Nonlinear Dyn (2021) 103:1099–1115
https://doi.org/10.1007/s11071-020-06113-4

ORIGINAL PAPER

A novel perturbation method to reduce the dynamical degradation of digital chaotic maps

Lingfeng Liu · Hongyue Xiang · Xiangjun Li

Received: 17 June 2020 / Accepted: 23 November 2020 / Published online: 5 January 2021

Abstract A chaotic map, which is realized on finite precision device, such as computer, will suffer dynamical degradation. Such chaotic maps cannot be regarded as rigorous chaos anymore, since their chaotic characteristics are degraded, and naturally, these kinds of chaotic maps are not secure enough for cryptographic use. Therefore, in this paper, a novel perturbation method is proposed to reduce the dynamical degradation of digital chaotic maps. Once the state is repeated during the iteration, the parameter and state are both perturbed to make the state jump out from a cycle. This method is convenient to implement without any external sources and can be used for different kinds of digital chaotic maps. The most widely used logistic map is used as an example to prove the effectiveness of this method. Several numerical experiments are provided to prove the effectiveness of this method. Under the same precision, the number of iterations when entering a cycle and the period of the improved map are greater than those of the original one. The complexity analysis shows that the improved map can get an ideal complexity level under a lower precision. All these results prove that this perturbed method can greatly improve the dynamical characteristics of original chaotic map and is competitive with other remedies. Furthermore, we improve this method by using a variable perturbation, where the perturbation is affected according to the number of iteration steps. Numerical experiments further prove that this improved perturbation method has a better performance in suppressing dynamical degradation.

Keywords Chaos · Digital chaotic maps · Dynamical degradation · Constant perturbation · Varying perturbation

L. Liu (✉) · H. Xiang · X. Li
School of Software, Nanchang University, Nanchang 330029, Jiangxi, China
e-mail: lfliu@ncu.edu.cn

1 Introduction

Chaotic maps are widely used in many different kinds of scientific fields for their complex characteristics, such as the sensitivity to initial value and parameter, topological transitivity, aperiodicity, high dynamical complexity [1–9]. As many characteristics are consistent with cryptographic requirements, chaotic maps are very suitable for designing cryptographic algorithms. The first chaos-based encryption algorithm is proposed by Matthews in 1989 [10]. Since then, chaotic cryptography becomes more and more popular, and many chaos-based encryption algorithms have been proposed [11–24].

However, chaotic cryptography has not been fully approved nowadays. Theoretically, chaotic maps have such complex characteristics since they are running in an infinite state space. While in application, chaotic

map is always implemented on a finite precision device, such as computer, and then, its state space becomes finite. We always call it digital chaotic map, while a chaotic map is implemented on finite precision device. Due to the influence of finite state space, the output sequence of digital chaotic map will naturally become periodic since chaotic map is deterministic. Consequently, all such complex characteristics will disappear. Therefore, digital chaotic map does not satisfy the rigorous chaos definition. We call it dynamical degradation [25]. Affected by the dynamical degradation, digital chaotic maps are not secure enough for designing cryptographic algorithm.

To solve this problem, till now, many different kinds of methods have been proposed to reduce the dynamical degradation of digital chaotic maps. Generally, these methods can be divided into five categories. (1) using higher precision [20, 26]. A digital chaotic map realized on a higher precision device will certainly extend its state space and make its output more difficult to fall into a cycle. While using higher precision will increase implementation cost, and additionally, it is difficult to control the period of the orbit generated by the digital chaotic map. (2) Switching/Cascading different chaotic maps [27–29]. This method makes the output orbit jump back and forth in different chaotic tracks, so as to extend its period. However, this method completely ignores the dynamical complexity, the switching/cascading sequence may have a lower complexity than a single chaotic map. (3) Perturbation [30, 31]. This may be the most useful method to reduce the dynamical degradation of digital chaotic maps [25]. In most of these studies, an external perturbation source is necessary, and the dynamics of the perturbed map are always dominated by the external perturbation source, and the implementation cost will also increase since an external source is introducing. (4) Feedback control [32]. The method applies a state feedback control function on the basis of chaotic mapping. However, this method cannot work effectively without using other auxiliary methods, since a feedback controlled chaotic map is still deterministic. Additionally, analog–digital mixed control method proposed in [33, 34] should belong to this category. In this method, an analog chaotic system is used to make the trajectories of digital chaotic map random-like. The costs of implementation increase sharply when introducing a new analog chaotic system, and it is worthless if we only consider the chaotic map on finite precision devices. (5) Extending dimensions [35, 36]. High-dimensional chaotic maps perform better than low-dimensional chaotic maps in inhibiting dynamical degradation. In [35], a digital chaotic model by coupling two chaotic maps is proposed. The coupled map has a larger dimension and is more complex than the original digital chaotic map. In [36], a delay introducing method is proposed by introducing the delayed state, which is also equivalent to expanding its dimension. While in these studies, no specific coupling or delay control mechanism is given, which makes this method difficult to apply to other digital chaotic maps.

Considering the advantages and disadvantages of the above methods, we propose a convenient perturbation method to reduce the dynamical degradation of digital chaotic maps. In this method, both parameter and state are perturbed. The innovation of this method is that the parameters and state variables are disturbed only when the current state is duplicated, which is used to make the state jump out from a cycle. In this perturbation method, no external perturbation source is needed. Furthermore, the digital chaotic map is only perturbed by some proper constant or variable constant, which is much easier to implement than other perturbation methods, such as [30, 31]. Two conditions are provided as the restrictions on selecting the disturbance constant, which can also be regarded as guidelines for selecting such proper constant. Theoretically, this method can be used for most of the digital chaotic maps. In this paper, the most widely used logistic map is taken as an example to prove the effectiveness of this method. The numerical simulation results show that the performances of digital logistic map have been greatly improved. Comparative analysis also indicates that this method is better than many other remedies, which implies that this method is quite competitive. Different from some other methods, the method in this paper can still maintain the basic structure of phase space. While in those remedies [32–34], the phase spaces are completely disrupted, which cannot be regarded as a method of reducing dynamical degradation, but designing new random sources. The period and complexity analysis prove that this method can reduce the dynamical degradation under a lower computing precision, which is an important measure for a remedy.

The perturbed digital chaotic maps have great potential applications in many different fields, especially in cryptography. The significant advantages of this method can be summarized as:

(1) This method can reduce the dynamical degradation of digital chaotic maps effectively and is competitive with many other remedies, especially under low computing precision.
(2) This method is easy to implement without any external sources.
(3) This method is universal for most of the digital chaotic maps.

The rest of this paper is organized as follows. In Sect. 2, the novel perturbation method is provided and applied to the digital logistic map. Some numerical simulations and comparative analysis of the perturbed digital logistic map are presented in Sect. 3. In Sect. 4, an improved varying perturbation method is proposed, and some experiments are presented as well. Finally, Sect. 5 concludes the whole paper.

2 A novel perturbation method for digital chaotic maps

The mathematical model of a general chaotic map can be written as

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

where x_i denotes the state variable, f is the chaotic iteration function, and a is the control coefficient. According to this iteration function, we can generate a chaotic sequence by using an initial value x_0. Theoretically, the generated sequence should be aperiodic and has high dynamical complexity. Once the chaotic map is realized on a finite precision device, whose mathematical model can be described as

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

where FL is the precision operator, its dynamical characteristics will degenerate. We call it digital chaotic map. Since the precision operator FL restricts the state space into finite, the state of digital chaotic map will inevitably enter a cycle. In this case, other dynamical performances will degenerate accordingly. Therefore, in order to reduce the dynamical degradation of digital chaotic map, a direct approach is to make the state jump out from the cycle, once it falls into a cycle. That is to say, since $x_p = x_q$ is inevitable, where p and q denote the iteration steps and $0 < p < q < N$, we should try to make $x_p \neq x_q$. Assume the largest precision be 2^{-m}, the inequality $x_p \neq x_q$ will hold if the following equation holds.

$$\left| f(x_q) - f(x_p) \right| > 2^{-m} \tag{3}$$

Motivated by this consideration, we propose a novel digital chaotic model, whose model can be described as

$$x_{q+1} = \begin{cases} FL \circ \left(f(x_q, a') + \delta \right) & \text{if } x_q = x_p \text{ happens} \\ FL \circ f(x_i, a) & \text{else} \end{cases} \tag{4}$$

where a' is a perturbation of coefficient, and δ is the perturbation of state variable. The effectiveness of this method depends on the following two conditions.

(1) Equation (3) should be satisfied to make the state x_q jump out from the cycle when $x_p = x_q$.
(2) The state variable of Eq. (4) should still locate in the chaos range of function f.

This method is universal for most of the digital chaotic maps by selecting some suitable parameter a' and δ. Next, we take the most widely used logistic map as an example to demonstrate the effectiveness of this method. The digital logistic map can be written as

$$x_{i+1} = FL \circ (a x_i (1 - x_i)) \tag{5}$$

Here, parameter a should be in the interval (3.6, 4]. According to Eq. (4), for simplicity, we select $a' = a - \Delta a$, and $\delta = k\Delta a$, where $\Delta a < a$ is a positive constant, which is used for parametric perturbation. This parameter reflects the difference from the original parameters. $k > 0$ is a constant which is used for state perturbation. Thus, the perturbed digital logistic map can be described as

$$x_{q+1} = \begin{cases} FL \circ \left((a - \Delta a) x_q (1 - x_q) + k\Delta a \right) & \text{if } x_q = x_p \text{ happens} \\ FL \circ f(x_q, a) & \text{else} \end{cases} \tag{6}$$

Based on the analysis above, the effectiveness of this method is that whether we can select an appropriate coefficient k to satisfy the Conditions 1 and 2. Next, we give some guidelines of the selection of k.

