Nonlinear Dyn (2018) 94:1535–1546
https://doi.org/10.1007/s11071-018-4440-6

ORIGINAL PAPER

Applications of symbolic dynamics in counteracting the dynamical degradation of digital chaos

Jun Zheng · **Hanping Hu** · **Xiang Xia**

Received: 25 April 2018 / Accepted: 17 June 2018 / Published online: 4 July 2018

Abstract Chaotic systems which are realized on the finite precision devices suffer from dynamical degradation. In the literature, there does not seem to be good basis for designing schemes to reduce its negative influence on digital chaotic systems. Meanwhile, symbolic dynamics is often used to study the behaviors of complicated dynamical systems. In this paper, a new mechanism based on symbolic dynamics is proposed for designing effective schemes, in order to counteract the dynamical degradation of digital chaotic systems. A concrete scheme with hybrid structure is discussed to show significance of the mechanism. Symbolic dynamics are used to rigorously prove that a class of chaos-based digital systems can be perturbed to be chaotic again by a continuous chaotic system. Numerical experiments demonstrate that this scheme can recover the dynamical properties of original system, which is different from the existing remedies.

Keywords Chaotic system · Finite precision · Dynamical degradation · Symbolic dynamics

J. Zheng (✉) · H. Hu · X. Xia
School of Automation, Huazhong University of Science and Technology, Wuhan 430074, People's Republic of China
e-mail: zjhh@hust.edu.cn

H. Hu
e-mail: hphu@mail.hust.edu.cn

X. Xia
e-mail: 1360197186@qq.com

J. Zheng · H. Hu · X. Xia
State Key Laboratory of Cryptology, Beijing 100878, People's Republic of China

J. Zheng · H. Hu · X. Xia
Key Laboratory of Image Information Processing and Intelligent Control, Ministry of Education, Wuhan 430074, People's Republic of China

1 Introduction

As a scientific paradigm, chaos can provide the concepts and methods for analyzing the bizarre phenomena in various fields. Chaotic system has ergodicity, initial value sensitivity, pseudo-randomness, and long unpredictability. Thanks to these great properties, chaos theory has applications in many disciplines, including mathematics [1], physics [2], biology [3], ecology [4], engineering [5], and computer science [6]. When chaos is realized on finite precision device, however, these properties will become non-meaningful and equivocal, which are replaced by non-ergodicity, cycle length, degraded distribution, low linear-complexity, and strong correlation [7,8], that is, continuous chaos will collapse in finite fields eventually.

In order to improve the dynamical degradation of digital chaotic systems, assorted methods have been put forward as remedies and enhancements: (1) Using higher precisions [9,10], which can only increase the average cycle length but cannot even obtain a non-periodic orbit. In addition, this method has an increasing impact on implementation costs. (2) Cascading multiple chaotic systems [11,12], which can extend

the period of orbits because of complicated functional form. This method has such flaws as ignoring some other properties and doing no good to dynamical degradation. (3) Perturbing the chaotic systems. The "perturbation" means perturbing system variables, perturbing control parameters, or perturbing both [13]. Without regard to implementation details, the perturbation-based schemes may include methods such as switching multiple chaotic systems [14,15] and error compensation method [16]. Other aspect that should be considered is the perturbation sources: one class of perturbation source is generated under the same computing precision of digital chaotic system [13,17,18], the other perturbs the degenerate system under the same computing precision, which in addition has its own dynamic behavior [16,19]. Most of the perturbation schemes belong to the first case, which may greatly reduce the dynamical degradation of digital chaotic systems and easily meet the requirement standards of applications, whereas it is far from enough to solve the problem since the system is still not chaotic. In the second case, the majority do reduce the dynamical degradation of a digital chaotic map by means of generating new random sequences, which is completely different from the original chaotic map.

Symbolic dynamical system is a kind of high generalization and abstraction of the actual dynamical system, which is based on the topological conjugacy between continuous evolution of the dynamical system and a shift map on the space of sequences of integer numbers reflecting the state of the evolution [20–22]. When the actual dynamical system is difficult to be analyzed, symbolic dynamics can provide a promising direction.

Because of the lack of a systematic theory on digital chaotic systems, all the remedies above which attempt to purify digital chaotic systems by extending the period of orbits are mainly based on the engineering point of views. Although these approaches cannot fundamentally solve the problem, the second case in perturbation schemes extend the state space to infinity inadvertently, which might provide a great starting point. In this paper, a new mechanism based on symbolic dynamics is proposed to counteract the dynamical degradation of digital chaotic system. The steps of this mechanism are as follows: a new space with the cardinality of the continuum is introduced to extend the discrete space after which a suitable continuous function is defined and finally a topological conjugacy from the extended space to a chaotic shift map in symbolic dynamics is established. After steps above, the digital chaotic systems become chaotic again. At the same time, a concrete scheme with hybrid structure, in which a continuous chaotic system is chosen as perturbation source to extend the discrete state space and counteract the dynamical degradation is proposed based on this mechanism. The chaotic dynamics of perturbed digital system is discussed theoretically, and the experiment results conclude that dynamical properties of systems are preserved. Moreover, the perturbation do not completely disrupt the phase space of the original chaotic map indicating that the proposed mechanism can provide guidance for effective schemes for dealing with the dynamical degradation of digital chaotic systems. More suitable schemes for different applications based on the mechanism will be discussed in further researches.

The rest of this paper is organized as follows. The problem statement and preliminaries are given in Sect. 2. Section 3 introduces a new mechanism and a concrete scheme with a hybrid structure based on the mechanism, followed by rigorous proofs of the existence of chaotic motion in a class of perturbed digital systems. Section 4 illustrates an example to show the effectiveness of the scheme. Finally, Sect. 5 concludes the whole paper.

2 Preliminaries and basic results

In this section, there is a short description of the dynamical degradation of digital chaotic systems. A review of Devaney's chaos and some preliminary results of symbolic dynamics are also given.

2.1 Problem statement and notation

Consider a digital chaotic system:

$$x^i = F_N\left(x^{i-1}\right) = B_N\left(F\left(x^{i-1}\right)\right)$$

where $x^i = x^i_{P-1}x^i_{P-2}\ldots x^i_0 x^i_{-1}\ldots x^i_{-Q} \in X_N, N = P + Q$ is a digital state vector and X_N is the limited version of real subset $X \in \mathrm{R}^m$. $F : X \to X$ is a continuous chaotic map which is also suitable for X_N. $B_N : X \to X_N$ is a quantization function which makes the state space confined.

Actually, dynamical degradation of digital chaotic systems can be explained from all sides. From the point

of chaos dynamics, chaos is defined on a compact metric space, while in computer simulations a discrete lattice of points appear instead of a continuous compact phase space. From the point of orbits, the state space of digital chaotic map is finite. Any orbit might fall into a cycle, whose maximum period is equal to the cardinality of the state space. From the point of topology, the space has finite possible states; hence, the constructed topology is discrete. The ambiguous topology makes our understanding completely different from that in differentiable manifolds where the usual topology of the real numbers is defined. The incapability of remedies mentioned above will be shown later again (see Sect. 3.2).

