Hindawi
Mathematical Problems in Engineering
Volume 2020, Article ID 4926937, 12 pages
https://doi.org/10.1155/2020/4926937

Research Article

Reducing the Dynamical Degradation of Digital Chaotic Maps with Time-Delay Linear Feedback and Parameter Perturbation

Bocheng Liu, Hongyue Xiang, and Lingfeng Liu

School of Software, Nanchang University, Nanchang 330031, China

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

Received 25 August 2019; Revised 31 December 2019; Accepted 10 January 2020; Published 11 February 2020

Academic Editor: Eric Florentin

Digital chaotic maps are not secure enough for cryptographic applications due to their dynamical degradation. In order to improve their dynamics, in this paper, a novel method with time-delay linear feedback and parameter perturbation is proposed. The delayed state variable is used to construct the linear feedback function and parameter perturbation function. This method is universal for all different digital chaotic maps. Here, two examples are presented: one is 1D logistic map and the other is 2D Baker map. To show the effectiveness of this method, we take some numerical experiments, including trajectory and phase space analysis, correlation analysis, period analysis, and complexity analysis. All the numerical results prove that the method can greatly improve the dynamics of digital chaotic maps and is quite competitive with other proposed methods. Furthermore, a simple pseudorandom bit generator (PRBG) based on digital Baker map is proposed to show its potential application. The proposed PRBG is completely constructed by the digital chaotic map, without any other complex operations. Several numerical results indicate that this PRBG has good randomness and high complexity level.

1. Introduction

Chaos has been widely used in many different kinds of scientific fields, including physics, biology, economics, and social science. Chaotic maps have several particular characteristics, such as sensitivity to initial condition and parameter, fast attenuation of autocorrelation, time domain-long range independence, random-like, aperiodicity, and high complexity, which have already received widespread attentions. Most of these characteristics are consistent with the requirements of cryptography. Therefore, constructing cryptosystems by using chaotic maps is widely studied in these decades [1–6].

According to essential structure and used methodologies, the encryption schemes using chaotic system are roughly divided into the following five parts: randomness-oriented chaos enhancement, single round of encryption, multiple rounds of encryption, encrypting multiple images simultaneously, and compression image encryption [7]. Among them, the appearance of randomness-oriented chaos enhancement is mainly due to the realization on a device with finite precision (such as computer); these particular properties of chaotic maps will not hold anymore. Since the precision is finite, the phase space of the chaotic map will be limited to a finite state space, and its trajectory will finally fall into a cycle inevitably. Accordingly, other properties will degrade as well. We call it dynamical degradation of chaotic maps [8, 9]. The chaotic map which is realized on finite precision device is called digital chaotic map.

Obviously, digital chaotic maps are not secure to construct cryptosystems anymore. Therefore, in order to reduce the dynamical degradation of digital chaotic maps, many different kinds of method are proposed. Overall, these methods can be divided into following six categories: (1) Enlarging the precision [10]: this method can expand the phase space of digital chaotic maps and, thus, extend the average period of chaotic trajectories. (2) Cascading multiple chaotic maps [2, 11]: this method can extend the period of chaotic trajectories, while its properties depend on the cascaded chaotic maps completely. (3) Switching multiple chaotic maps [12, 13]: the effectiveness of this method depends on the switching strategy. (4) Perturbing the chaotic

maps [14–18]: generally, this method is proved to be better than the first three methods [19]. This method can improve the dynamics of digital chaotic map by introducing an external perturbation source. However, the introducing of external perturbation source will certainly increase its cost. (5) Error compensation method [20]: this method tries to compensate the state of digital chaotic map to the original chaotic map. However, the parameter space of this method is always small, and the compensated digital chaotic map cannot be driven to display desirable properties [21]. (6) Feedback control method [22]: this method uses a state function to control the state variable of digital chaotic maps. However, this method cannot improve the properties of digital chaotic maps significantly without other auxiliary methods.

Motivated by the summary above, in this paper, we proposed a novel effective method to reduce the dynamical degradation of digital chaotic maps. This method is composed of linear feedback control and parameter perturbation. The state variable of the digital chaotic map is used to construct a feedback function and a parameter perturbation function to control the next state and the system parameter, respectively. In order to increase the uncertainty of digital chaotic map, the time-delay state variable is used in these two control functions. In this paper, two examples are presented to show the effectiveness of our method, including 1D logistic map and 2D Baker map. Numerical experiments show that this method can greatly improve the performances of digital chaotic maps, which means that the dynamical degradation of digital chaotic maps can be reduced effectively. Moreover, the performance of this improved digital chaotic map is better than other proposed remedies, which implies that this method is quite competitive. Overall, the significant advantages of this method can be described as follows:

(1) This method is more effective than other proposed methods in improving the chaotic complexity of digital chaotic maps.

(2) This method is universal for all different digital chaotic maps, including 1D maps and high-dimensional maps.

(3) The external source is not necessary here, which implies that this method is much easier to implement than some other remedies [15, 16, 18].

Our method has more potential in cryptographic applications. To prove this viewpoint, in this paper, we also propose a simple PRBG based on the improved digital chaotic map. The proposed PRBG is constructed directly based on the improved digital Baker map, without any other complex operations. Some numerical simulations show that the generated bit sequence has good randomness and high security level.

The rest of this paper is organized as follows. In Section 2, the digital chaotic model with time-delay linear feedback and parameter perturbation is proposed. The improved 1D logistic map and 2D Baker map with several numerical experiments are presented in Sections 3 and 4, respectively. In Section 5, a simple PRBG based on improved digital Baker map is presented, as well as some randomness and security analysis. Finally, Section 6 concludes the whole paper.

2. Digital Chaotic Model with Time-Delay Linear Feedback and Parameter Perturbation

A general chaotic map can be described as

$$x_{i+1} = f(p, x_i), \tag{1}$$

where $x_i \in X$ is the state variable and p is the control parameter. According to equation (1), we have that the state x_{i+1} is completely determined by the current state x_i. Once an initial value x_0 is given, a corresponding sequence $\{x_i\}$ can be generated. The map f will be chaotic when the parameter p is in the suitable domain A. Theoretically, the chaotic sequence $\{x_i\}$ is aperiodic and random-like and has a high complexity. Based on these good characteristics, chaotic maps are widely used in some security fields, including cryptography.

However, when the chaotic map is realized on computer, it will be limited by the finite precision. The general digital chaotic map realized on computer can be written as

$$x_{i+1} = \mathrm{FL}(f(p, x_i)), \tag{2}$$

where FL denotes the precision function. Limited by function FL, the state space X will be finite. It indicates that the case $x_k = x_l$ is inevitable along with the iteration of equation (2), where k and l are the iterative steps. As the state x_{i+1} is completely determined by x_i, spontaneously, we will have $x_{k+1} = x_{l+1}$, $x_{k+2} = x_{l+2}$, ... Therefore, the sequence becomes periodic with a period $l - k$ (we assume $l > k$). Furthermore, the randomness and complexity will also degrade, which makes the chaotic map not secure anymore.