Condition 1 Assume the largest precision be 2^{-m} and $x_p = x_q$, Eq. (3) will hold for Eq. (6) if $k > \frac{1}{2^m \Delta a} + \frac{1}{4}$.

Proof According to Eq. (6), if $x_p = x_q$, we have

$$\begin{aligned} \left|f(x_q) - f(x_p)\right| &= \left|(a-\Delta a)x_q(1-x_q) + k\Delta a - a x_p(1-x_p)\right| \\ &= \left|-\Delta a x_q(1-x_q) + k\Delta a\right| \\ &= \left|\Delta a x_q^2 - \Delta a x_q + k\Delta a\right| \\ &= |\Delta a| \cdot \left|\left(x_q - \frac{1}{2}\right)^2 + k - \frac{1}{4}\right| \end{aligned} \tag{7}$$

Put $k > \frac{1}{2^m \Delta a} + \frac{1}{4}$ into Eq. (7), we can have

$$\begin{aligned} \left|f(x_q) - f(x_p)\right| &> |\Delta a| \cdot \left|\left(x_q - \frac{1}{2}\right)^2 + \frac{1}{2^m \Delta a} + \frac{1}{4} - \frac{1}{4}\right| \\ &= |\Delta a| \cdot \left|\left(x_q - \frac{1}{2}\right)^2 + \frac{1}{2^m \Delta a}\right| > \frac{1}{2^m} \end{aligned} \tag{8}$$

which proves that Eq. (3) is satisfied. □

Condition 2 The state variable of Eq. (6) still locate in the chaos range (0, 1) if $k < \frac{1}{\Delta a} - \frac{a}{4\Delta a} + \frac{1}{4}$.

Proof This condition equals to prove the inequality $0 < (a - \Delta a)x(1 - x) + k\Delta a < 1$ if $0 < x < 1$. After some derivation, we have

$$\begin{aligned} (a-\Delta a)x(1-x) + k\Delta a &= -(a-\Delta a)\cdot\left(x^2 - x\right) + k\Delta a \\ &= -(a-\Delta a)\cdot\left(\left(x - \frac{1}{2}\right)^2 - \frac{1}{4}\right) + k\Delta a \\ &= -(a-\Delta a)\left(x - \frac{1}{2}\right)^2 + \frac{a}{4} - \frac{\Delta a}{4} + k\Delta a \end{aligned} \tag{9}$$

Since $k > 0$, $0 < \Delta a < a$ and $0 < x < 1$, we have

$$\begin{aligned} &-\frac{a-\Delta a}{4} + \frac{a}{4} - \frac{\Delta a}{4} + k\Delta a < (a-\Delta a)x(1-x) \\ &+ k\Delta a < \frac{a}{4} - \frac{\Delta a}{4} + k\Delta a \end{aligned} \tag{10}$$

Thus, we can conclude that

$$\begin{aligned} (a-\Delta a)x(1-x) + k\Delta a &> -\frac{a-\Delta a}{4} + \frac{a}{4} - \frac{\Delta a}{4} \\ &+ k\Delta a \\ &= k\Delta a > 0 \end{aligned} \tag{11}$$

and

$$(a-\Delta a)x(1-x) + k\Delta a < \frac{a}{4} - \frac{\Delta a}{4} + k\Delta a \tag{12}$$

Assume $k < \frac{1}{\Delta a} - \frac{a}{4\Delta a} + \frac{1}{4}$, we have

$$\begin{aligned} (a-\Delta a)x(1-x) + k\Delta a &< \frac{a}{4} - \frac{\Delta a}{4} \\ &+ \left(\frac{1}{\Delta a} - \frac{a}{4\Delta a} + \frac{1}{4}\right)\Delta a \\ &= 1 \end{aligned} \tag{13}$$

Summarily, according to Eqs. (11) and (13), we can conclude that $0 < (a - \Delta a)x(1 - x) + k\Delta a < 1$ which indicates the validity of Condition 2.

Therefore, to make this method valid, the linear coefficient k should be selected from the interval $\left(\frac{1}{2^m \Delta a} + \frac{1}{4}, \frac{1}{\Delta a} - \frac{a}{4\Delta a} + \frac{1}{4}\right)$. This condition can be easily satisfied. For example, we can choose $a = 3.9$, $\Delta a = 0.02$, $m = 12$. Thus, the linear coefficient k should select in the interval (0.25, 1.5) to satisfy Conditions 1 and 2, which is easy to select. The flowchart diagram of the perturbation method is shown in Fig. 1. □

3 Numerical simulations for the perturbed digital logistic map

In this Section, the following numerical simulations will be provided to prove the effectiveness of this method. The parameters are selected as $a = 3.9$, $\Delta a = 0.02$, $m = 12$, $k = 0.8811$ and $x_0 = 0.1562$ unless otherwise indicated.

3.1 Maximum Lyapunov exponent

Lyapunov exponents (LE) can be used to express the characteristics of motion of chaotic systems. The maximum Lyapunov exponent ($\lambda_{\max}$) determines the fastest divergence speed of trajectories in a certain direction. For s chaotic system, one exponent should be positive at least. Therefore, a system can be regarded as chaotic if $\lambda_{\max} > 0$. As we know, the sequences generated by digital chaotic maps will

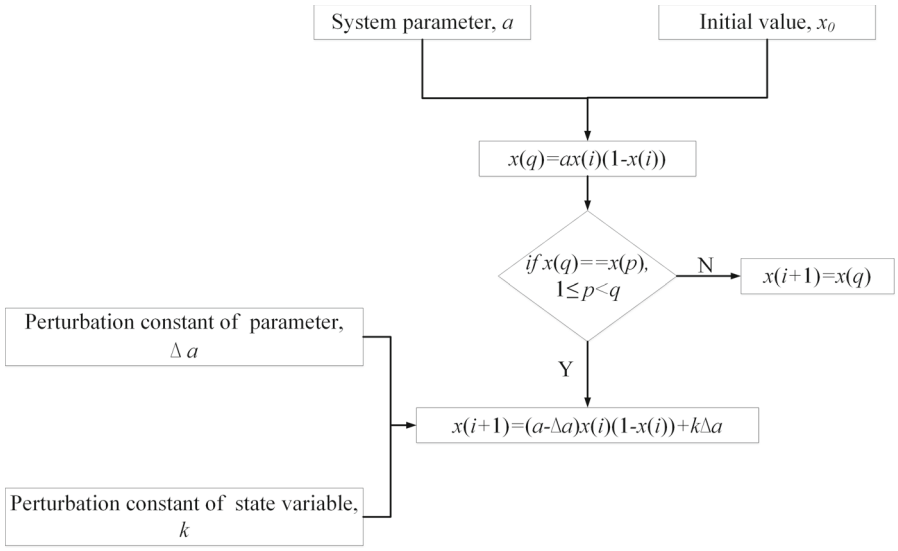

Fig. 1 Flowchart diagram of the specific perturbation method for digital logistic map

finally enter a cycle, and the LE will be zero since they are periodic. Thus here, we discuss the LE of model (6) in an ideal theoretical case (without degradation). The maximum Lyapunov exponent spectrum diagram is shown in Fig. 2. Form Fig. 2, we can find that the LE of the improved map will be greater than zero in some suitable range of parameter a, which indicates that the improved logistic map is still chaotic.

3.2 Trajectories and phase space

Trajectory is the most intuitive way to reflect the output characteristics of chaotic maps. In this test, the precision is set to be 2^{-12}. The trajectories of the original digital logistic map Eq. (5) and the perturbed digital logistic map Eq. (6) are depicted in Fig. 3a, b, respectively. As shown in Fig. 3, after less than 100 times iterations, the trajectory of original digital logistic map will quickly fall into a cycle, while the trajectory of the perturbed digital logistic map is still random-like, with no obvious structural features. This result implies that the perturbed method can extend the period of digital logistic map. We will take some more detailed experiments in the period analysis sub-section later. Figure 4a, b shows the phase space of Eqs. (5) and (6), respectively. From Fig. 4, we can find that the phase space of the perturbed digital logistic map is much denser than the phase space of original map, which indicates that the perturbed method can greatly improve its ergodicity. Furthermore, the phase space of the perturbed map has certain similarity to the original map, which means that this method does not disrupt the phase space structure of original chaotic map completely. This is a very important criteria in reducing the dynamical degradation of digital chaotic map. To reduce the dynamical degradation of digital chaotic map, the improved map should maintain its basic structure of phase space. In some studies, such as [32–34], the phase space of the digital chaotic maps is all completely disrupted, with no structure characteristics maintained. Thus, we should call these remedies designing new random sources, rather than reducing the dynamical degradation of digital chaotic maps.