2.2 Devaney's chaos

Consider a metric space (X, d) with metric d and a continuous function $f : X \to X$. Assuming that there exists a non-empty closed bounded subset A of X which is invariant under f, that is, $f^n(A) \in A$ for all $n \geq 0$. The most popular definition of chaos is due to Devaney [23], and let us recall it.

Definition 1 f is said to be chaotic on the invariant set A in the sense of Devaney if the following conditions are satisfied:

(1) f is topologically transitive, that is, for any two non-empty open subsets $U, V \subset A$ in the topology of (X, d), there exists $k \geq 0$ such that $f^k(U) \cap V \neq \varnothing$;
(2) The periodic points are dense in A;
(3) The property of sensitive dependence on initial conditions: there exists $\delta > 0$ such that, for any $x \in A$ and any neighborhood V of x, there exists $y \in V$ and $k \geq 0$ such that $\left| f^k(x) - f^k(y) \right| > \delta$.

This definition was discussed at length in the articles [23–26], published shortly after [23]. In [24], Banks et al. prove that the first two conditions can introduce the third condition in a metric space. However, the other conditions cannot derive transitivity nor the density of the periodic points as shown in [25]. Moreover, when attention is limited to maps on an interval, a stronger result is acquired in [26]: let f be a continuous map on a interval which is not necessarily finite, then transitivity is equivalent to Devaney's chaos.

2.3 Symbolic dynamics

Let (S, d) be a separable metric space, and card $(S) \geq 2$, where card $(\cdot)$ denotes cardinality of set. And it is natural to define the distance between two elements as follows: $d(a, b) \equiv |a - b|, \forall a, b \in S$. Let

$$\sum(S) = \prod_{i=0}^{+\infty} S_i, \quad S_i = S, \quad i = 0, 1, \ldots,$$

and define the metric on $\sum(S)$ from many possible choices as follows:

$$\rho(s, \bar{s}) = \sum_{i=0}^{+\infty} \frac{1}{2^i} \frac{d(s_i, \bar{s}_i)}{1 + d(s_i, \bar{s}_i)},$$

$$s = (s_0, s_1, \ldots), \bar{s} = (\bar{s}_0, \bar{s}_1, \ldots) \in \sum(S)$$

Apparently, the metric implies that if two symbolic sequences agree on a beginning long block, then they are sufficiently "close".

Proposition 1 *The space $\sum(S)$ with the metric has the following structure* [22]*: (1) compactness, (2) total disconnectivity, (3) completeness.*

Now that the structure of $\sum(S)$ is established, next denote by σ the shift map of $\sum(S)$ into itself:

$$\sigma((s_0, s_1, \ldots)) = (s_1, s_2, \ldots) \in \sum(S)$$

then $\left(\sum(S), \sigma\right)$ is a one-side symbolic dynamics.

The shift map σ is chaotic in the sense of Devaney and Li-Yorke, if S is a metric space with card $(S) \geq 2$ and S is separable [27].

Proposition 2 *The shift map σ defined above has sets of motions as follows:*

(1) a countable infinity of periodic orbits consisting of orbits of all cycles;
(2) uncountable non-periodic orbits;
(3) a dense orbit.

When analyzing the dynamics of a (X, f) is a daunting task, it is viable to find a simpler or familiar space which is topologically conjugate to (X, f).

Definition 2 f and h are topological conjugate (denoted $(X, f) \simeq (Y, h)$) if and only if $C : X \to Y$ is a homeomorphism such that the following diagram commutes.

$$\begin{array}{ccc} X & \xrightarrow{C} & Y \\ f \uparrow & & \uparrow h \\ X & \xrightarrow{C} & Y \end{array}$$

Which means that the relation $C \circ f = h \circ C$ holds.

Since topological conjugacy maintains the dynamics of a system, it is convenient to study a system with simpler dynamics by establishing a conjugacy from (X, f) to $\left(\sum(S), \sigma\right)$.

$$\begin{array}{ccc} X & \overset{C}{\rightarrow} & \Sigma(S) \\ f\uparrow & & \uparrow\sigma \\ X & \overset{C}{\rightarrow} & \Sigma(S) \end{array}$$

Definition 3 For $x \in X$, let $C(x) = s \in \sum(S)$, where $s = (s_0 s_1 \ldots)$, such that $f^i(x) \in X_{s_i}, \forall i \in N^*$, where X_S is a partition. Meanwhile $X_{s_0 s_1 s_2 \ldots} = \left\{x \left| x \in X_{s_0} \right.\right\} \cap \left\{x \left| f(x) \in X_{s_1} \right.\right\} \cap \left\{x \left| f^2(x) \in X_{s_2} \right.\right\} \cap \cdots \cap \cdots$.

Lemma 1 *Assume f is continuous, for $x, x' \in X, x \neq x'$, and there exists a sufficiently small value $\delta > 0$ for any $n \in N^*$, if $\left|x - x'\right| < \delta$, then $C(x), C\left(x'\right) \in (s_0 s_1 \ldots s_n)$.*

Proof Since $f : X \rightarrow X$ is continuous, it is easy to know that f^n (e.g., f^2 means $f \circ f$) is also continuous on X, then for any $n \in N^*$ and $\varepsilon > 0$, we can choose a $\delta > 0$, if $\left|x - x'\right| < \delta$, such that $\left|f^n(x) - f^n\left(x'\right)\right| < \varepsilon$. That is to say, when ε is sufficiently small, $f^n(x), f^n\left(x'\right)$ are in the same set of the partition, therefore $C(x), C\left(x'\right) \in (s_0 s_1 \ldots s_n)$. □

Theorem 1 *Assume that the function $C : X \rightarrow \sum(S)$ is defined as in Definition 3. If C is injective and surjective, besides f is continuous, then C is bicontinuous.*

Proof (a) Since C is injective, for any $x, x' \in X, x \neq x'$, $C(x) \neq C\left(x'\right)$ holds. Next, for any $\varepsilon > 0$, we can choose $n \in N^*$ such that $\varepsilon > \frac{1}{2^n}$, then according to Lemma 1 For $x \in X$, where $C(x) = (s_0 s_1 s_2 \ldots s_n \ldots)$, choose $\delta(\varepsilon) > 0$ such that if $d(x, y) < \delta(\varepsilon)$, $C(y) = (s_0 s_1 s_2 \ldots s_n)$. Then $\rho(C(x), C(y)) = \sum_{i=n+1}^{+\infty} \frac{1}{2^i} \frac{d(s_i, \bar{s}_i)}{1+d(s_i, \bar{s}_i)} < \frac{1}{2^n} < \varepsilon$. So C is continuous;

(b) Since C is surjective, for any $(s_0 s_1 s_2 \ldots s_n \ldots) \in \sum(S)$, there is at least one element $x \in X$ such that $C(x) = (s_0 s_1 s_2 \ldots s_n \ldots)$. Next, for any $\varepsilon > 0$, we can choose $n \in N^*$ which satisfies $C((x, \varepsilon)) = (s_0 s_1 s_2 \ldots s_n \ldots) \in X_{s_0 s_1 s_2 \ldots s_n}$ such that if $\rho(C(x), C(y)) < \delta(\varepsilon) < \frac{1}{2^n}$, that means $C(y) = (s_0 s_1 s_2 \ldots s_n)$, obviously, $y \in (x, \varepsilon)$, then C^{-1} is continuous as well; □

From the above, C is bicontinuous.