To solve this problem, in this paper, we propose a novel method to reduce the dynamical degradation of digital chaotic maps, whose mathematical model can be described as

$$x_{i+1} = FL(f(h(x_{i-1}, x_{i-2}, \ldots, x_{i-s}), x_i) + g(x_{i-1}, x_{i-2}, \ldots, x_{i-t})), \tag{3}$$

where h denotes the parameter perturbation function (PPF) and g denotes the linear feedback function (LFF). Both h and g are the functions of delayed states. s and t denote the cardinal numbers of delayed states of PPF and LFF. This model can reduce the dynamical degradation of digital chaotic maps effectively due to the following advantages:

(1) With the introduction of PPF, the control parameter is varying along with the iteration. This means that the parameters are always different at each iteration. Therefore, the generated sequence will become nonstationary. Obviously, the nonstationary chaotic sequence is much more difficult to predict and analyze and is more complex than the stationary sequence [23].

(2) In mode (3), a LFF is introduced. The function can be regarded as a perturbation of state variable. With the perturbation of state variable, the chaotic trajectory will not only be generated by the function f. The function g can disrupt the state space of chaotic map f, which makes the model much more complex.

(3) Both PPF and LFF are the functions of delayed states. With the introduction of delayed states, the state x_{i+1} will be determined not only by x_i but also by some

delayed states. It is evidently effective in expanding the period. Generally, even if $x_k = x_l$, the equation $x_{k+1} = x_{l+1}$ will not hold since their delayed states $x_{k-1}, x_{l-1}, x_{k-2}, x_{l-2}, \ldots$ may be different. Therefore, the trajectory will not fall into a cycle once $x_k = x_l$, unless their delayed states of PPF and LFF are all the same. It is a definite improvement of equation (2).

In practical use, the most pivotal issue for this method is the construction of PPF and LFF. It should be noted that although the construction of PPF and LFF is not unique, some necessary conditions should be satisfied to make the model valid.

(1) The PPF is used to vary the control parameter of chaotic map. The range of the PPF should be a subset of chaotic parameter domain A. Otherwise, the map f will not be chaotic. PPF is a function of delayed variable $x_{i-1}, x_{i-2}, \ldots, x_{i-s}$. Given that the basic idea is the same, in this paper, we make the PPF only relate to the delayed variable x_{i-1}; thus, it can be written as $h(x_{i-1})$.

(2) The LFF is used to perturb the state variable of chaotic map. All the chaotic maps are bounded; therefore, the function value of $f + g$ should also be located in the state space X. In this paper, we use modular operation to ensure this condition can be satisfied. The same as PPF, we only consider the case $g(x_{i-1}, x_{i-2}, \ldots, x_{i-t}) = g(x_{i-2})$ for convenience, which indicates that the LLF is only related to one delayed variable x_{i-2}.

Remark 1. Compared with some other remedies [15, 16, 18], our proposed digital chaotic model does not require any external systems, which is much easier to implement. Furthermore, the effect of our method is no worse than these complex models, but even better. Some comparisons will be shown in the numerical experiments to prove this viewpoint.

Remark 2. From equation (3), we can find that this model has no restrictions on chaotic maps. It indicates that our remedy is universal to all chaotic maps. In the next two sections, 1D logistic map and 2D Baker map are used to show the effectiveness of our method.

Remark 3. In [22, 24], the time-delayed variables are also used. In [22], the delayed variable is used to control the state, and in [24], the delayed variable is used to control the parameters. The delayed variable used in these two remedies can improve the digital chaotic maps to a certain extent, but their effects are not as well as ours. We will compare our method with these two remedies in the following sections.

3. Improved Digital Logistic Map

The basic model of logistic map realized on finite device can be described as

$$x_{i+1} = FL(f(a, x_i)) = FL(ax_i(1 - x_i)), \tag{4}$$

where $x \in (0, 1)$ is the state variable and a is the control parameter. If $a \in (3.5699, 4]$, map f will be chaotic. Under the influence of precision function FL, dynamical degradation is inevitable. Based on the proposed method above, we use the following PPF and LFF to improve its dynamics:

$$h(x_{i-1}) = b + (4 - b)x_{i-1}^2, \tag{5}$$

$$g(x_{i-2}) = cx_{i-2}, \tag{6}$$

where parameter $b \in [3.6, 4)$ and c is linear feedback coefficient. In order to make the variable state x bounded, we add a modulator operation in our model. The improved digital logistic map can be written as

$$x_{i+1} = FL\left(\left(b + (4 - b)x_{i-1}^2\right)x_i(1 - x_i) + cx_{i-2}\right) \mod 1. \tag{7}$$

Next, some characteristics are analyzed to highlight the effectiveness of this method.

We set $a = b = 3.99$, $x_0 = 0.2145$, $x_1 = 0.2458$, and $x_2 = 0.365$ in the following numerical experiments unless otherwise specified. The largest precision is set at 2^{-12}. The linear feedback coefficient c will affect the complexity of equation (7). Here, we use perturbation entropy (PE) to help us to select the most appropriate c. PE is a natural complexity measure proposed by Bandt and Pompe [25], which measures the uncertainty of different orderings. Figure 1 depicts the PE value of sequences generated by equation (7) with different c. From Figure 1, we can find that the PE will firstly increase with c, and then approach to be stable since $c = 2$. Therefore, we always choose $c = 2$ in equation (7).

Next, we use some characteristics to highlight the effectiveness of this method, including trajectory, phase space, autocorrelation function, period, complexity, and state-mapping network [26].

3.1. Trajectory and Phase Space. The trajectories of equations (4) and (7) are depicted in Figures 2(a) and 2(b), respectively. From Figure 2(a), we can find that, after about 20 iterations, the trajectory will fall into a cycle with a short period, which indicates that the dynamics has been degenerated, while Figure 2(b) shows that the trajectory of equation (7) will still keep random-like after 1000 iterations with no period, which indicates that the period has been extended. Figures 3(a) and 3(b) show the phase space of equations (4) and (7), respectively. As Figure 3(a) shows, the phase space of equation (4) presents a parabolic shape, with an obvious structural feature, while the space phase of equation (7) is randomly distributed in the whole space. The space phase of equation (7) has no obvious structural feature, which makes the improved digital logistic map more complex.

3.2. Autocorrelation Function. Autocorrelation function is always used as a randomness measure. The autocorrelation should be delta function for an ideal random sequence.

Figures 4(a) and 4(b) depict the autocorrelation functions of sequences generated by equations (4) and (7), respectively. From Figure 4(b), we can see that the autocorrelation function of the sequence generated by equation (7) is decreased rapidly with the interval increases, which indicates that the sequence generated by equation (7) can be considered as a good random sequence, while the sequence generated by equation (4) is not.

3.3. Period Analysis. Periodicity is the most important measure to evaluate the effectiveness of a remedy of digital chaotic maps. Here, we vary the computer precision from 2^{-4} to 2^{-15}. The period analysis of the sequences generated by equations (4) and (7) is shown in Table 1. In this test, the length of the sequences is 10^6. All period results are calculated by averaging the periods of 10 sequences which are generated by 10 different initial conditions. From Table 1, we can find that the period of the sequences generated by equation (7) is always larger than that of equation (4), which proves that our method can greatly extend the period of original digital chaotic map. Furthermore, since the largest precision is larger than 2^{-10}, the period cannot be detected anymore. Compared to other remedies, our results are very competitive. In [22, 24], the period can still be detected when the largest precision is 2^{-12}, which is worse than our results.