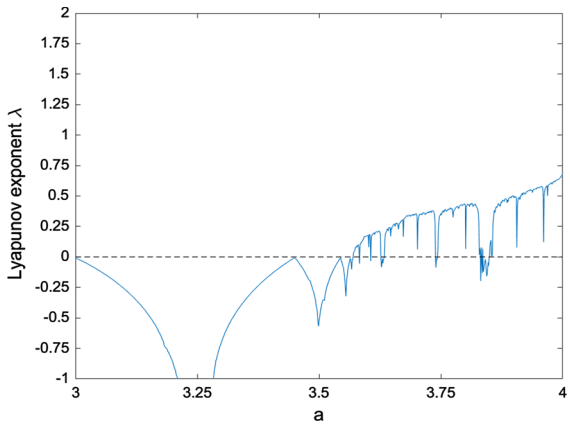

Fig. 2 Maximum Lyapunov exponent spectrum diagram of the improved logistic map

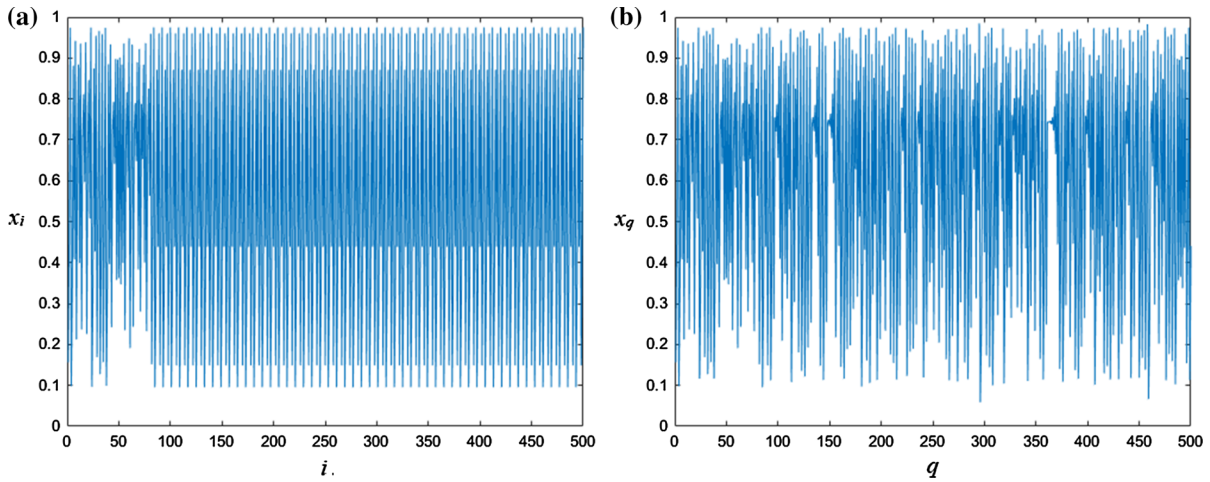

Fig. 3 Trajectories analysis of the digital logistic maps. **a** Original digital logistic map; **b** perturbed digital logistic map

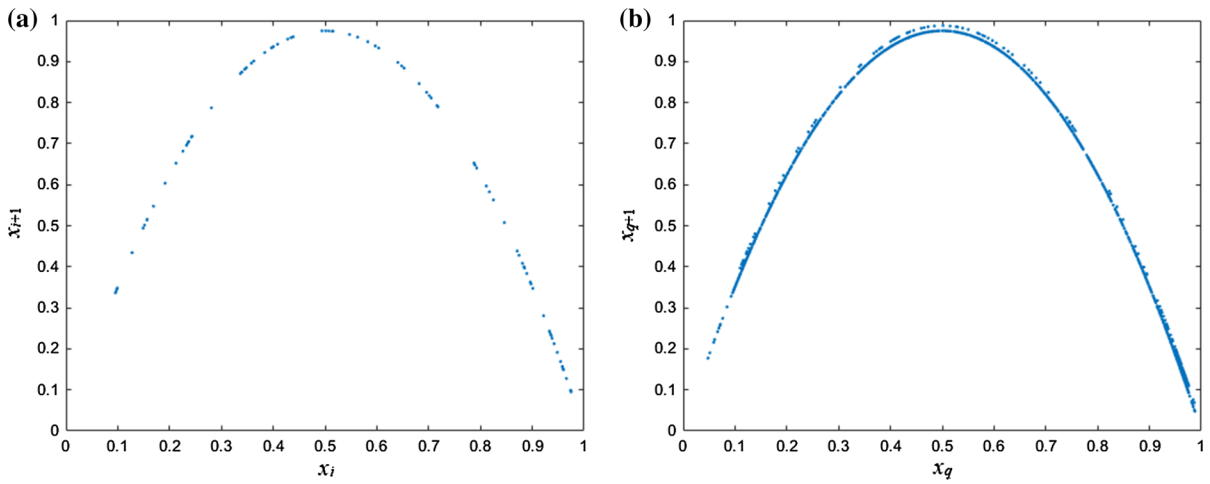

Fig. 4 Phase space analysis of the digital logistic maps. **a** Original digital logistic map; **b** perturbed digital logistic map

3.3 Period analysis

Period is the most important indicator in reducing the dynamical degradation of digital chaotic maps, since it has great impact on all chaotic characteristics. The degradation of other characteristics results from the periodicity of digital chaotic maps. To evaluate the periodicity of a digital map, two aspects should be considered, one is the length of period, and the other is the number of iterations when it firstly enters a cycle. Set the length of the generated sequences be 10^6 in this test. We selected 1000 groups of parameters (a, Δa, k, x_0) randomly in the parameter range, varying the largest precision from 2^{-12} to 2^{-24}, the average period length and average number of iterations when entering a cycle are shown in Table 1. Here, the arithmetic mean is used to calculate the average period length and average number of iterations. From Table 1, we can find that, (1) The length of the period is extended by using the perturbation method for different precision. (2) The number of iterations when the sequence firstly enters a cycle are all greatly increased for different precision (This indicator is often ignored in other studies, such as [35, 36, 40]). Both these results prove that this perturbation method can greatly improve the period characteristics of digital logistic map. Comparing with other remedies, for example, in [36], the period cannot be detected (larger than 200,000) since the largest precision be 2^{-36}. While in this method, the period cannot be detected since the largest precision be

Table 1 Period analysis of original digital logistic map and perturbed digital logistic map (U denotes undetected)

Precision	Period of Eq. (5)	Period of Eq. (6)	Number of iterations when entering a cycle (Eq. (5))	Number of iterations when entering a cycle (Eq. (6))
2^{-12}	25	56	51	2609
2^{-13}	51	88	48	4457
2^{-14}	66	116	54	8743
2^{-15}	84	147	87	16,167
2^{-16}	127	203	95	32,274
2^{-17}	182	238	141	60,328
2^{-18}	190	342	177	70,500
2^{-19}	261	362	280	136,971
2^{-20}	277	U	431	U
2^{-21}	525	U	468	U
2^{-22}	703	U	922	U
2^{-23}	1479	U	911	U
2^{-24}	1133	U	1183	U

2^{-20}, which implies that this method is competitive with other remedies in extending period. From the table, we also could estimate the typical number of steps required for transition to aperiodic state after the perturbation by subtracting the number of iterations when entering a cycle of Eq. (6) and the number of iterations when entering a cycle of Eq. (5). The effect is more significant with the growth of computing precision.

3.4 Auto-correlation analysis

Auto-correlation function is used to measure the randomness of a given sequence. For an ideal chaotic sequence, its auto-correlation function should rapidly vanish along with the interval, which is similar to the delta function. Set the largest precision be 2^{-12}. The auto-correlation functions of Eqs. (5) and (6) are presented in Fig. 5a, b, respectively. From Fig. 5, we can easily find that the auto-correlation function of the perturbed digital logistic map rapidly decreases along with the interval and then remain stable around 0, which can be observed more clearly by the insert figure. Thus, it can be regarded as an ideal delta function. However, the auto-correlation function of the original digital logistic map still remains a high correlation for a large interval. These results indicate that the perturbed method has improved the chaotic characteristics of digital chaotic map effectively.

3.5 Sensitivity analysis

Sensitivity to the initial value and parameters of chaotic map can be described as the differences with slight change in initial value and parameters. For an ideal chaotic map, the generated sequences should have a high sensitivity. In this test, we change the initial value a and parameter x_0 by only 2^{-12}, the differences between the two generated sequences are depicted in Figs. 6 and 7, respectively. From the figures, we can conclude that the sequences are completely separated after a few times of iteration for both x_0 and a, which implies that the improved map has a high sensitivity to both initial value and parameter.