Let us recall the topological conjugacy, by appropriately chosen $\left(\sum(S), \sigma\right)$, C is well defined and commutes f to σ. It is enough to show that C is a topological conjugacy when C is injective and surjective. Furthermore, f is continuous, which is easily obtained.

3 The mechanism based on symbolic dynamics

In spite of many papers centering on analyses of digital chaotic systems from both academic and practical perspective, a mature digitization-analysis theory has not been constructed until now. Moreover, many research results just play a role of improving the dynamical degradation of digital chaotic systems. In the section, we give a brief presentation of diverse remedies and attempt to make clear from a new perspective that how dynamical degradation of digital chaotic systems occurs and how to purify digital chaos.

3.1 A new feasible mechanism for chaos degradation

When a chaotic map is realized on a finite precision device, the state space become finite, denoted by X_N, where N is the computing precision, and card $(X_N) = 10^N$, then the function $C : X_N \rightarrow \sum(S)$ is only injective without surjective property, which cannot be a topological conjugacy, the dynamical degradation is seen**.** Intuitively, on the finite state space, the degenerate system possess only finite periodic orbits (including fixed points), without non-periodic orbits and dense orbits.

A new feasible mechanism is proposed in this paper: First, we introduce a new system to extend the finite state space. The state space of new system has cardinality of the continuum. The extended state space is denoted by $\bar{X}_N$. If the discrete space can be extended to infinite, or rather, card $\left(\bar{X}_N\right) = \text{card}\left(\sum S\right) = \aleph$, the prerequisite is satisfied. Then by defining a suitable continuous function C, and establishing a topological conjugacy from $\left(\bar{X}_N, f_F\right)$ to $\left(\sum(S), \sigma\right)$, such that $\left(\bar{X}_N, f_F\right)$ is a chaotic system, and the problem of dynamical degradation of digital chaos is fundamentally solved

Remarkably, there are three sufficient conditions to judge if a scheme fit our mechanism and can truly counteract the dynamical degradation. The prerequisite is that the extended space must have cardinality of

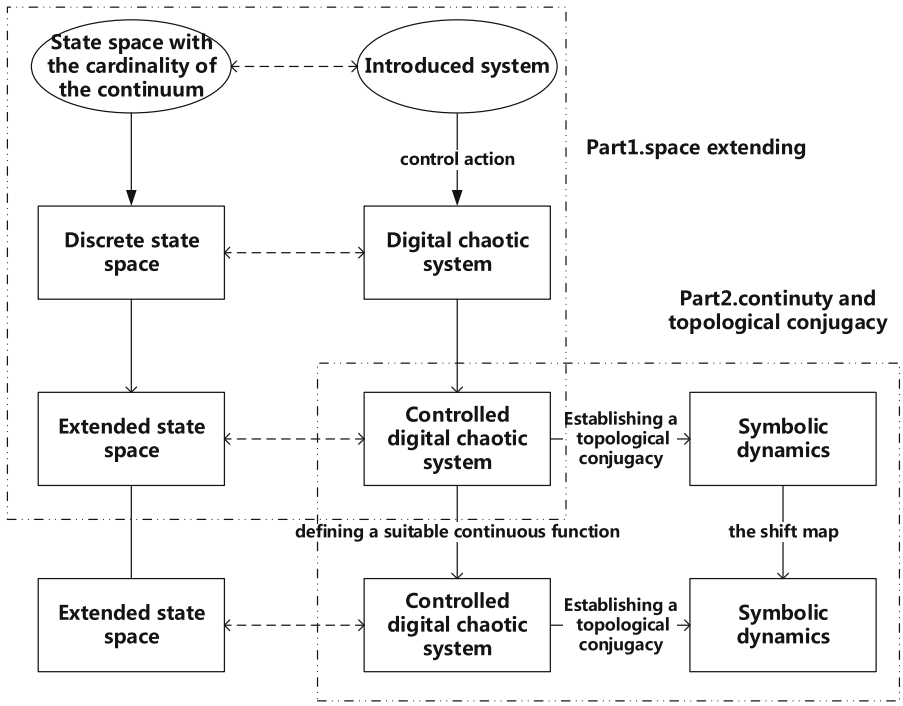

Fig. 1 Basic framework of our mechanism

the continuum, without which next steps are meaningless. If the cardinality of extended space is countable, the introduced system might be chosen wrongly. To meet the second condition, that the function defined must be continuous, scholars need some engineering experience. Because the inappropriate control action cannot satisfy the continuity condition. The last one is exactly what we need. If a topological conjugacy cannot be established, the continuous function defined is not chaotic. The basic framework of our mechanism is shown in Fig. 1.

3.2 Differences the remedies

In Sect. 1, three possible methods for dynamical degradation of digital chaotic systems have been introduced: using higher precisions; cascading multiple chaotic systems; perturbing the chaotic systems. Actually, all these methods aim at extending the state space, which coincide with our mechanism. The differences between them are to be uncovered.

Theorem 2 *For any non-empty set A and B, the cardinality of the Cartesian product $A \times B$ is equal to the product of the cardinalities of both A and B. That is, $card(A \times B) = card(A) \cdot card(B)$, naturally, $card(A \times B \times C) = card(A) \cdot card(B) \cdot card(C)$ and so on.*

Proof Obviously, every element of A is paired with every element of B. Then every pair makes up one element of the Cartesian product. Therefore, $\text{card}(A \times B) = \text{card}(A) \cdot \text{card}(B)$, similarly, $\text{card}(A \times B \times C) = \text{card}(A) \cdot \text{card}(B) \cdot \text{card}(C)$ is gained. □

Remark Assume that one of the input sets is infinite (countably and uncountably) and other sets are not empty sets, $\text{card}(A \times B) = \max\{\text{card}(A), \text{card}(B)\}$ holds.

Corollary 1 *If either A or B is uncountably infinite and the other is not the empty set. the set $A \times B$ is uncountably infinite.*

For the convenience of illustration, we introduce a new space Y to extend the state space of digital chaotic systems, which can mirror the effects of various methods on digital chaotic systems, then all the ordered pairs (x_i, y) where $x_i \in X_N$ and $y \in Y$ consist in the Cartesian product $\bar{X}_N = X_N \times Y$.

Using higher precision means the introduced space $Y = X_{M-N}$, where M is the higher computing precision, according to Theorem 2, $\text{card}(X_N \times X_{M-N}) = 10^M$. Cascading multiple chaotic systems can extend

the period of chaotic orbits. Notably, when cascading the seed chaotic maps, we must do normalization transforms. By this means, the range of one map matches the domain of its succeeder. The normalization stage keeps the same discrete space. Therefore, what actually effects is that the function $f_F : \bar{X}_N \to \bar{X}_N$ becomes more complicated by cascading multiple chaotic systems. It is also the reason that this method cannot guarantee some other property. As for the perturbation-based solution, we first divide the perturbation sources into two classes. One class of perturbation source is generated under the computing precision of the degenerate system. Most perturbation-based methods belong to this class. According to Theorem 2, the introduced space $Y = X_N$, then card $(X_N \times X_N) = 10^{2N}$. It may explain that the perturbation-based solution is indeed better than the other two. However, dynamical degradation is still only reduced greatly. It is far not enough to solve the problem of dynamical degradation of digital chaos. The other class of perturbation source perturbs the degenerate system under the same computing precision. Nevertheless, it has its own dynamic behavior such as random number [19], which may be a feasible idea. According to Corollary 1, the introduced space is uncountably infinite, so card $(X_N \times Y) = \aleph$.

