "Improving security of a chaotic encryption approach," Physics Letters A, vol. 290, no. 3–4, pp. 127–133, 2001.
[13] T. Sang, R. Wang, and Y. Yan, "Perturbation-based algorithm to expand cycle length of chaotic key stream," Electronics Letters, vol. 34, pp. 873–874, 1998.
[14] 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.
[15] L. F. Liu, H. P. Hu, and Y. S. Deng, "An analog-digital mixed method for solving the dynamical degradation of digital chaotic systems," IMA Journal of Mathematical Control and Information, vol. 32, no. 4, pp. 703–715, 2015.
[16] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," International Journal of Bifurcation and Chaos, vol. 15, no. 10, pp. 3119–3151, 2005.
[17] S. M. Pincus, “Approximate entropy as a measure of system complexity,” Proceedings of the National Academy of Sciences, vol. 88, no. 6, pp. 2297–2301, 1991.
[18] M. François, T. Grosjes, D. Barchiesi, and R. Erra, "Pseudo-random number generator based on mixing of three chaotic maps," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 4, pp. 887–895, 2014.

[19] L. Nian-Sheng, "Pseudo-randomness and complexity of binary sequences generated by the chaotic system," *Communications in Nonlinear Science and Numerical Simulation*, vol. 16, no. 2, pp. 761–768, 2011.

[20] A. Akhshani, A. Akhavan, A. Mobarakl, S.-C. Lim, and Z. Hassan, "Pseudo random number generator based on quantum chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 1, pp. 101–111, 2014.

[21] Y. T. Chiang, H. S. Wang, and Y. N. Wang, "A chaotic-based pseudo-random bit generator for navigation applications," *Applied Mechanics and Materials*, vol. 311, pp. 99–104, 2013.

[22] A. Runkin, S. Miles, N. James, and S. Juan, "Statistical test suite for random and pseudo random number generators for cryptographic applications," NIST special publication 800-22, Gaithersburg, MA, USA, 2001.

[23] S.-J. Kim, K. Umeno, and A. Hasegawa, "Corrections of the NIST statistical test suite for randomness," Cornell University, Ithaca, NY, USA, 2004, http://arxiv.org/abs/0401040.

[24] D. Knuth, *The Art of Computer Programming: Semiempirical Algorithms*, Addison-Wesley, Boston, MA, USA, 1998.

[25] H. Gustafson, E. Dawson, L. Nielsen, and W. Caelli, "A computer package for measuring the strength of encryption algorithms," *Computers & Security*, vol. 13, no. 8, pp. 687–697, 1994.

[26] G. Marsaglia and A. Zaman, *Some Portable Very-long-period Random Number Generators*, American Institute of Physics Inc, College Park, MA, USA, 1994.

[27] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise Logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.

[28] Y. Eidelman and I. Gohberg, "Inversion formulas and linear complexity algorithm for diagonal plus semiseparable matrices," *Computers & Mathematics with Applications*, vol. 33, no. 4, pp. 69–79, 1997.