3.6 Approximate entropy analysis

Approximate entropy (ApEn) was first proposed in [37], which calculates the probability of the new pattern generated in a sequence with the growth of embedding dimension. Nowadays, it is widely used as a complexity measure for sequence. If a sequence has a greater ApEn, it is regarded to be more complex than the other one. In this test, we set $a = 3.95$, $k = 0.85$ to

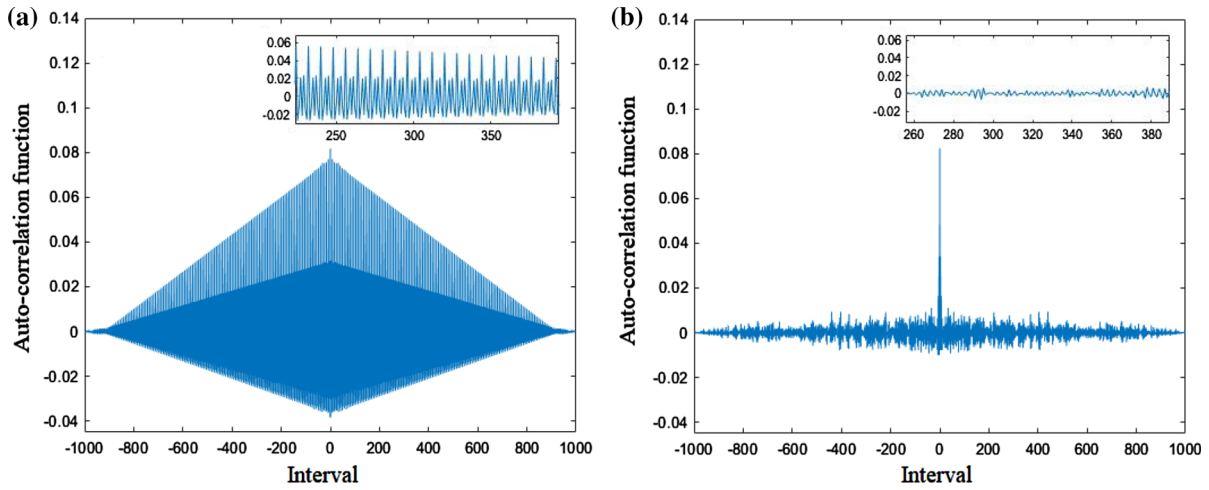

Fig. 5 Auto-correlation function analysis of the digital logistic maps. **a** Original digital logistic map; **b** perturbed digital logistic map

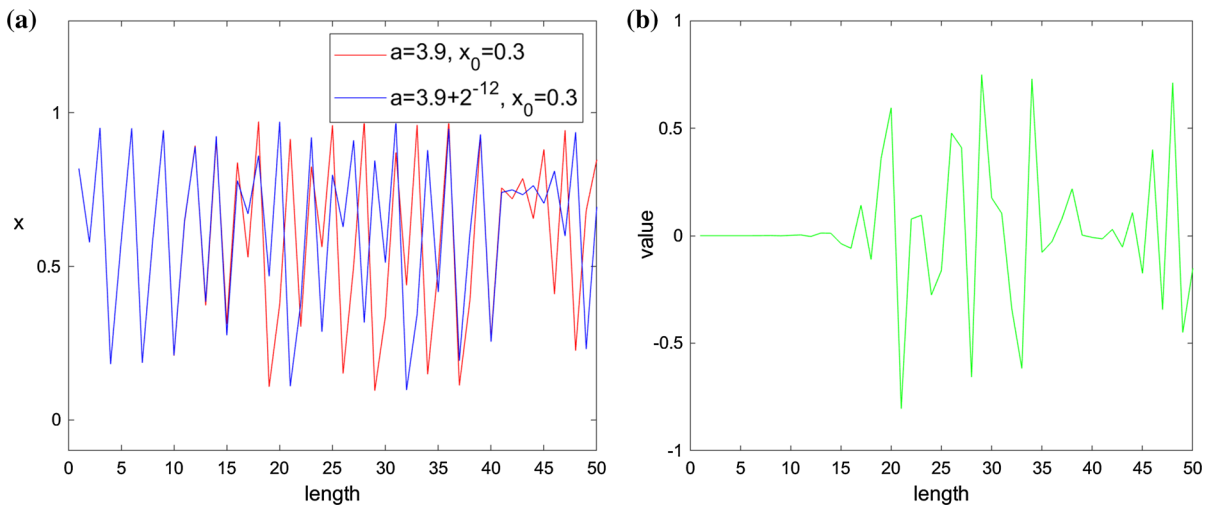

Fig. 6 Sensitivity analysis of the perturbed digital logistic map for parameter a, **a** two trajectories with different parameter a (The red line represents the trajectory with $a = 3.9$; the blue line represents the trajectory with $a = 3.9 + 2^{-12}$), **b** the difference between these two curves

compare our results with other remedies under the same control coefficient. The precision is varying from 2^{-6} to 2^{-20}, and the ApEn test results are plotted in Fig. 8. From Fig. 8, we can easily find that the ApEn of the perturbed logistic map are always larger than the ApEn of original logistic map with low computing precision. While with the growth of the largest precision, the difference between ApEn of the original digital logistic map and the perturbed digital logistic map will dwindle. This is because that with the growth of computing precision, the case $x_p = x_q$ is more difficult to appear. While this perturbation mechanism is only implemented when the case $x_p = x_q$ happens. Therefore, the generated sequences of these two maps will tend to be similar, and their ApEn will be close naturally. We should note that it is more important to evaluate the effectiveness of a remedy on a low computing precision condition. Since for a large computing precision, the original digital chaotic map has good performances already, such remedies are unnecessary for practical uses. Furthermore, there is an obvious oscillation of ApEn at low precision. This is because that the sequence generated by digital chaotic map under a low computing precision will

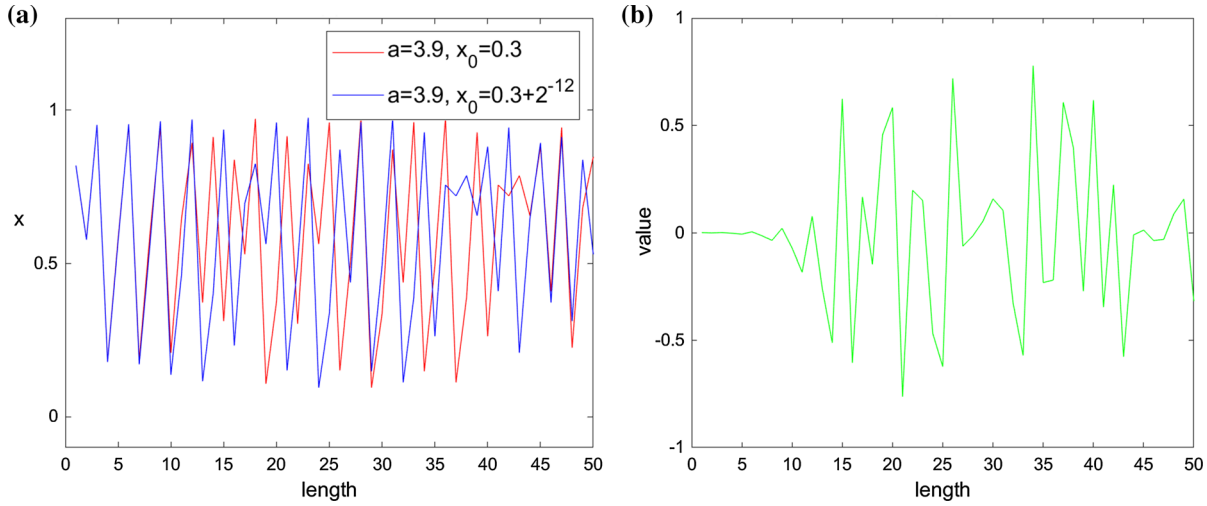

Fig. 7 Sensitivity analysis of the perturbed digital logistic map for initial value x_0, **a** two trajectories with different initial value x_0 (The red line represents the trajectory with $x_0 = 0.3$; the blue line represents the trajectory with $x_0 = 0.3 + 2^{-12}$), **b** the difference between these two curves

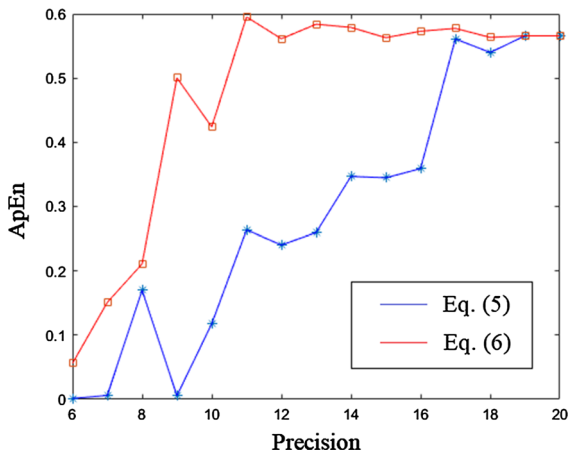

Fig. 8 ApEn analysis of the original digital logistic map (Eq. (5), blue line) and the perturbed digital logistic map (Eq. (6), red line) under different precision

quickly enter a cycle. Theoretically, the average period of the generated sequences will be larger under a higher precision. While for a certain experiment, the period of the generated sequence may be smaller under a higher computing precision than the period of the generated sequence under a lower precision, and so as the complexity may decrease when the computing precision increases. Similar results can be found in the following PE analysis.