For the first three methods, although the introduced spaces are different, the extended state space is finite. Because the cardinality of extended state space is smaller than the cardinality of symbolic space, namely card $\left(\bar{X}_N\right) <$ card $\left(\sum S\right) = \aleph$. This common point causes failing to establish the suitable function C with injective and surjective property. Fortunately, the last route that satisfied card $(X_N \times Y) =$ card $\left(\sum S\right) = \aleph$ seems promising. The rest is to define a suitable function C and establish a topological conjugacy from $\left(\bar{X}_N, f_F\right)$ to $\left(\sum(S), \sigma\right)$, such that $\left(\bar{X}_N, f_F\right)$ is a chaotic system.

3.3 Concrete scheme

In this section, a scheme is put forward for solving the dynamical degradation of digital chaotic systems. The digital chaotic system has been defined in Sect. 2.1. In our method, we choose a continuous chaotic system as perturbation source to extend the discrete state space. The continuous chaotic system has the form as follows:

$$y' = G(y)$$

Whose state space is Y. Then the extended state space is $\bar{X}_N = X_N \times Y$. Defining the function:

$$F : \bar{X}_N \to X_N$$
$$\left(x^i, y^i\right) \mapsto \left(x^i + \tfrac{1}{10^Q} h\left(x^i, y^i\right)\right)$$

here $h\left(x^i, y^i\right)$ is the perturbation function:

$$h\left(x^i, y^i\right) = \begin{cases} 1, & \left(y^i - x^i\right) \times 10^Q \bmod 1 \geq 0.5 \\ 0, & \left(y^i - x^i\right) \times 10^Q \bmod 1 < 0.5 \end{cases}$$

where x^i is the state of perturbed system, y^i denotes the sampled output of continuous chaotic system, and Q denotes the decimal width of computing precision. Then defining the map on $\bar{X}_N = X_N \times Y$:

$$f : \bar{X}_N \to X_N$$
$$\left(x^i, y^i\right) \mapsto \left(F_G\left(x^i, y^i\right), y^{i+1}\right)$$

It is noteworthy that the evolution of a continuous chaotic system appears as a component of our scheme. Before establishing a topological conjugacy from $\left(\bar{X}_N, f\right)$ to $\left(\sum(S), \sigma\right)$, f_F must be continuous in the extended space $\bar{X}_N = X_N \times Y$. We first define a new distance between two points $P = (x, y)$, $\widehat{P} = \left(\widehat{x}, \widehat{y}\right) \in \bar{X}_N$, by

$$d\left(P, \widehat{P}\right) = d_x\left(x, \widehat{x}\right) + d_y\left(y, \widehat{y}\right) = \sum_{k=1}^{N} \delta\left(x_k, \widehat{x}_k\right) + \left|y - \widehat{y}\right|$$

Theorem 3 *f_F is a continuous function.*

Proof We use the definition of continuity in topological space. Let $2^{X_N} = \{S \,|\, S \subseteq X_N\}$ be the power set of X_N, $U = \{(x, y) \,|\, x \in S, y \in (a, b) \subseteq Y\}$ be an arbitrary subset. For a point $P' = \left(x', y'\right) \in U$, an a sufficiently small value $\varepsilon_1 > 0$, the spherical neighborhood of P' denotes by $B\left(P', \varepsilon_1\right) = \left\{P \in \bar{X}_N \,\middle|\, d\left(P, P'\right) < \varepsilon_1\right\}$. In fact, $d_x\left(x, \widehat{x}\right)$ is an integer, so in the spherical neighborhood, $d_x\left(x, \widehat{x}\right) = 0$ holds. Let $\varepsilon = \min\{y - a, b - y, \varepsilon_1\}$, such that $B\left(P', \varepsilon\right) \subset U$, therefore, U is an open set, all the open sets construct a topology. We will prove that $f_F^{-1}(U)$ is an open set in U. Let us recall the perturbation function $h\left(x^i, y^i\right)$, then $f_F^{-1}(U) = \left\{(x, y) \,\middle|\, x - \frac{1}{10^Q} \in S, y \in G^{-1}(a, b) \subseteq Y\right\}$ or $f_F^{-1}(U) = \left\{(x, y) \,\middle|\, x \in S, y \in G^{-1}(a, b) \subseteq Y\right\}$. Considering that G is continuous, then $f_F^{-1}(U)$ in either case is still an open set. To sum up, f_F is consequently continuous. □

Since we have extended the state space, the function C defined in Definition 3 must be redefined as follows.

Definition 4 For $P \in \bar{X}_N$, let $\bar{C}(P) = s \in \sum(S)$, where $s = (s_0 s_1 \ldots)$, such that $F_G\left(f_F^i(P)\right) \in X_{s_i}, \forall i \in N^*$, where X_S is a partition on X_N, meanwhile $\bar{X}_S$ is a partition on $\bar{X}_N$, $\bar{X}_{s_0 s_1 s_2 \ldots} = \left\{P \left| F_G(P) \in X_{s_0}\right.\right\} \cap \left\{P \left| F_G(f_F(P)) \in X_{s_1}\right.\right\} \cap \left\{P \left| F_G\left(f_F^2(P)\right) \in X_{s_2}\right.\right\} \cap \cdots \cap \cdots$.

Theorem 4 *For $P, P' \in \bar{X}_N, P \neq P'$, and there exists a sufficiently small value $\delta > 0$ for any $n \in N^*$, if $\left|P - P'\right| < \delta$, then $\bar{C}(P), \bar{C}\left(P'\right) \in (s_0 s_1 \ldots s_n)$*

Proof According to Lemma 1 and Theorem 3, this theorem is clearly true. □

Theorem 5 $\left(\bar{X}_N, f_F\right) \simeq \left(\sum(S), \sigma\right)$.

Proof Let $\bar{C}(P)$ be defined as in Definition 4. Then $\bar{C}(P)$ is well defined. First we will prove that $\bar{C}(P)$ is bicontinuous.

Injective For $P, P' \in \bar{X}_N, P \neq P'$, such that $f_F^n(P), f_F^n\left(P'\right)$ are defined for all $n \in N^*$. Different situations are discussed: (1) $x = x', y \neq y'$, since G is a chaotic map, G has sensitive dependence on initial conditions. Then, for $y, y', \left(y - y'\right) \times 10^Q \bmod 1 < 0.5$, there exists $n \in N^*$, such that $\left(y^n - y^{n'}\right) \times 10^Q \bmod 1 > 0.5$, then it is easy to verify that $F_G\left(f_F^n(P)\right) \neq F_G\left(f_F^n\left(P'\right)\right)$, so they must lie in different orbits, that is, $\bar{C}(P) \neq \bar{C}\left(P'\right)$. (2) $x \neq x', y = y'$, openly, $F_G\left(f_F^n(P)\right) \neq F_G\left(f_F^n\left(P'\right)\right)$. (3) $x \neq x', y \neq y'$, in this case, after a couple of iterations, this case is reduced to case (1). Therefore $\bar{C}(P)$ is one-to-one.