3.4. Complexity Analysis. In this experiment, we use approximate entropy (ApEn) and PE to measure the complexity of the generated sequences by equations (4) and (7). ApEn measures the probability of new patterns generated in sequences with embedding dimension growth [27]. Set $a = b = 3.95$. The results of ApEn are shown in Figure 5. From Figure 5, we can see that the ApEn of the sequence generated by equation (7) is much larger than the ApEn of the sequence generated by equation (4) under the same precision, which implies that our method can greatly improve the complexity of original digital logistic map. Compared with the results in [22, 24], our method is also much better in enhancing the complexity of chaotic map; see Figure 5 as well. The PE analysis is shown in Figure 6. From Figure 6, we can obtain several similar results as ApEn analysis. The PE of the sequence generated by equation (7) is much larger than the PE of the sequence generated by equation (4) and Refs. [22] and [24] under the same precision, which also indicates that our method is more effective in improving the complexity of digital chaotic map.

3.5. State-Mapping Network [26]. For the state-mapping network, perturbing the state is to jump from a walk path in an SMN to another one, and the control parameters are to walk from a path of an SMN corresponding to one control parameter to that corresponding to another one with a timely jump, essentially. Hence, perturbing the state and the control parameters can indeed improve the randomness of chaotic maps. Figure 7 shows the state-mapping networks of the sequence generated by the original logistic mapping and the improved one, respectively. The largest precision is set at 2^{-5}. From the figure, we can conclude that the average length of the orbit of the SMN of improved map is larger than that of the original map, which indicates the effectiveness of our method.

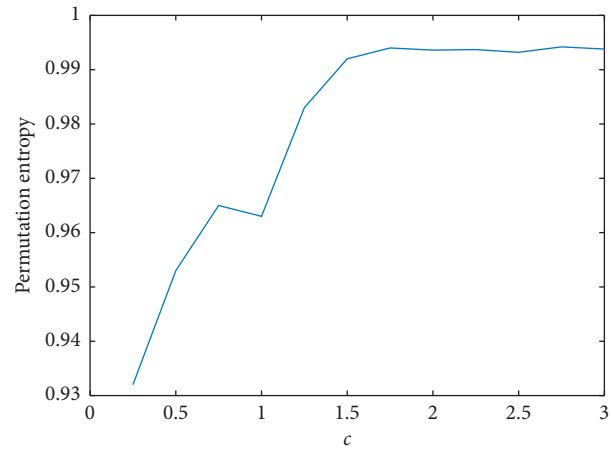

Figure 1: PE of sequences generated by equation (7) with different c.

4. Improved Digital Baker Map

Besides 1D logistic map, in this section, we use the following 2D digital Baker map as an example to show the effectiveness of our method as well,

$$(x_{i+1}, y_{i+1}) = \begin{cases} \mathrm{FL}\left(\dfrac{x_i}{a}, a y_i\right), & 0 < x \le a, \\ \mathrm{FL}\left(\dfrac{(x_i - a)}{(1-a)}, (1-a) y_i + a\right), & a < x \le 1, \end{cases} \tag{8}$$

where $a \in (0, 1)$ is the chaotic control parameter. The PPF is selected as

$$h(x_{i-1}, y_{i-1}) = b x_{i-1} + b y_{i-1} + 1 - 2b, \tag{9}$$

where b is the parameter in the interval (0, 0.5) to satisfy the necessary condition. The LFF is selected as the same as equation (6). With a modulator operation, the improved digital Baker map can be described as

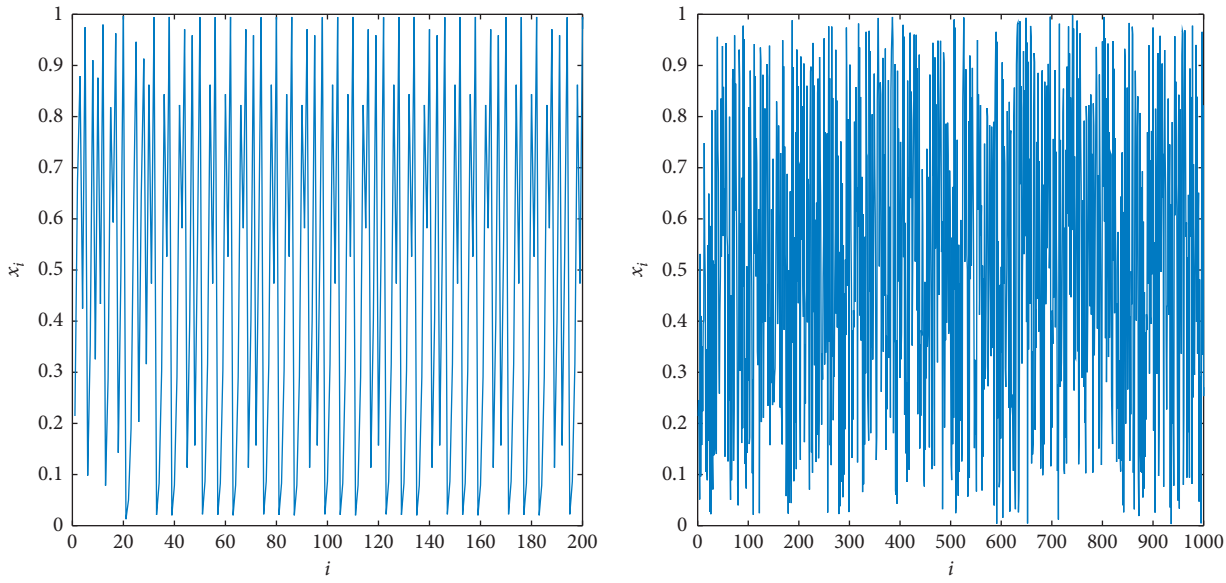

Figure 2: The trajectories of (a) equation (4) and (b) equation (7).

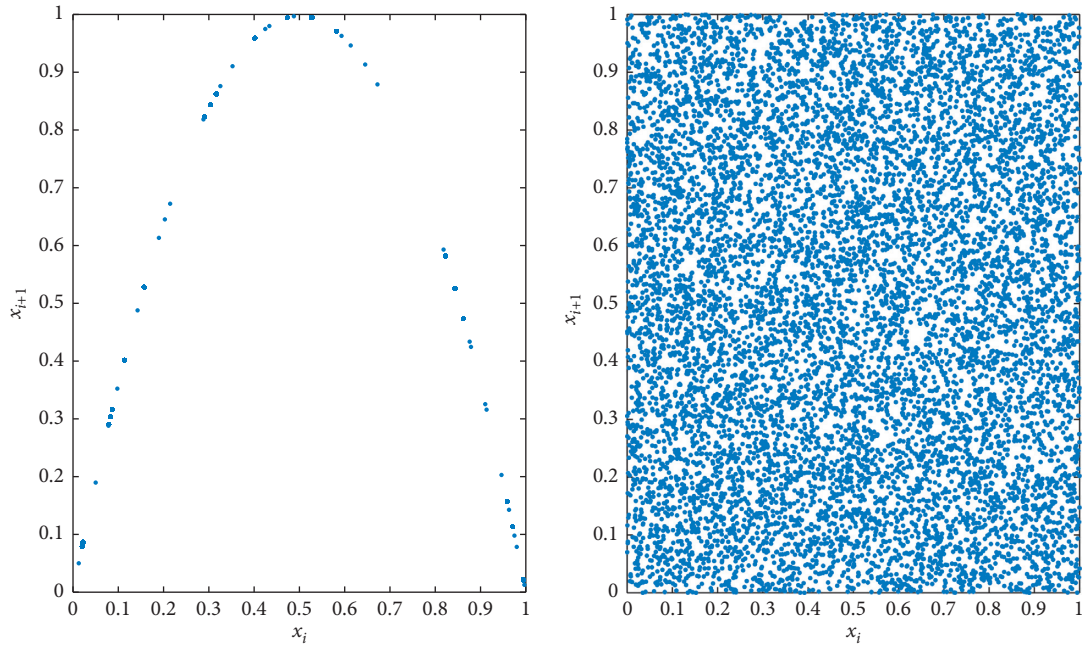

Figure 3: The phase space of (a) equation (4) and (b) equation (7).