3.7 Permutation entropy analysis

Permutation entropy (PE) is also a sequence complexity measure, which is proposed in [38]. PE measures the uncertainty of orders which based on the size of consecutive values in the sequence. This measure is proved to be more robust to the noise [39]. In this test, the ordinal pattern length L and the embedding delay D is selected as 6 and 2, respectively, due to the suggestion in [38]. Set $a = 3.95$, $k = 0.85$, and the test results are depicted in Fig. 9. Similar to the ApEn test, for every precision, the PE of the perturbed

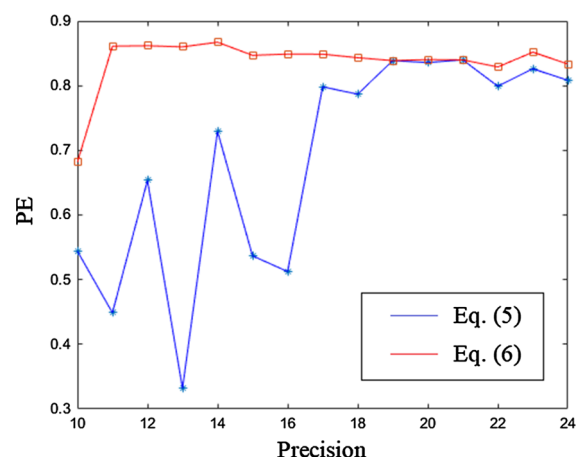

Fig. 9 PE analysis of the original digital logistic map (Eq. (5), blue line) and the perturbed digital logistic map (Eq. (6), red line)

digital logistic map is no less than the PE of original digital logistic map, especially with a low computing precision. These results also prove that this perturbation method is effective in improving the complexity of digital chaotic maps in this sense.

From the results of previous experiments, it is clear that the perturbed digital logistic map shows a good chaotic performance under the parameters selected randomly. As we know, the chaotic system is sensitive to its parameters. The performances will be different with different parameters. Here, we use PE to evaluate the influences of different parameters. By using the Conditions 1 and 2 to determine the range of each parameters, the PE of the generated sequences via different parameters is shown in Fig. 10. From Fig. 10a, we can find that the PE complexity is increasing monotonically with the growth of parameter a. While for the changes in other parameters Δa, k and x_0, the PE have no obvious difference, as shown in Fig. 10b–d. Thus, for practical use, the parameter a should be close to 4 to ensure a higher complexity, while other parameters can be selected randomly within the range.

4 An improved varying perturbation method for digital chaotic maps

From the numerical simulation results above, we can conclude that the perturbation method can improve the dynamical characteristics of digital chaotic map to some extent. However, there exist a fatal flaw in this method, that is Eq. (4) can only ensure the state x_q jump out from the cycle when the case $x_q = x_p$ firstly appear. That means if the case $x_p = x_q = x_r$ appears, $p < q < r$, we will have $x_{q+1} = x_{r+1}$ since they are generated by the same iteration equation. Therefore, to improve the perturbation method, we can construct the following varying perturbation model

$$x_{q+1} = \begin{cases} FL \circ \left(f(x_q, a') + \delta_q\right) & \text{if } x_q = x_p \text{ happens} \\ FL \circ f(x_q, a) & \text{else} \end{cases} \tag{14}$$

where the state perturbation term δ_q is varying for different iteration steps. Similarity, take 1D logistic map as an example, the varying perturbed digital logistic map can be described as

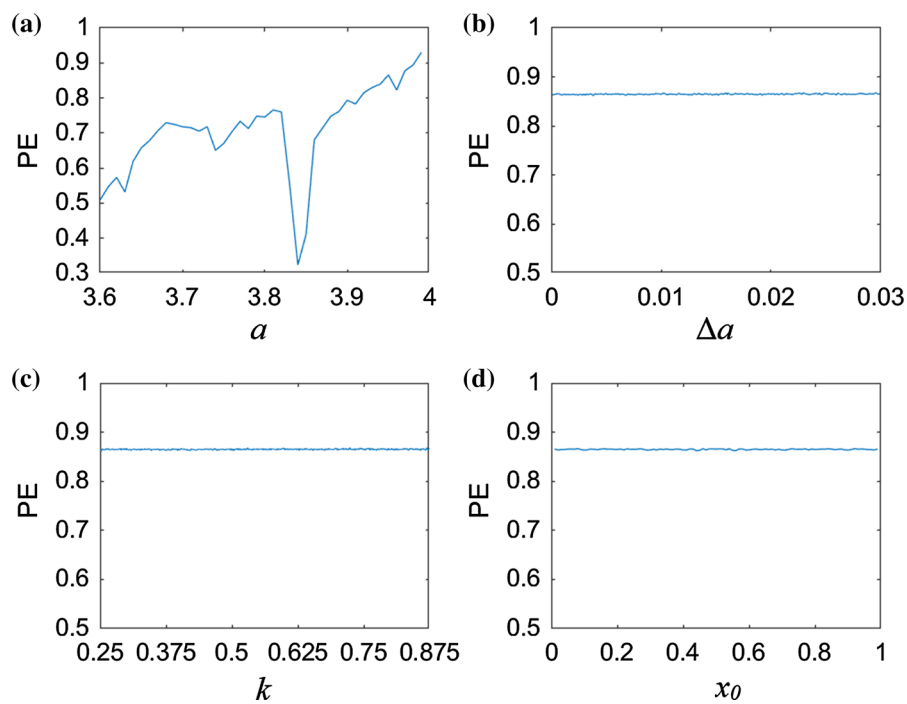

Fig. 10 PE changes with different coefficients **a** a value; **b** Δa value; **c** k value; **d** x_0 value

$$x_{q+1} = \begin{cases} FL \circ \left((a - \Delta a)x_q(1 - x_q) + k_q \Delta a\right) \text{ if } x_q = x_p \text{ happens} \\ FL \circ f(x_q, a) \text{ else} \end{cases} \tag{15}$$

Here, k_q is a varying parameter which is influenced by the iteration step q and is used as state perturbation, which can be written as

$$k_q = \frac{1}{2^m \Delta a} + \frac{1}{4} + \left(\frac{4 - a + \Delta a}{4\Delta a} - \frac{1}{2^m \Delta a} - \frac{1}{4}\right) \cdot |\cos q| \tag{16}$$

Since $0 < |\cos\ q| < 1$, the varying k_q will always located in the interval $\left(\frac{1}{2^m \Delta a} + \frac{1}{4}, \frac{1}{\Delta a} - \frac{a}{4\Delta a} + \frac{1}{4}\right)$, so that the Conditions 1 and 2 can be satisfied. The flowchart diagram of the improved varying perturbation method for 1D Logistic map is shown in Fig. 11.

Set a = 3.9, Δa = 0.02, m = 12 and x_0 = 0.1562, we do some similar numerical experiments to prove the effectiveness of this improved method.

Figure 12a, b depicts the trajectory and phase space of the improved perturbed digital logistic map, respectively. As shown in Fig. 12a, the trajectory of the improved perturbed logistic map is random-like, with no obvious structure, and the period cannot be detected within 500 times iterations. Figure 12b shows that the phase space of Eq. (15) is still a parabola-like structure on the whole, which indicates that the improved perturbed logistic map does not disrupt the phase space as well. Comparing with Fig. 4a, the phase space of Eq. (15) is also much denser than the phase space of original digital logistic map, which means that more new states can be generated by Eq. (15). Figure 13 plots the auto-correlation function of this improved perturbed