Surjective Let $s = (s_0, s_1, \ldots)$. Consider the period $\bar{X}_{s_0} = \left\{P \left| F_G(P) \in X_{s_0}\right.\right\}$. According to the definition of $h\left(x^i, y^i\right)$, there exists an open set $(a, b) \in Y$, and $x \in X_{s_0}$, such that $X_{s_0} \times (a, b) \subseteq \bar{X}_{s_0}$. Since (a, b) is isomorphic to $R\ (x \in (a, b) \mapsto \tan\left(\frac{\pi}{2}\left(\frac{2x-b-a}{b-a}\right)\right)$ is an isomorphism), for $\bar{X}_{s_0 s_1 s_2 \ldots}$, there is at least one element P in $\bar{X}_N$ such that $\bar{C}(P) \in (s_0 s_1 \ldots s_n)$, so $\bar{C}(P)$ is onto. □

By Theorem 1 $\bar{C}(P)$ is bicontinuous. Last but not least, by Definition 2 the following diagram commutes:

$$\begin{array}{ccc} \bar{X}_N & \overset{C}{\rightarrow} & \sum(S) \\ f_F \uparrow & & \uparrow \sigma \\ \bar{X}_N & \overset{C}{\rightarrow} & \sum(S) \end{array}$$

Therefore, we conclude that f_F is chaotic in the sense of Devaney and Li-Yorke on $\bar{X}_N = X_N \times Y$.

4 Example and simulations

Logistic map is one of the most widely used 1-D discrete chaotic maps in many applications. In this section, Logistic chaotic map is studied as an example to show the role of the proposed hybrid method. Mathematically, consider the following logistic chaotic map realized on the finite precision device:

$$x^i = B_N\left(ax^{i-1}\left(1 - x^{i-1}\right)\right), \tag{1}$$

where a is the control parameter with range of [3.57, 4], and it has more complex chaotic behaviors when a approaches to 4. Since the Logistic map has unpredictable trajectories and good ergodicity in the interval [0, 1], B_N keeps N significant and confines all the states in the finite set as follows:

$$X_N = \left\{x \left| x = k \times \frac{1}{10^N}, k = 0, 1, 2, \ldots, 10^N - 1\right.\right\}$$

On the other side, as a perturbation source, Lorenz system is applied to extend the discrete state space:

$$\begin{cases} \dot{\bar{x}} = \sigma(\bar{y} - \bar{x}) \\ \dot{\bar{y}} = \rho\bar{x} - \bar{y} - \bar{x}\bar{z} \\ \dot{\bar{z}} = \bar{x}\bar{y} - \beta\bar{z} \end{cases}$$

which is chaotic when parameters $\sigma = 10$, $\rho = 30$ and $\beta = \frac{8}{3}$. Then the perturbed digital logistic map can be represented as:

$$x^i = B_N\left(ax^{i-1}\left(1 - x^{i-1}\right)\right) + \frac{1}{10^N}h\left(x^i, y^i\right) \bmod 1, \tag{2}$$

Next, several indicators are analyzed to appraise the behavior of the perturbed digital logistic map. The quantization function is chosen as $B_N(\cdot) = round(\cdot)$.

4.1 Trajectories and phase diagrams

The precision is set at 10^{-3} and 10^{-6} (denoted by $N = 3$ and $N = 6$), respectively. Let $a = 4$, the

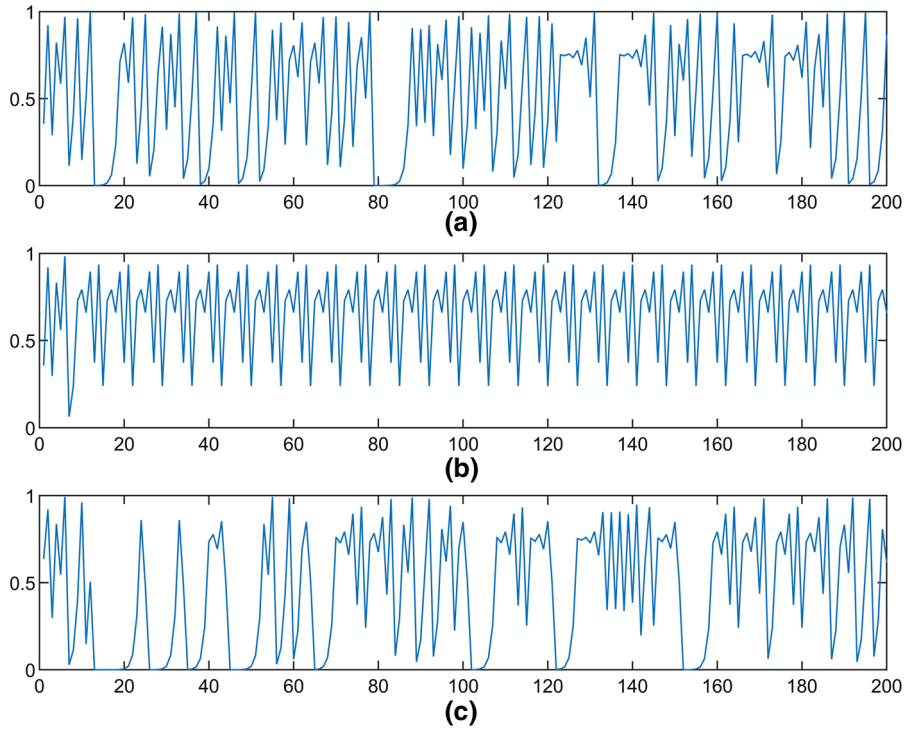

Fig. 2 Trajectories of three comparative systems. **a** The chaotic trajectory of original logistic map with initial value $x_0 = 0.1$. **b**, **c** The trajectories of digital Logistic map and perturbed map with precision $N = 3$ and the same initial value $x_0 = 0.1$

initial value $x_0 = 0.1$ for both Eqs. (1) and (2). The trajectories of two maps with different precisions are shown in Figs. 2 and 3. Figure 2 shows that the trajectory of Eq. (1) quickly falls into a cycle; conversely, the trajectory of Eq. (2) behaves chaotically again after being perturbed. As the precision increases, the trajectory of Eq. (1) falls into a cycle more slowly. The red box in Fig. 3b clearly shows that cycle appears. However, Eq. (2) still behaves chaotically, as Fig. 3c shows. As we all know, Logistic chaotic map has a parabolic attractor. All the subplots in Fig. 4 show relatively complete retention of parabolic attractor, indicating that the perturbed Logistic map in Eq. (2) revert to the original version of the phase diagram to a great extent.

4.2 Autocorrelation analysis

The analysis of autocorrelation is a mathematical tool when testing randomness. For ideal random sequences, the autocorrelation should be delta function. The autocorrelation of ideal Logistic chaotic map is similar to delta function. The precision is set at $N = 6$. When the sequences are confined to finite state space, the correlation of a trajectory with a delayed copy becomes strong, which causes the system vulnerable to correlation attack, as shown in Fig. 5a. Figure 5b shows, after being perturbed, the correlation of outputs is driven to be delta-like again. This result shows that the hybrid method can restore ideal chaotic feature.