$$(x_{i+1}, y_{i+1}) = \mathrm{FL}\begin{cases} \left(\dfrac{x_i}{bx_{i-1} + by_{i-1} + 1 - 2b} + cx_{i-2} \bmod 1, \left(bx_{i-1} + by_{i-1} + 1 - 2b\right)y_i\right), & 0 < x \le a, \\ \left(\dfrac{x_i - bx_{i-1} - by_{i-1} - 1 + 2b}{2b - bx_{i-1} - by_{i-1}}, \left(2b - bx_{i-1} - by_{i-1}\right)y_i + bx_{i-1} + by_{i-1} + 1 - 2b\right), & a < x \le 1. \end{cases} \tag{10}$$

In order to select a suitable linear feedback coefficient c, PE is also used here as a guideline. The PE value of sequences generated by equation (10) with different c is depicted in Figure 8. As Figure 8 shows, since $c = 2.5$, the PE

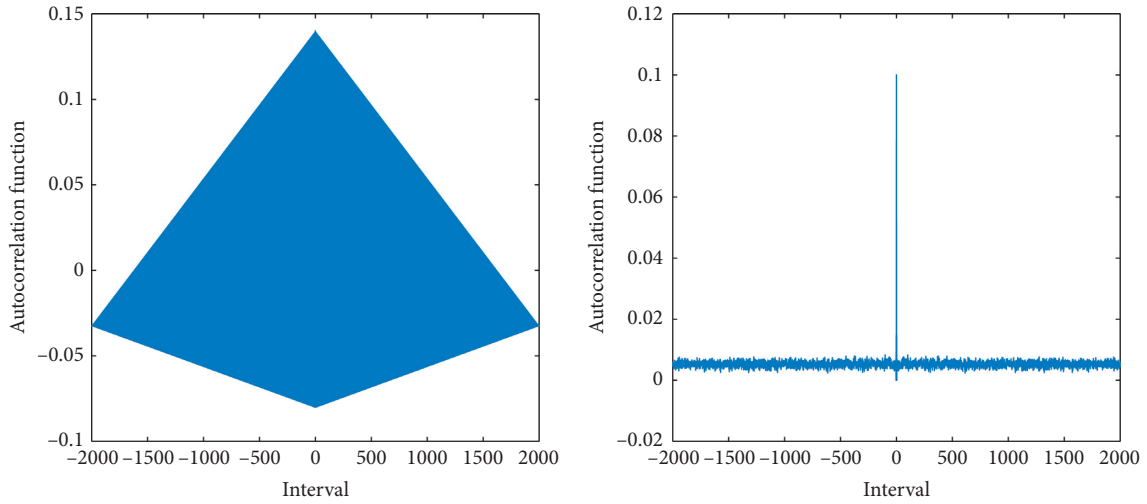

Figure 4: The autocorrelation functions of (a) equation (4) and (b) equation (7).

Table 1: Period analysis of equations (4) and (7).

Precision	Equation (4)	Equation (7)	Precision	Equation (4)	Equation (7)
2^{-4}	2	3	2^{-10}	37	Undetected
2^{-5}	5	34	2^{-11}	21	Undetected
2^{-6}	4	190	2^{-12}	83	Undetected
2^{-7}	5	1682	2^{-13}	7	Undetected
2^{-8}	16	1511	2^{-14}	131	Undetected
2^{-9}	8	8569	2^{-15}	259	Undetected

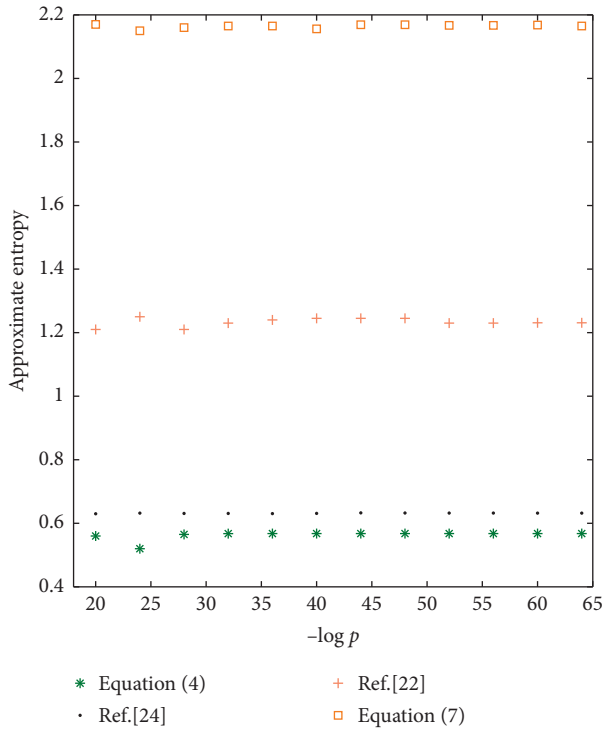

Figure 5: The ApEn analysis of sequences generated by equations (4) and (7) and Refs. [22] and [24].

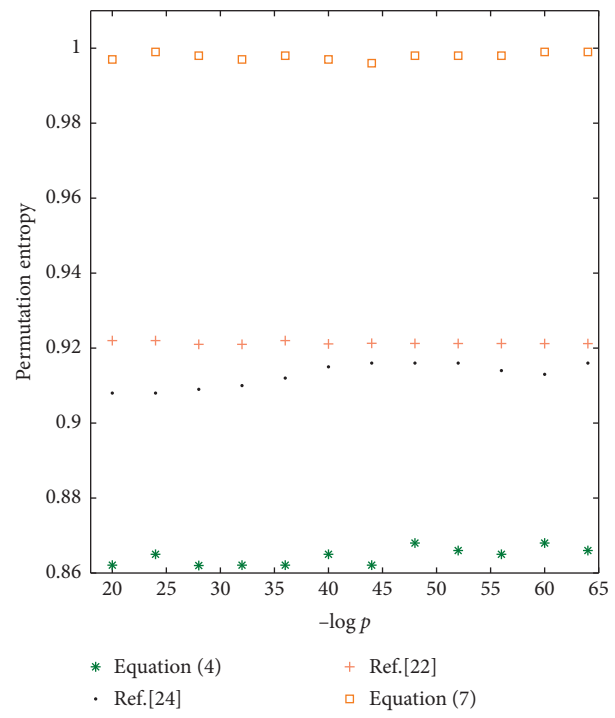

Figure 6: The PE analysis of sequences generated by equations (4) and (7) and Refs. [22] and [24].