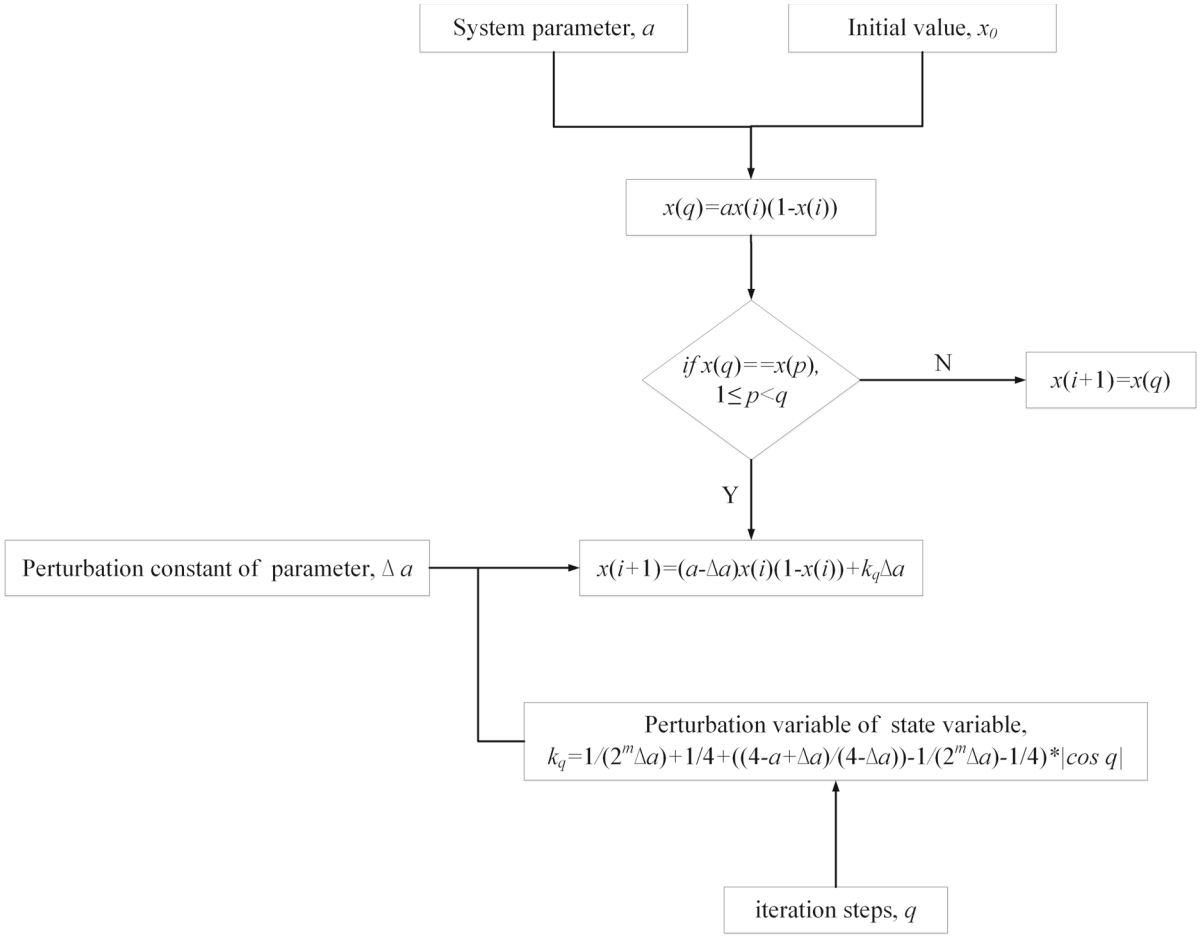

Fig. 11 Flowchart diagram of the improved varying perturbation method for 1D Logistic map

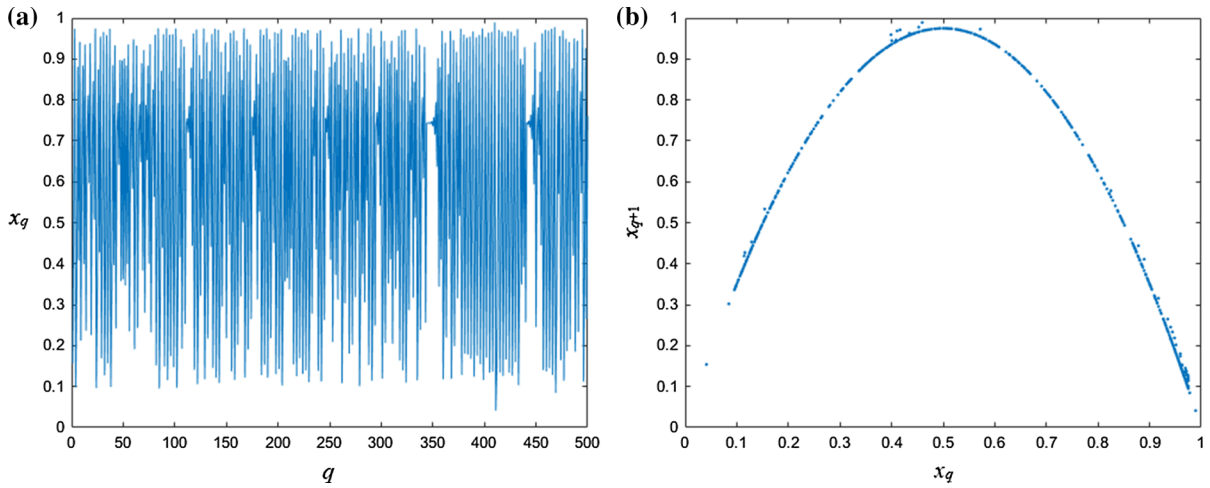

Fig. 12 Trajectory and phase space of the improved perturbed digital logistic map. **a** Trajectory; **b** phase space

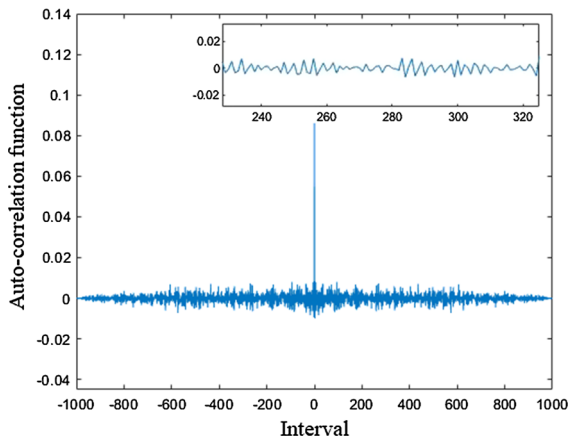

Fig. 13 Auto-correlation function of the improved perturbed digital logistic map

logistic map. As shown in Fig. 13, the correlation will quickly decline with the growth of interval and become stable around 0. More details can be found in the insert diagram. Thus, the auto-correlation function is quite similar to the ideal delta function. Obviously, the trajectory, phase space, and auto-correlation function test results show that the improved perturbation method can improve the chaotic characteristics of digital chaotic maps.

In order to show the progressiveness of this improve perturbation method, we further do the periodicity analysis, ApEn analysis and PE analysis, and compare the test results with other proposed remedies, including the perturbation method in Sect. 2. As we mentioned above, it is more important to evaluate the effectiveness of a remedy on a low computing precision condition. Therefore, in this test, we vary the precision from 2^{-6} to 2^{-15}.

Similarly, we select 1000 groups of parameters (a, $\triangle a$, k, x_0) randomly in the valid parameter ranges, varying the largest precision from 2^{-6} to 2^{-15}. The average period length and average number of iterations when entering a cycle are presented in Table 2 and 3, respectively. The length of test sequence is 10^6. From Table 2, we can find that the period of the improved perturbed digital logistic map (Eq. (15)) is much larger than the original digital logistic map (Eq. (5)), and also larger than the perturbed digital logistic map (Eq. (6)) proposed in Sect. 2, which proves that this improved varying perturbation method can greatly extend the period of digital chaotic map. The period of Eq. (15) cannot be detected since the computing precision is larger than 2^{-9}. With more detailed study, for the sequences generated by Eq. (15), we can always find the case that $x_p = x_q$, $x_{p+1} = x_{q+1}$, $x_{p+2} = x_{q+2}$,..., while $x_{p+k} \neq x_{q+k}$, $x_{p+k+1} \neq x_{q+k+1}$,... This case implies that the improved varying perturbation method can make the trajectory jump out from the cycle, which is the main purpose of this method. Furthermore, comparing with some digital logistic maps in other remedies [35, 36, 40], we can find that the period of this improved varying perturbed digital logistic map has the largest period under the same precision, which indicates that this method is effective and competitive with other recent remedies.

Table 2 Period comparison between different remedies (U denotes undetected)

Precision	Equation (5)	Equation (6)	Equation (15)	Ref. [36]	Ref. [40]	Ref. [35]
2^{-6}	5	6	994	11	15	9
2^{-7}	7	9	621	14	9	20
2^{-8}	11	17	355	7	33	14
2^{-9}	15	25	U	12	18	84
2^{-10}	23	26	U	13	129	424
2^{-11}	28	32	U	12	90	90
2^{-12}	25	56	U	9	165	8
2^{-13}	51	88	U	148	48	16
2^{-14}	66	116	U	151	198	10,469
2^{-15}	84	147	U	388	105	7

Table 3 Number of iterations when firstly entering a cycle (U denotes undetected)

Precision	Equation (5)	Equation (6)	Equation (15)	Ref. [36]	Ref. [40]	Ref. [35]
2^{-6}	6	59	942,333	2	27	16
2^{-7}	8	137	959,908	12	38	66
2^{-8}	10	245	977,894	9	18	75
2^{-9}	15	504	U	57	14	63
2^{-10}	17	838	U	66	39	144
2^{-11}	26	1439	U	99	20	1528
2^{-12}	51	2609	U	64	111	192
2^{-13}	48	4457	U	63	45	1165
2^{-14}	54	8743	U	110	156	4508
2^{-15}	87	16,167	U	21	303	538

Another point of view to evaluate the periodicity of a digital chaotic map is the number of iterations when firstly entering a cycle. The test results are shown in Table 3. From Table 3, we can find that the improved varying perturbation method can greatly delay the steps of the trajectory when firstly entering a cycle and performs better than Eq. (5) and (6), and the methods in Refs. [35, 36, 40] as well, which further proves the effectiveness of this improved perturbation method.