4.3 Frequency distributions

Logistic chaotic map has a U type invariant density function, as shown in Fig. 6a. In order to compare the distributions of digital Logistic maps before (Fig. 6b) and after (Fig. 6c) perturbed, we divide the whole interval [0,1] into 256 equal subintervals. Figure 6b shows that the density function is destroyed with obvious jagged edges appearing. The distribution becomes worse due to finite precision, which is set at $N = 6$. After being perturbed, the degraded distribution can be restored to become U type function, which is even smoother. Therefore, frequency attacks can be effectively resisted in the proposed hybrid method.

4.4 Approximate entropy

Further, we investigate the complexity of three comparative systems via approximate entropy, which was

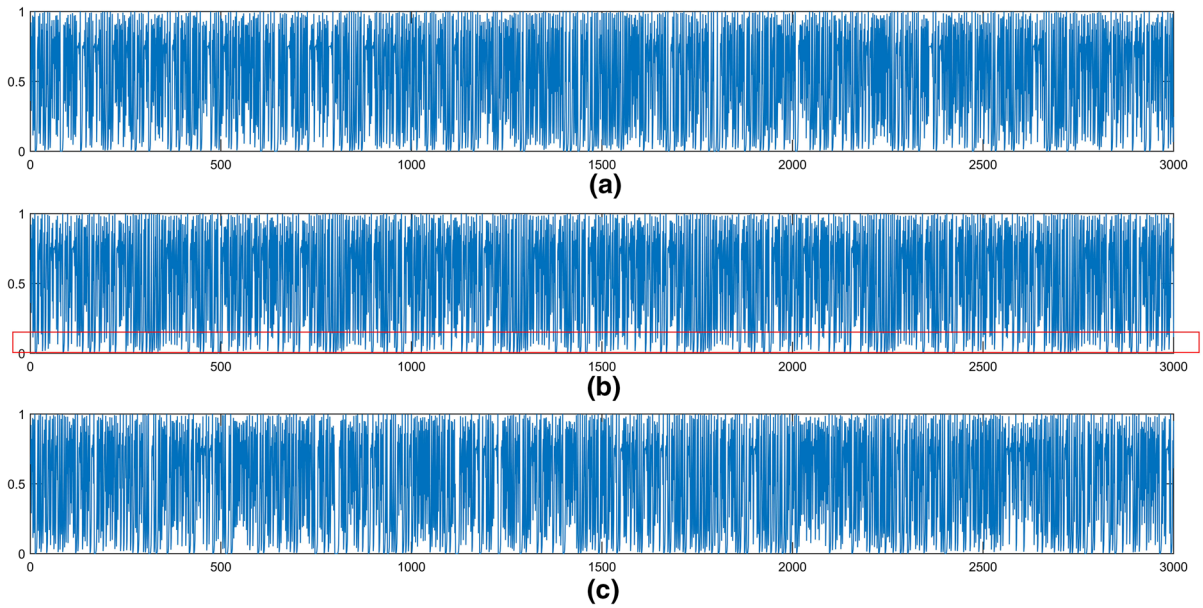

Fig. 3 Trajectories of three comparative systems. **a** The chaotic trajectory of original logistic map with initial value $x_0 = 0.1$. **b**, **c** the trajectories of digital Logistic map and perturbed map with precision $N = 6$ and the same initial value $x_0 = 0.1$

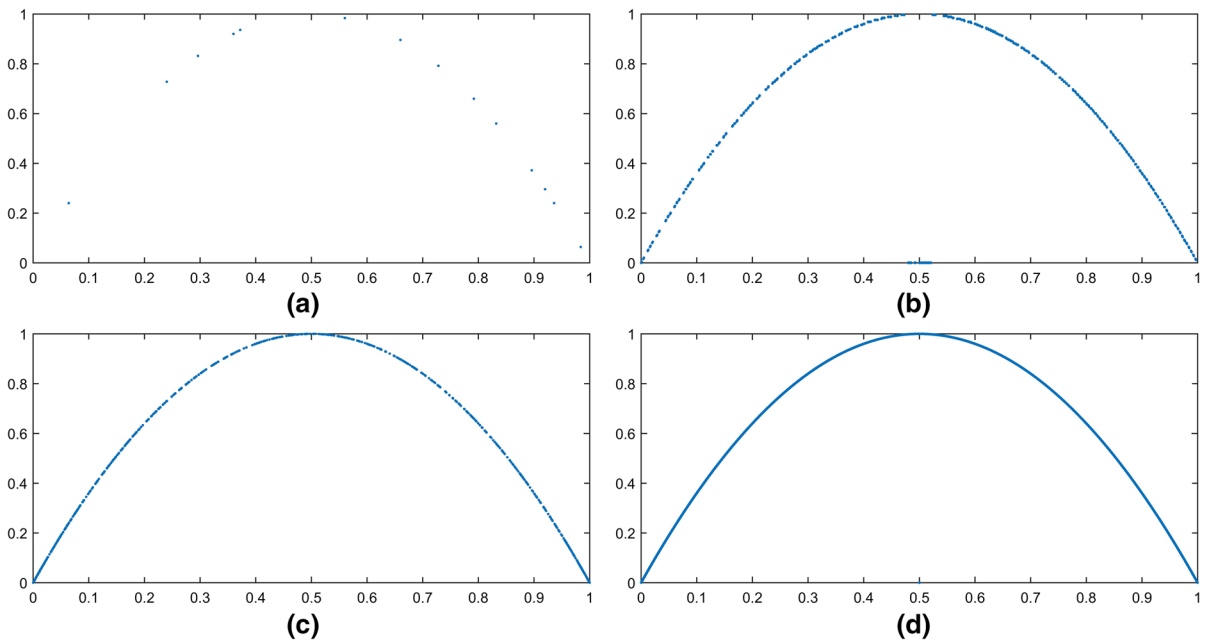

Fig. 4 Phase diagrams of digital Logistic map before (left column) and after (right column) being perturbed with the same initial value $x_0 = 0.1$ and different computing precisions

proposed by Pincus [28], is a technique used to quantify the amount of regularity and unpredictability of fluctuations over time series data. Figure 7 shows that the approximate entropy of digital Logistic map remains in a small range at first; then, it increases significantly and converges to that of the original Logistic chaotic map as the precision increases. However, the approximate entropy in our scheme fluctuates around that of