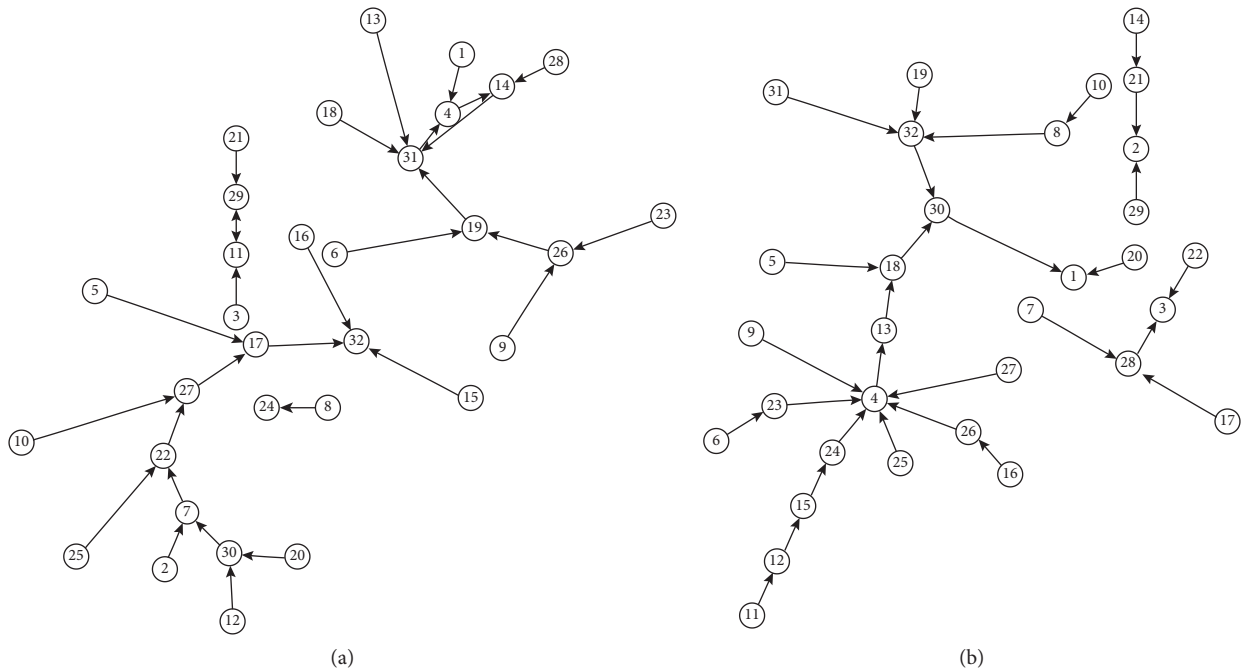

Figure 7: The state-mapping networks analysis of sequences generated by equations (4) and (7).

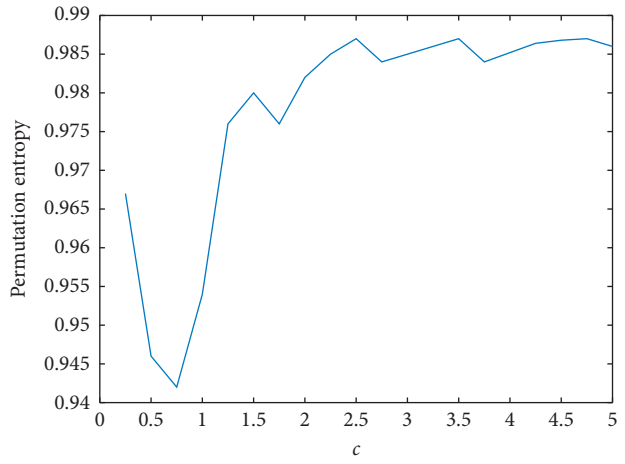

Figure 8: PE of sequences generated by equation (10) with different c.

will reach its maximum value and becomes stable approximately. Therefore, in this section, we always choose $c = 2.5$ in equation (10).

To prove the effectiveness of our method, we also use trajectory, phase space, autocorrelation function, period, and complexity measure to evaluate the dynamics of equation (10). In all these numerical experiments, we set $a = b = 0.49$, $x_0 = 0.214$, $x_1 = 0.547$, $x_2 = 0.651$, $y_0 = 0.654$, $y_1 = 0.782$, and $y_2 = 0.982$ unless otherwise specified. The largest precision is set at 2^{-12}. All the experiment methods are similar to the experiments in Section 3. Without loss of generality, we only use the x-dimensional state variable in some experiments to avoid redundancy.

4.1. Trajectory and Phase Space. The trajectories of equations (8) and (10) are depicted in Figures 9(a) and 9(b), respectively. As Figure 9(a) shows, the trajectory of equation (8) will quickly fall into a cycle after less than 60 iterations, while Figure 8(b) implies that the trajectory of equation (10) is disordered which can be regarded as a random sequence. Figure 10 shows the phase space of equations (8) and (10). By comparison, the phase space of equation (8) is much sparser than the phase space of equation (10). This is because the period of (8) is very short, and the variable is repeated without creating new states, while the state variable of equation (10) has no period and can create more different states.

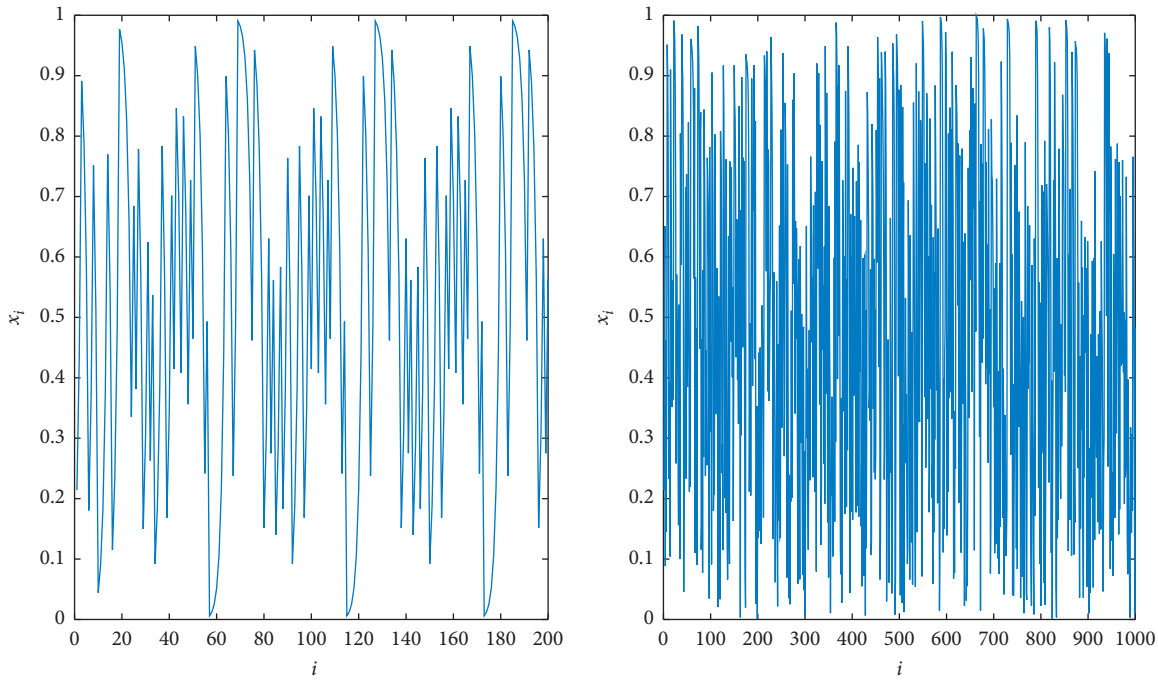

Figure 9: The trajectories of (a) equation (8) and (b) equation (10).