Figure 14 compares the ApEn complexity of the improved perturbation method with other proposed remedies. From Fig. 14, we can find that with low computing precision, the ApEn of the improved perturbed digital chaotic map (Eq. (15)) is significantly larger than ApEn of the perturbed digital chaotic map (Eq. (6)). With the growth of computing precision, the ApEn of these two digital maps will tend to be consistent. This result implies that the improved perturbation method can make great improvement for low computing precision. Furthermore, from Fig. 14 we can also find that the remedies in Refs. [36, 40]

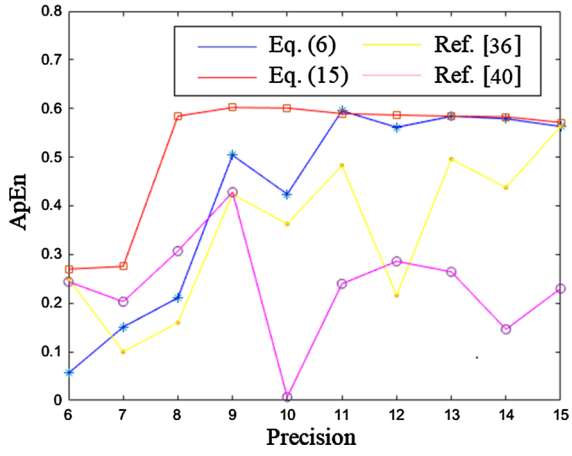

Fig. 14 ApEn analysis of the improved perturbed digital logistic map and comparison with other digital logistic maps (The red line is for the improved perturbed digital logistic map Eq. (15); The blue line is for the perturbed digital logistic map Eq. (6); The yellow line is for the improved digital logistic map in Ref. [36]; The purple line is for the improved digital logistic map in Ref. [40].)

make no effect for low computing precision in this sense, and the perturbed digital logistic maps proposed in this paper have a larger complexity than the improved logistic maps in Refs. [36, 40], which indicates that our perturbation method is quite competitive.

Similar with Fig. 14, as shown in Fig. 15, the PE complexity of the improved perturbed digital logistic map (Eq. (15)) will always larger than the PE complexity of the proposed digital maps in Refs. [36, 40] for different precision, which indicates that this improved perturbation method is quite competitive. Comparing with the perturbed logistic map Eq. (6), we can find that this improved perturbation method has a significant effect for low computing precision. While for large computing precision, there is no significant difference between these two methods.

The sensitivity analysis of initial value x_0 and parameter a is shown in Figs. 16 and 17, respectively. Both these two figures show that the trajectories will be separated greatly when the initial value x_0 and parameter a are changing slightly by only 2^{-12}, which indicates that the improved perturbed digital logistic map is quite sensitive to its initial condition and parameters.

In conclusion, when the computing precision is large enough, the sequences generated by different

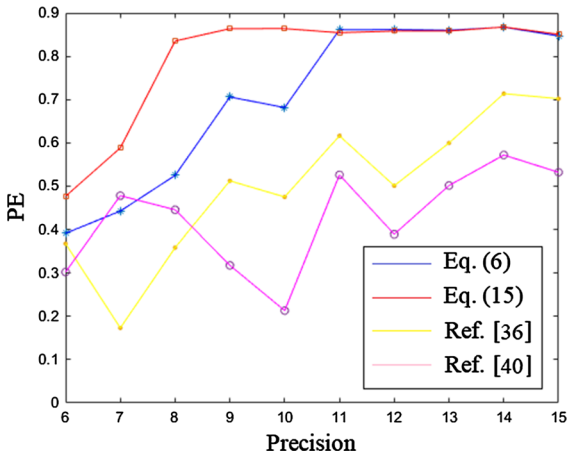

Fig. 15 PE analysis of the improved perturbed digital logistic map and comparison with other digital logistic maps (The red line is for the improved perturbed digital logistic map Eq. (15); The blue line is for the perturbed digital logistic map Eq. (6); The yellow line is for the improved digital logistic map in Ref. [36]; The purple line is for the improved digital logistic map in Ref. [40].)

improved digital chaotic maps will not enter a cycle due to the limitation of test data. Thus, there are no significant differences between these remedies in the numerical experiments. All the improved digital chaotic sequences will be similar with the original chaotic sequence, since the original digital chaotic map always performs well for a large computing precision. While for low computing precision, different remedies will perform different. Experiment results show that this improved perturbation method can make the period larger with a low computing precision, and delay the time of entering the cycle. Correspondingly, the improved digital chaotic sequence has a larger complexity. All these results prove that the improved perturbation method in this paper is progressive and competitive with other remedies.

5 Conclusions

Digital chaotic maps have wide application in many different kinds of field, including designing an encryption algorithm [1–9]. However, when a digital chaotic map is realized on finite precision device, such as computer, its state space will be discretized and finite. These factors will make the digital chaotic map degenerate, and its characteristics will not suit for cryptographic uses [25]. In order to reduce such dynamical degradation of digital chaotic maps, we propose a simple perturbation method in this paper. In this method, periodicity is the main consideration since it is the cause of degradation. When repetitive states occur, the system parameters and state variables are disturbed to make them jump out from the cycle. Both fixed perturbation and varied perturbation are considered in this paper. For the varied perturbation, the perturbation is affected according to the number of iteration steps. From the numerical experiments, we can find that the varied perturbation method is significantly better than the fixed perturbation method for low computing precision. While for large computing precision, these two perturbation methods have no obvious differences. This method can still maintain the basic structure of phase space. While in some other methods [32–34, 41], the phase spaces are completely disrupted, which cannot be regarded as a method of reducing dynamical degradation, but designing new random sources. Comparing with the improved digital

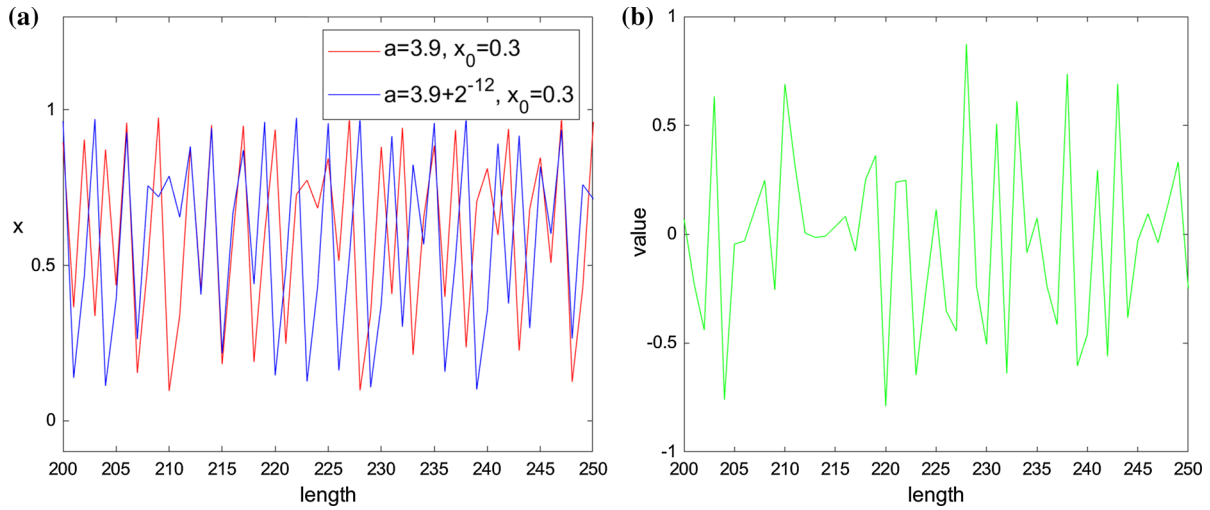

Fig. 16 Sensitivity analysis of the improved varying perturbed digital logistic map for parameter a, **a** two trajectories with different parameter a (The red line represents the trajectory with $a = 3.9$; the blue line represents the trajectory with $a = 3.9 + 2^{-12}$), **b** the difference between these two curves

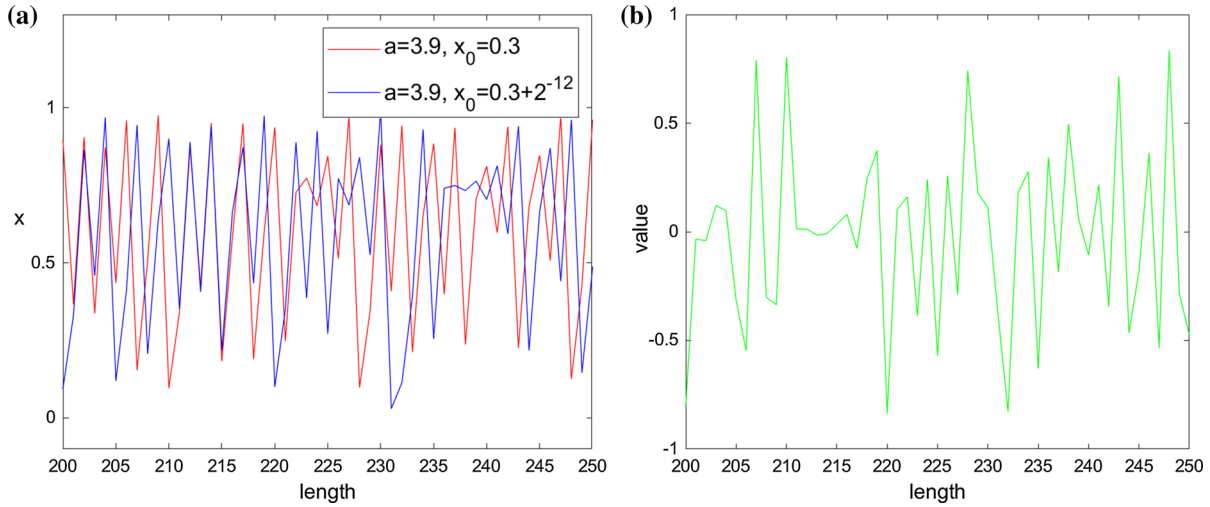

Fig. 17 Sensitivity analysis of the improved varying perturbed digital logistic map for initial value x_0, **a** two trajectories with different initial value x_0 (The red line represents the trajectory with $x_0 = 0.3$; the blue line represents the trajectory with $x_0 = 0.3 + 2^{-12}$), **b** the difference between these two curves

chaotic maps in other studies [35, 36, 40], the period cannot be detected since the largest precision be 2^{-20}, which is much better than the results in other remedies. The complexity (both ApEn and PE) can get an ideal level under a lower computing precision, et al. All these results show that the improved perturbation method has better performances in periodicity and complexity, which indicates that this method is quite competitive with other methods, especially for low computing precision.