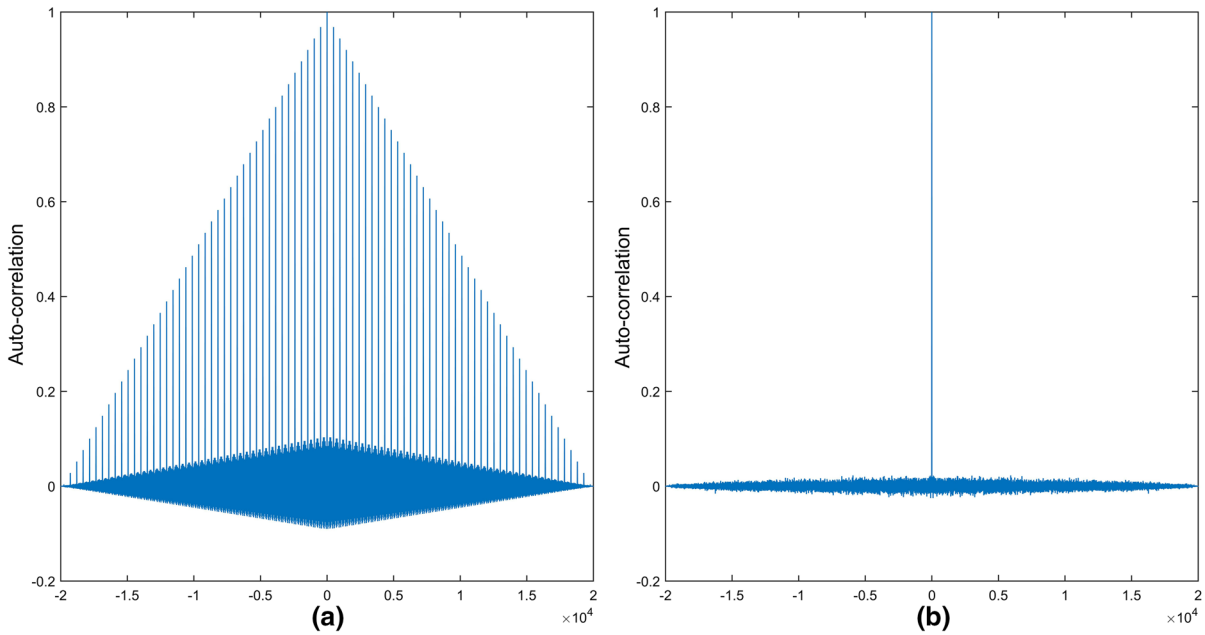

Fig. 5 Autocorrelation functions of outputs of **a** Eq. (1) and **b** Eq. (2) with the same initial value $x_0 = 0.1$ and computing precision $N = 6$

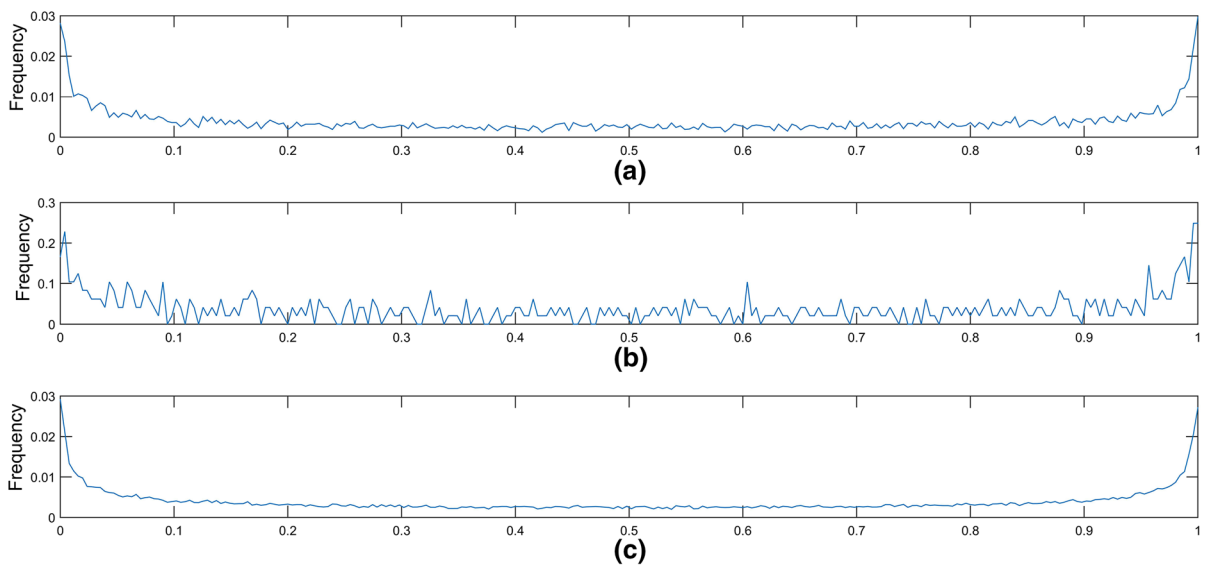

Fig. 6 Frequency distributions of three comparative systems. **a** The original logistic map with initial value $x_0 = 0.1$. **b**, **c** the frequency distributions of digital Logistic map and perturbed map with computing precision $N = 6$ and the same initial value $x_0 = 0.1$

the Logistic chaotic map even in low precisions. After carefully observing the sequences in low precisions, we find that 0's appears a lot. This inevitable phenomena caused by low precisions can explain the fluctuation mentioned above. Actually, the approximate entropy of the perturbed digital Logistic map is a little larger than that of the Logistic chaotic map as the precision increases, which implies the validity of our scheme to solve the dynamical degradation of digital chaotic systems.

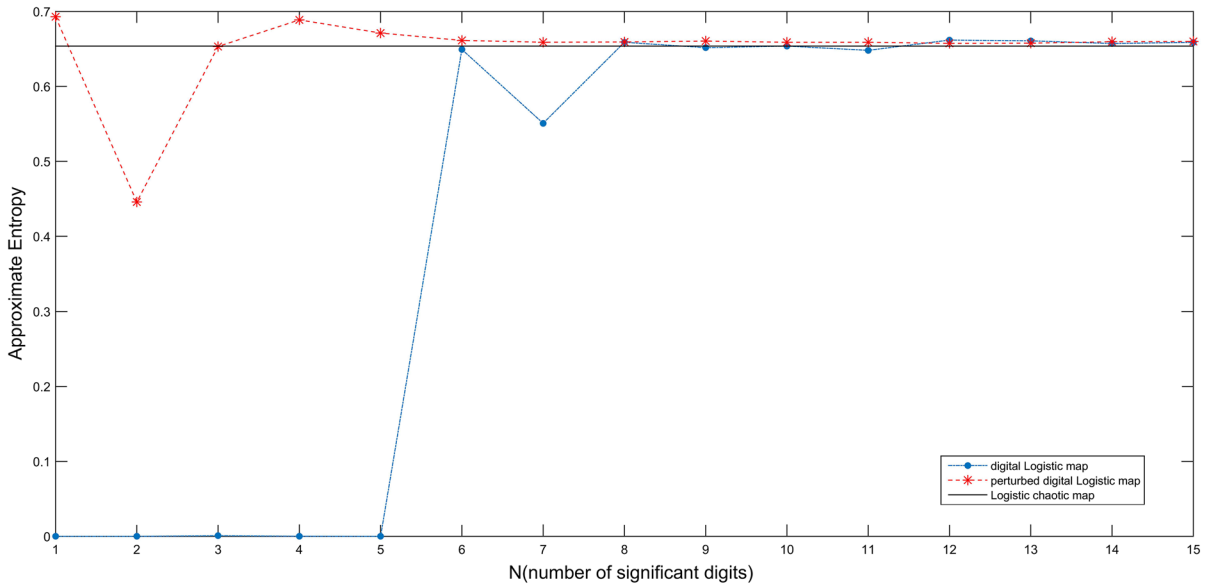

Fig. 7 Approximate entropy values of three comparative systems under different number of significant digits with the same initial value $x_0 = 0.1$

5 Conclusions

In this paper, a new mechanism, which can provide guidance for effective schemes for dealing with the dynamical degradation of digital chaotic systems is proposed. The mechanism mainly includes two aspects. One is extending discrete state space by introducing a space with cardinality of the continuum, the other is defining a suitable continuous function and establishing a topological conjugacy from the extended space to a chaotic shift map in symbolic dynamics. Based on the mechanism, it is rigorously proven that a class of chaos-based digital systems can be perturbed to be chaotic again by a continuous chaotic system. Simulation results show that the perturbation well preserve the complexity, the ergodicity of orbits, distribution and other statistical properties of the original chaotic systems. Last but not least, the mechanism proposed in this paper can direct to design more suitable schemes to counteract dynamical degradation for different application scenarios.