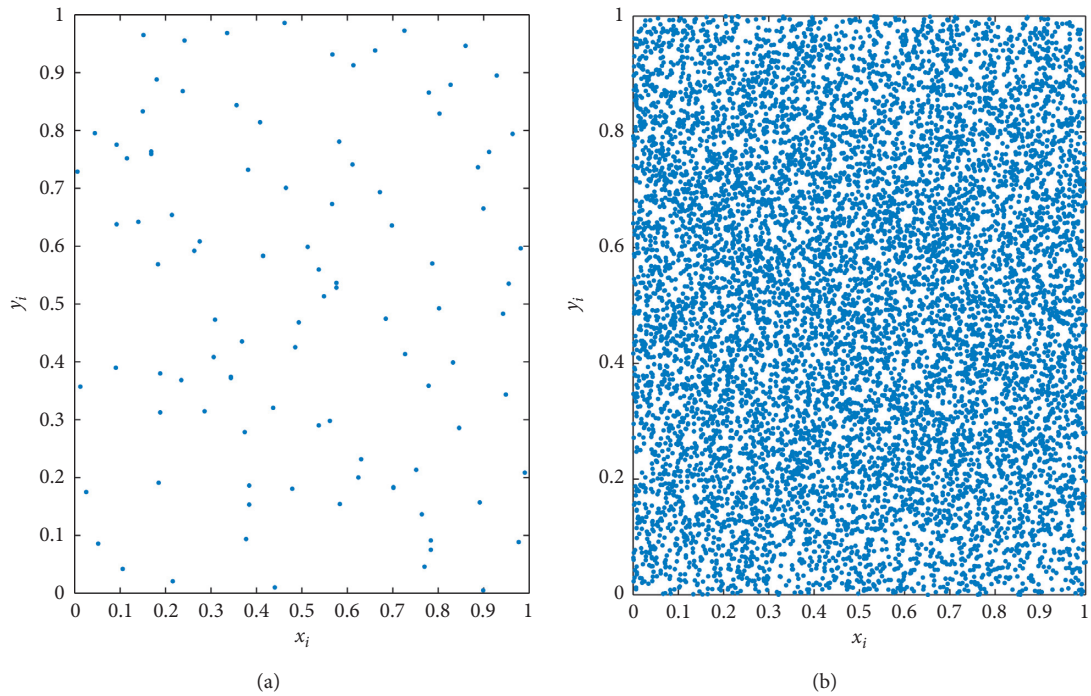

Figure 10: The phase space of (a) equation (8) and (b) equation (10).

4.2. Auto-Correlation Function. The autocorrelation functions of equations (8) and (10) are shown in Figure 11. From Figure 11, we can have that the autocorrelation function of equation (10) is delta-like, which can be regarded as good randomness, but not the autocorrelation function of equation (8).

4.3. Period Analysis. Varying the computer precision from 2^{-4} to 2^{-15}, the periods of the sequences generated by equations (8) and (10) are detected and shown in Table 2. As we can see from Table 2, the period can be extended greatly under the same precision. Since the largest precision is larger than 2^{-12}, the period cannot be detected any more. In [24],

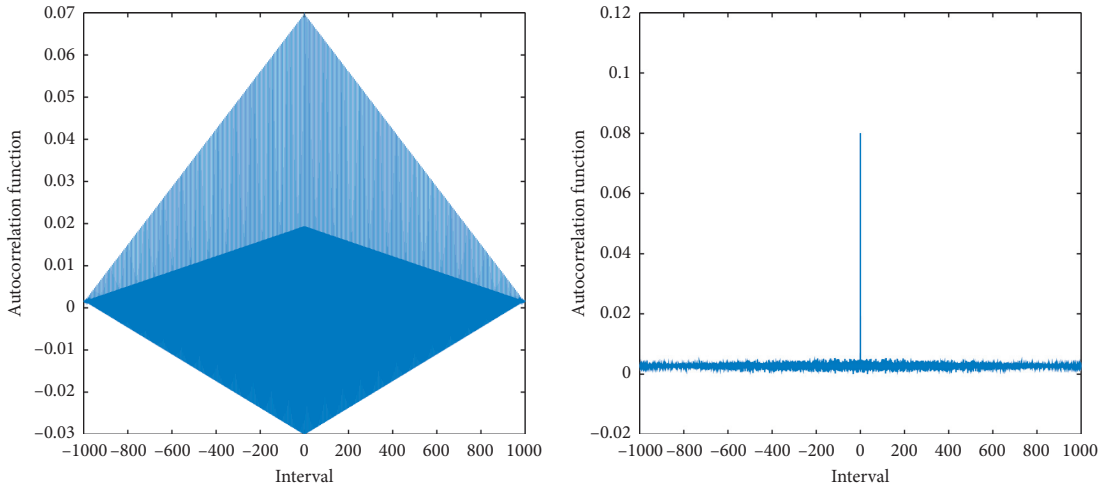

Figure 11: The autocorrelation functions of (a) equation (8) and (b) equation (10).

Table 2: Period analysis of equations (8) and (10).

Precision	Equation (8)	Equation (10)	Precision	Equation (8)	Equation (10)
2^{-4}	1	19	2^{-10}	34	10920
2^{-5}	1	91	2^{-11}	21	6346
2^{-6}	3	245	2^{-12}	42	Undetected
2^{-7}	5	308	2^{-13}	128	Undetected
2^{-8}	19	973	2^{-14}	193	Undetected
2^{-9}	5	3127	2^{-15}	306	Undetected

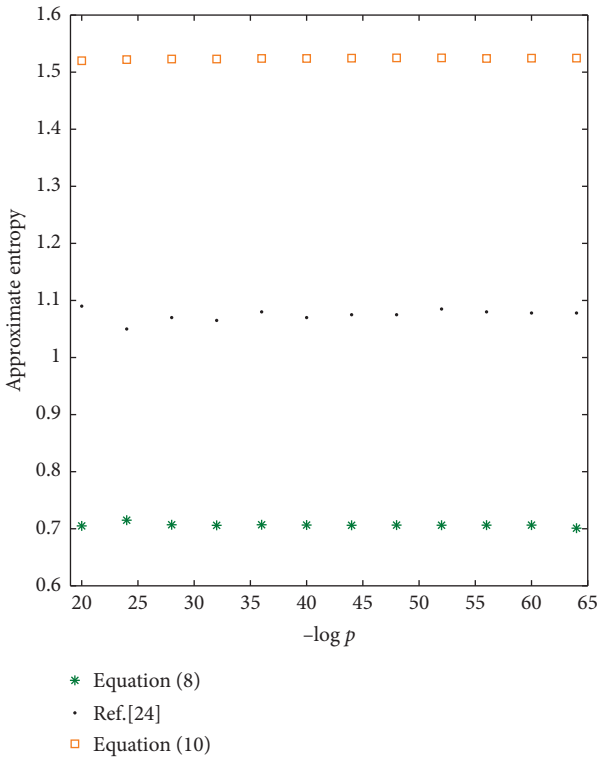

Figure 12: The ApEn analysis of sequences generated by equations (8) and (10), and Ref. [24].