Acknowledgements This work is supported by the National Natural Science Foundation of China (61862042), and the Innovation Special Fund Designated for Graduate Students of Jiangxi Province (YC2019-S101).

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

References

1. Alvarez, G., Montoya, F., Romera, M., Pasto, G.: Keystream cryptanalysis of a chaotic cryprographic method. Comput. Phys. Commun. **156**, 205–207 (2003)
2. Hamza, R.: A novel pseudo random sequence generator for image-cryptographic applications. J. Inf. Secur. Appl. **35**, 119–127 (2017)
3. Lambic, D., Nikolic, M.: Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dyn. **90**, 223–232 (2017)
4. Chen, J.X., Zhu, Z.L., Zhang, L.B., Zhang, Y.S., Yang, B.Q.: Exploiting self-adaptive permutation-diffusion and DNA random encoding for secure and efficient image encryption. Sig. Process. **142**, 340–353 (2017)
5. Li, X.W., Wang, Y., Wang, Q.H., Liu, Y., Zhou, X.: Modified integral imaging reconstruction and encryption using an improved SR reconstruction algorithm. Opt. Lasers Eng. **112**, 162–169 (2019)
6. Wang, X.Y., Li, Z.M.: A color image encryption algorithm based on Hopfield chaotic neural network. Opt. Lasers Eng. **115**, 107–118 (2019)
7. Zhao, H.M., Liu, H.D., Xu, J.J., Wu, D.: Performance prediction using high-order differential mathematical morphology gradient spectrum entropy and extreme learning machine. IEEE Trans. Instrum. Meas. **69**, 4165–4172 (2020)
8. Zhao, H.M., Zheng, J.J., Deng, W., Song, Y.J.: Semi-supervised broad learning system based on manifold regularization and broad network. IEEE Trans. Circuits Syst. I Regul. Pap. **67**, 983–994 (2020)
9. Deng, W., Liu, H.L., Xu, J.J., Zhao, H.M., Song, Y.J.: An improved quantum-inspired differential evolution algorithm for deep belief network. IEEE Trans. Instrum. Meas. **69**, 7319–7327 (2020)
10. Matthews, R.: On the derivation of a "chaotic" encryption algorithm. Cryptologia **13**, 29–42 (1989)
11. Rajagopalan, S., Poori, S., Narasimhan, M., Rethinam, S., Kuppusamy, C.V., Balasubramanian, R., Annamalai, V.M.P., Rengarajan, A.: Chua's diode and strange attractor: a three-layer hardware–software co-design for medical image confidentiality. IET Image Process. **14**, 1354–1365 (2020)
12. Wang, T., Wang, M.H.: Hyperchaotic image encryption algorithm based on bit-level permutation and DNA encoding. Opt. Laser Technol. **132**, 106355 (2020)
13. Yu, S.S., Zhou, N.R., Gong, L.H., Nie, Z.: Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. Opt. Lasers Eng. **124**, 105816 (2020)
14. Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A.M., Hirota, K., Abd El-Latif, A.A.: Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption. Inf. Sci. **515**, 191–217 (2020)
15. Ben Farah, M.A., Guesmi, R., Kachouri, A., Samet, M.: A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt. Laser Technol. **121**, 105777 (2020)
16. Ismail, S.M., Said, L.A., Radwan, A.G., Madian, A.H., Abu-ElYazeed, M.E.: A novel image encryption system merging fractional-order edge detection and generalized chaotic maps. Sig. Process. **167**, 107280 (2020)
17. Lambic, D.: A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dyn. **100**, 699–711 (2020)
18. Dogan, S.: A new data hiding method based on chaos embedded genetic algorithm for color image. Artif. Intell. Rev. **46**, 129–143 (2016)
19. Golomb, S.W.: Shift Register Sequences. Holden-Day, San Francisco, CA (1967)
20. Gustafson, H., Dawson, E., Nielsen, L., Caelli, W.: A computer package for measuring the strength of encryption algorithms. Comput. Secur. **13**, 687–697 (1994)
21. Hu, H.P., Xu, Y., Zhu, Z.Q.: A method of improving the properties of digital chaotic system. Chaos, Solitons Fractals **38**, 439–446 (2008)
22. Hu, H.P., Liu, L.F., Ding, N.D.: Pseudorandom sequence generator based on the Chen chaotic system. Comput. Phys. Commun. **184**, 765–768 (2013)
23. Jawad, L.M., Sulong, G.: Chaotic map-embedded Blowfish algorithm for security enhancement of colour image encryption. Nonlinear Dyn. **81**, 2079–2093 (2015)
24. Flores-Vergara, A., Inzunza-Gonzalez, E., Garcia-Guerrero, E.E., Lopez-Bonilla, O.R., Rodriguez-Orozco, E., Hernandez-Ontiveros, J.M., Cardenas-Valdez, J.R., Tlelo-Cuautle, E.: Implementing a chaotic cryptosystem by performing parallel computing on embedded systems with multiprocessors. Entropy **21**, 268 (2019)
25. Li, S.J., Chen, G.R., Mou, X.Q.: On the dynamical degradation of digital piecewise linear chaotic maps. Int. J. Bifurc. Chaos **15**, 3119–3151 (2004)
26. Wang, S.H., Liu, W.R., Lu, H.P., Kuang, J.Y., Hu, G.: Periodicity of chaotic trajectories in realizations of finite computer precisions and its implication in chaos communications. Int. J. Mod. Phys. B **18**, 2617–2622 (2004)
27. Cristina, D.A., Eugen, B.R.: A new method to improve cryptographic properties of chaotic discrete dynamical systems. In: 2012 International Conference for Internet Technology and Secured Transactions, pp. 60–65 (2012)
28. Zhou, Y.C., Hua, Z.Y., Pun, C.M., Chen, C.L.P.: Cascade chaotic system with applications. IEEE Trans. Cybern. **45**, 2001–2012 (2015)
29. Hua, Z.Y., Zhou, Y.C.: One-dimensional nonlinear model for producing chaos. IEEE Trans. Circuits Syst. I-Regul. Pap. **65**, 235–246 (2018)
30. Liu, L.F., Lin, J., Miao, S.X., Liu, B.C.: A double perturbation method for reducing dynamical degradation of the digital baker map. Int. J. Bifurc. Chaos **27**, 1750103 (2017)
31. Liu, Y.Q., Luo, Y.L., Song, S.X., Cao, L.C., Liu, J.X., Harkin, J.: Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation. Int. J. Bifurc. Chaos **27**, 1750033 (2017)
32. Deng, Y.S., Hu, H.P., Xiong, W., Xiong, N.N., Liu, L.F.: Analysis and design of digital chaotic systems with desirable performance via feedback control. IEEE Trans. Syst. Man Cybern.-Syst. **45**, 1187–1200 (2015)
33. Liu, L.F., Hu, H.P., Deng, Y.S.: An analogue-digital mixed method for solving the dynamical degradation of digital chaotic systems. IMA J. Math. Control Inf. **32**, 703–715 (2015)

34. Deng, Y.S., Hu, H.P., Xiong, N.X., Xiong, W., Liu, L.F.: A general hybrid model for chaos robust synchronization and degradation reduction. Inf. Sci. **305**, 146–164 (2015)
35. Liu, L.F., Liu, B.C., Hu, H.P., Miao, S.X.: Reducing the dynamical degradation by bi-coupling digital chaotic maps. Int. J. Bifurc. Chaos **28**, 1850059 (2018)
36. Liu, L.F., Miao, S.X.: Delay-introducing method to improve the dynamical degradation of a digital chaotic map. Inf. Sci. **396**, 1–13 (2017)
37. Pincus, S.M.: Approximate entropy as a measure of system complexity. Proc. Natl. Acad. Sci. **88**, 2297–2301 (1991)
38. Bandt, C., Pompe, B.: Permutation entropy: a natural complexity measure for time series. Phys. Rev. Lett. **88**, 174102 (2002)
39. Toomey, J.P., Kane, D.M.: Mapping the dynamic complexity of a semiconductor laser with optical feedback using permutation entropy. Opt. Express **22**, 1713–1725 (2014)
40. Liu, L.F., Miao, S.X.: A universal method for improving the dynamical degradation of a digital chaotic system. Phys. Scr. **90**, 085205 (2015)
41. Xiang, H.Y., Liu, L.F.: An improved digital logistic map and its application in image encryption. Multimedia Tools Appl. **79**, 30329–30355 (2020)