Acknowledgements This work was supported in part by the National Key R&D Program of China under Grant 2017YFB0802000, in part by the Cryptography Theoretical Research of National Cryptography Development Fund under Grant MMJJ20170109, in part by the Open Research Fund of State Key Laboratory of Cryptology under Grant MMKFKT201613, and in part by the Independent Innovation Fund of Huazhong University of Science and Technology under Grant 2016YXMS067.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest concerning the publication of this manuscript.

References

1. Kennedy, J., Kocak, S., Yorke, J.A.: A chaos lemma. Am. Math. Mon. **108**(5), 411–423 (2001). https://doi.org/10.2307/2695795
2. Wu, G.-C., Baleanu, D.: Discrete fractional logistic map and its chaos. Nonlinear Dyn. **75**(1–2), 283–287 (2014). https://doi.org/10.1007/s11071-013-1065-7
3. Coffey, D.S.: Self-organization, complexity and chaos: the new biology for medicine. Nat. Med. **4**(8), 882–885 (1998). https://doi.org/10.1038/nm0898-882
4. Bednekoff, P.A., Lima, S.L.: Randomness, chaos and confusion in the study of antipredator vigilance. Trends Ecol. Evolut. **13**(7), 284–287 (1998). https://doi.org/10.1016/s0169-5347(98)01327-5
5. Sudret, B.: Global sensitivity analysis using polynomial chaos expansions. Reliab. Eng. Syst. Saf. **93**(7), 964–979 (2008). https://doi.org/10.1016/i.ress.2007.04.002
6. Li, S.J., Mou, X.Q., Cai, Y.L., Ji, Z., Zhang, J.H.: On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision. Comput. Phys. Commun. **153**(1), 52–58 (2003). https://doi.org/10.1016/s0010-4655(02)00875-5

7. Blank, M.: Pathologies generated by round-off in dynamical systems. Physica D **78**(1–2), 93–114 (1994)
8. Li, S.J., Chen, G.R., Mou, X.Q.: On the dynamical degradation of digital piecewise linear chaotic maps. Int. J. Bifurc. Chaos **15**(10), 3119–3151 (2005). https://doi.org/10.1142/s0218127405014052
9. Lin, T., Chua, L.O.: On chaos of digital filters in the real world. IEEE Trans. Circuits Syst. **38**(5), 557–558 (1991)
10. Wheeler, D.D., Matthews, R.A.J.: Supercomputer investigations of a chaotic encryption algorithm. Cryptologia **15**(2), 140–152 (1991)
11. Heidari-Bateni, G., Mcgillem, C.D.: Chaotic direct-sequence spread-spectrum communication system. IEEE Trans. Commun. **42**(234), 1524–1527 (1994)
12. Zhou, Y., Hua, Z., Pun, C.-M., Chen, C.L.P.: Cascade chaotic system with applications. IEEE Trans. Cybern. **45**(9), 2001–2012 (2015). https://doi.org/10.1109/tcyb.2014.2363168
13. Liu, L., Lin, J., Miao, S., Liu, B.: A double perturbation method for reducing dynamical degradation of the digital baker map. Int. J. Bifurc. Chaos **27**(7), 1750103 (2017)
14. Jallouli, O., El Assad, S., Chetto, M., Lozi, R.E., Caragata, D., IEEE: a novel chaotic generator based on weakly-coupled discrete skewtent maps. In: 2015 10th International Conference for Internet Technology and Secured Transactions, pp. 38–43 (2015)
15. Wu, Y., Zhou, Y., Bao, L.: Discrete wheel-switching chaotic system and applications. IEEE Trans. Circuits Syst. I Regul. Pap. **61**(12), 3469–3477 (2014). https://doi.org/10.1109/tcsi.2014.2336512
16. Hu, H., Deng, Y., Liu, L.: Counteracting the dynamical degradation of digital chaos via hybrid control. Commun. Nonlinear Sci. Numer. Simul. **19**(6), 1970–1984 (2014). https://doi.org/10.1016/j.cnsns.2013.10.031
17. Liu, Y., Luo, Y., Song, S., Cao, L., Liu, J., Harkin, J.: Counteracting dynamical degradation of digital chaotic chebyshev map via perturbation. Int. J. Bifurc. Chaos (2017). https://doi.org/10.1142/s021812741750033x
18. Liu, L., Miao, S.: Delay-introducing method to improve the dynamical degradation of a digital chaotic map. Inf. Sci. **396**, 1–13 (2017)
19. Wang, Q., Yu, S., Li, C., Lu, J., Fang, X., Guyeux, C., Bahi, J.M.: Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems. IEEE Trans. Circuits Syst. I Regul. Pap. **63**(3), 401–412 (2016). https://doi.org/10.1109/tcsi.2016.2515398
20. Misiurewicz, M., Stimac, S.: Symbolic dynamics for Lozi maps. Nonlinearity **29**(10), 3031–3046 (2016). https://doi.org/10.1088/0951-7715/29/10/3031
21. Hao, B.L., Liu, J.X., Zheng, W.M.: Symbolic dynamics analysis of the Lorenz equations. Phys. Rev. E **57**(5), 5378–5396 (1998). https://doi.org/10.1103/PhysRevE.57.5378
22. Wiggins, S.: Global Bifurcations and Chaos. Springer, Berlin (1988)
23. Chillingworth, D.R.J.: An Introduction to Chaotic Dynamical Systems by Robert L. Devaney. Benjamin/Cummings, San Francisco (1986)
24. Kolesov, A.Y., Rozov, N.K.: On the definition of 'chaos'. Rus. Math. Surv. **64**(4), 701–744 (2009). https://doi.org/10.1070/RM2009v064n04ABEH004631
25. Assaf IV, D., Gadbois, S.: Definition of chaos. Am. Math. Mon. **99**(9), 865 (1994)
26. Vellekoop, M., Berglund, R.: On intervals, transitivity = chaos. Am. Math. Mon. **101**(4), 353–355 (1994)
27. Chou, X.C., Fu, X.C.: Chaotic behaviour of the general symbolic dynamics. Appl. Math. Mech. **13**(2), 117–123 (1992)
28. Pincus, S.M.: Approximate entropy as a measure of system complexity. Proc. Nat. Acad. Sci. USA **88**(6), 2297–2301 (1991)