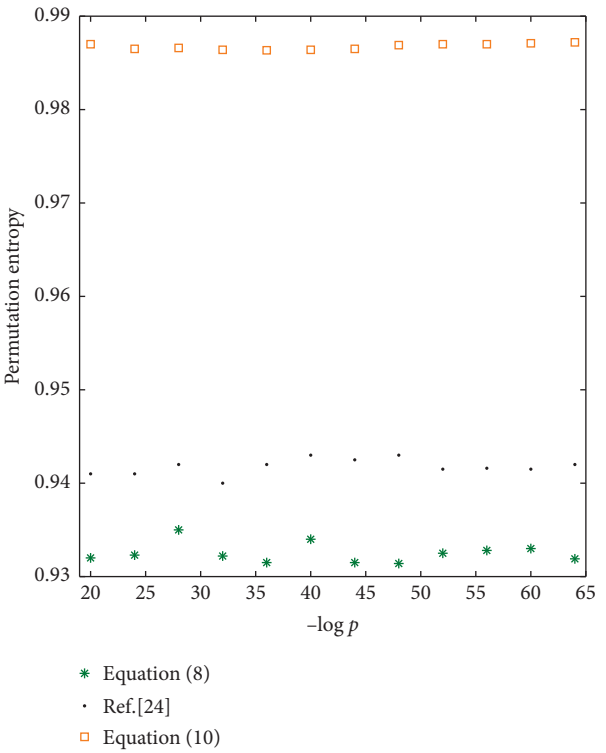

Figure 13: The PE analysis of sequences generated by equations (8) and (10), and Ref. [24].

the period cannot be detected since the precision is larger than 2^{-16}. Therefore, our method can significantly extend the period of the original digital Baker map and is competitive with other proposed methods.

4.4. Complexity Analysis. The ApEn and PE of the sequences generated by equations (8) and (10) and Ref. [24] are plotted in Figures 12 and 13, respectively. These two figures show that the complexity of the improved system equation (10) is much larger than the complexity of original digital Baker map under the same precision and is also larger than the complexity of the proposed system in [24], which concludes that our method can greatly improve the complexity of digital chaotic maps.

5. A Novel PRBG Based on Improved Logistic Map

In order to show the practical usage of our method, in this section, we design a simple PRBG based on the improved digital Baker map as an example. This example proves that the method proposed in this paper can be used in many different scientific fields, especially cryptography.

The basic scheme of the simple PRBG is shown in Figure 14, and its mathematical model can be described as

$$\begin{aligned} a_i &= 10^5 \cdot x_i \bmod 256, \\ b_i &= 10^5 \cdot y_i \bmod 256, \\ z_i &= a_i \oplus b_i. \end{aligned} \tag{11}$$

Here, x_i and y_i are the state variables of (10). $\{z_i\}$ is the generated pseudorandom bit sequence. From this model, we can see that the bit sequence is completely determined by (10); no other complex operations are added here. Thus, the randomness of $\{z_i\}$ totally depends on the characteristics of the improved Baker map. Next, we will do some numerical experiments to show that the generated bit sequence has a good randomness and high security level which can be used in cryptography.

5.1. Randomness Analysis. Currently, several statistical tests have been provided to measure the randomness of bit sequences, including Beker and Piper's statistical test [28], FIPS140-1 statistical test [29], Crypt-XS statistical test suite [30], and NIST statistical test [31]. Among all these test suites, the NIST statistical test suite may be the most popular randomness test which has been regarded as an industrial random number standard. The NIST test suite is a statistical package comprising 16 tests that are developed to test the randomness of binary sequences produced by either hardware or software based cryptographic random or PRBGs. These tests focus on a variety of different types of non-randomness that could exist in a binary sequence. In the NIST statistical tests, the significance level is set at 0.01. A bit string is said to pass the test if and only if P value ≥ 0.01. Once the P value of all tests is larger than 0.01, the sequence can be regarded as random. In this test, 500 sequences are generated by using different initial conditions, which are selected randomly. Table 3 shows the NIST test results are all larger than 0.01. Hence, we can conclude that the generated bit sequences have passed all the statistical tests, which implies good randomness.

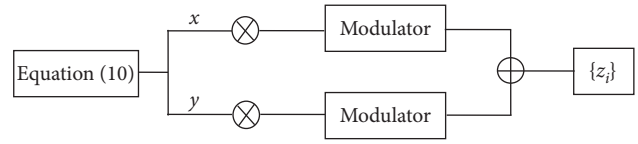

Figure 14: The basic scheme of the proposed PRBG based on equation (10).

Table 3: Results of NIST tests.

Test index	Passing ratio	Mean value of P values
Approximate entropy	0.996	0.406268
Block frequency	0.996	0.198724
Cumulative sums	0.994	0.356497
FFT	0.997	0.491376
Frequency	0.999	0.209782
Linear complexity	0.998	0.406798
Random excursions	0.996	0.204886
Random excursions variant	0.999	0.375429
Longest runs of ones	0.995	0.203973
Overlapping template of all ones	0.997	0.487922
Rank	0.997	0.379849
Runs	0.998	0.421798
Serial	0.998	0.379845
Universal statistical	0.999	0.264978
Lempel-Ziv compression test	0.996	0.239871

5.2. Key Space Analysis. The key space of a PRBG should be larger than 2^{128} to be secure for cryptographic use. Set the largest precision to be 10^{-r}. In this PRBG, the initial values $x_0, x_1, x_2, y_0, y_1 \in (0, 1)$ and the parameter $b \in (0, 0.5)$ can be selected as the secret keys. Therefore, the key space of this PRBG equals 0.5×10^{6r} approximately. Assume $r = 14$; the key space is approximately equal to $0.5 \times 10^{84} \approx 2^{278}$, which is much larger than 2^{128}. This result indicates that the key space of our PRBG is large enough to resist all kinds of brute-force attacks, which can satisfy the cryptographic requirement. Furthermore, the key space of this PRBG is also larger than the key space of the recently proposed PRBGs in [15, 32], which are 2^{184} and 2^{199}, respectively. Therefore, our PRBG is competitive with other proposed chaotic PRBGs in this sense.

5.3. Key Sensitivity Analysis. To resist differential attack (chosen-plaintext attack), the output sequence should be sensitive enough to the secret keys. In this test, we change the secret keys of the PRBG slightly by only 10^{-14} to generate two different bit sequences. Then, compare these two-bit sequences bit by bit. The length of the sequences is 10^6 bits. The variance ratio is denoted by V; the results are shown in Table 4. As Table 4 shows, the variance ratios are all close to 50% for the secret keys, which implies that the PRBG is

Table 4: Results of key sensitivity analysis.

Secret key	Variance ratio H (%)
x_0	49.97
x_1	50.04
x_2	50.07
y_0	49.98
y_1	49.98
b	50.02

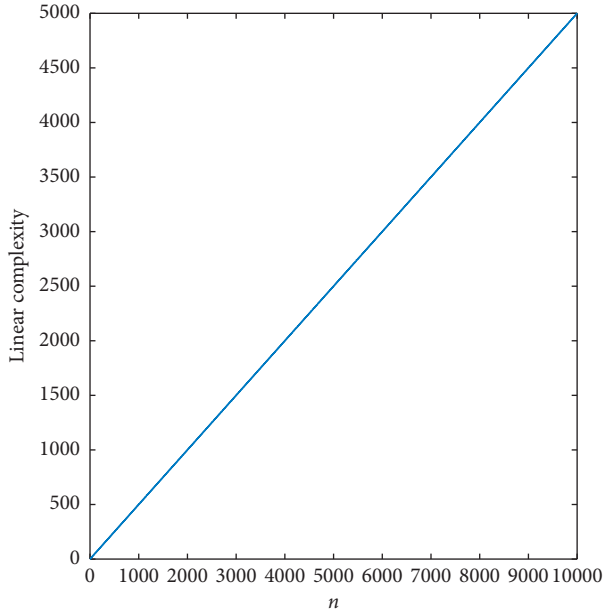

Figure 15: The linear complexity analysis.

extremely sensitive to the secret keys, which can resist the differential attack effectively.

5.4. Linear Complexity Analysis. Linear complexity is one of the most important complexity measures of bit sequence, which measures the order of the shortest linear feedback shift register which can generate this sequence. For an ideal random sequence, the linear complexity should be half of the sequence length. In this test, the linear complexity is calculated by using the algorithm in [33]. Figure 15 depicts the linear complexity of the generated bit sequence. From Figure 15, we can see that the linear complexity curve is extremely close to the ideal $n/2$ line (n is the length of the bit sequence), which concludes that the generated bit sequence has a high linear complexity level.

6. Conclusion

When the encryption algorithm based on chaotic map is implemented on the equipment with finite precision, due to truncation error and rounding error, the chaotic map will degenerate dynamically and enter a period finally, which leads to the insecurity of the encryption algorithm. However, applications based on chaotic maps only need to use a finite number of states variables. Therefore, it is necessary to improve the dynamic degradation of digital chaotic mapping to prolong its period. In this paper, we use parameter perturbation and time-delay linear feedback to suppress the dynamic degradation of digital chaotic mapping to improve the security of encryption algorithm. The numerical results of two examples, including 1D logistic map and 2D Baker map, show that our method can significantly improve the dynamic characteristics of digital chaotic mapping and is competitive with other methods. The introduction of parameter perturbation, linear feedback, and time-delay variables provides a new research direction for how to suppress the dynamic degradation of digital chaotic maps. In order to prove that the improved map can be applied to the encryption algorithm, we designed a simple PRBG and analyzed its performance, concluding that the improved chaotic mapping can greatly improve the security of the image encryption algorithm, which is of great significance to suppress the degradation of digital chaotic mapping and improve the security of the image encryption algorithm.

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 competing financial interests.

Authors' Contributions

Bocheng Liu wrote the main manuscript text, Lingfeng Liu proposed this new idea and made the data analysis, and Hongyue Xiang did the numerical experiments and revised this paper.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (61862042 and 61601215).

References

[1] X. Tang, G. Chen, and T. Lu, "Some iterative properties of (F_1, F_2)—chaos in non-autonomous discrete systems," *Entropy*, vol. 20, no. 3, p. 188, 2018.

[2] Z. Hua, B. Zhou, and Y. Zhou, "Sine-transform-based chaotic system with FPGA implementation," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 3, pp. 2557–2566, 2018.

[3] Q. Yin and C. Wang, "A new chaotic image encryption scheme using breadth-first search and dynamic diffusion," *International Journal of Bifurcation and Chaos*, vol. 28, no. 4, p. 1850047, 2018.

[4] S. J. Sheela, K. V. Suresh, and D. Tandur, "Image encryption based on modified Henon map using hybrid chaotic shift transform," *Multimedia Tools and Applications*, vol. 77, no. 19, pp. 25223–25251, 2018.

[5] Z. Shao, Y. Shang, X. Fu, H. Yuan, and H. Shu, "Double-image cryptosystem using chaotic map and mixture amplitude-phase retrieval in gyrator domain," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 1285–1298, 2018.

[6] X. Lv, X. Liao, and B. Yang, "A novel scheme for simultaneous image compression and encryption based on wavelet packet transform and multi-chaotic systems," *Multimedia Tools and Applications*, vol. 77, no. 21, pp. 28633–28663, 2018.

[7] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: a year in review," *Journal of Information Security and Applications*, vol. 48, p. 102361, 2019.

[8] F. Chemashkin and A. Moiseev, "Analysis of dynamical properties of digital chaotic systems approximated in finite precision computers," in *Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 1162–1164, Moscow, Russia, January 2019.

[9] J. Zheng, H. Hu, and X. Xia, "Applications of symbolic dynamics in counteracting the dynamical degradation of digital chaos," *Nonlinear Dynamics*, vol. 94, no. 2, pp. 1535–1546, 2018.

[10] A. Flores-Vergara, E. Inzunza-González, E. García-Guerrero et al., "Implementing a chaotic cryptosystem by performing parallel computing on embedded systems with multiprocessors," *Entropy*, vol. 21, no. 3, p. 268, 2019.

[11] M. Alawida, A. Samsudin, and J. S. Teh, "Enhancing unimodal digital chaotic maps through hybridisation," *Nonlinear Dynamics*, vol. 96, no. 1, pp. 601–613, 2019.

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

[13] A. Maximiliano, D. M. Luciana, L. Hilda et al., "Complexity of simple, switched and skipped chaotic maps in finite precision," *Entropy*, vol. 20, no. 2, p. 135, 2018.

[14] L. Liu, J. Lin, S. Miao, and B. Liu, "A double perturbation method for reducing dynamical degradation of the digital Baker map," *International Journal of Bifurcation and Chaos*, vol. 27, no. 7, p. 1750103, 2017.

[15] 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.

[16] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ramírez, "A novel pseudorandom number generator based on pseudorandomly enhanced logistic map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 407–425, 2017.

[17] L. C. Cao, Y. L. Luo, S. H. Qiu, and J. X. Liu, "A perturbation method to the tent map based on Lyapunov exponent and its application," *Chinese Physics B*, vol. 24, no. 10, pp. 82–89, 2015.

[18] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, and J. Harkin, "Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation," *International Journal of Bifurcation and Chaos*, vol. 27, no. 3, p. 1750033, 2017.

[19] 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.

[20] A. Wagemakers, F. J. Escribano, Sáez-Landete, and B. José, "Optimization of chaos-based coded modulations for compensation of amplifier nonlinearities," *Electronics Letters*, vol. 52, no. 22, pp. 1855-1856, 2016.

[21] K. J. Persohn and R. J. Povinelli, "Analyzing Logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation," *Chaos, Solitons and Fractals*, vol. 45, no. 3, pp. 238–245, 2012.

[22] Y. S. Deng, H. P. Hu, W. Xiong, N. N. Xiong, and L. F. Liu, "Analysis and design of digital chaotic systems with desirable performance via feedback control," *IEEE Transactions on System, Man and Cybernetics: Systems*, vol. 45, no. 8, pp. 1187–1200, 2015.

[23] L. F. Liu and S. X. Miao, "A universal method for improving the dynamical degradation of a digital chaotic system," *Physica Scripta*, vol. 90, no. 8, p. 85205, 2015.

[24] L. Liu, H. Hu, Y. Deng, and S. Miao, "Pseudorandom bit generator based on non-stationary logistic maps," *IET Information Security*, vol. 10, no. 2, pp. 87–94, 2016.

[25] C. Bandt and B. Pompe, "Permutation entropy: a natural complexity measure for time series," *Physical Review Letters*, vol. 88, no. 17, p. 174102, 2002.

[26] C. Q. Li, B. Feng, S. Li et al., "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 6, pp. 2322–2335, 2019.

[27] 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.

[28] H. Beker and F. C. Piper, *Cipher Systems: The Protection of Comminications*, Wiley, New York, NY, USA, 1982.

[29] NIST, *Federal Information Processing Standards Publication (FIPS140-1), Security Requirements for Cryptographic Modules*, NIST, Gaithersburg, MD, USA, 1994.

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

[31] A. Rukin, J. Soto, J. Nechvatal et al., *A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications*, NIST Special Publication 800-22rev1a, Gaithersburg, MD, USA, 2010.

[32] 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.

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