# One-Dimensional Nonlinear Model for Producing Chaos

Zhongyun Hua, *Member, IEEE*, and Yicong Zhou, *Senior Member, IEEE*

***Abstract*— Motivated by the concept of circuit design in digital circuit, this paper proposes a one-dimensional (1D) nonlinear model (1D-NLM) for producing 1D discrete-time chaotic maps. Our previous works have designed four nonlinear operations of generating new chaotic maps. However, they focus only on discussing individual nonlinear operations and their properties, but fail to consider their relationship among these operations. The proposed 1D-NLM includes these existing nonlinear operations, develops two new nonlinear operations, discusses their relationship among different nonlinear operations, and investigates the properties of different combinations of these operations. To show the effectiveness of 1D-NLM in generating new chaotic maps, as examples, we provide four new chaotic maps and study their dynamics properties from following three aspects: equilibrium point, stability, and bifurcation diagram. Performance evaluations are provided using the Lyapunov exponent, Shannon entropy, correlation dimension, and initial state sensitivity. The evaluation results show that these new chaotic maps have more complex chaotic behaviors than existing ones. To demonstrate the performance of 1D-NLM in practical applications, we use a pseudo-random number generator (PRNG) to compare new and existing chaotic maps. The randomness test results indicate that new chaotic map generated by 1D-NLM shows better performance than existing ones in designing PRNG.**

***Index Terms*— Chaotic behavior, chaotic map, chaotification, 1D nonlinear model.**

## I. Introduction

CHAOTIC behaviors widely exist in many natural and non-natural phenomena, such as the weather and climate [1]. It can be studied through some analytical techniques or mathematical models, known as chaotic systems. Although there is no universally accepted mathematical definition for chaos, a chaotic system with chaotic behavior always displays the following properties: initial state sensitivity, topological transitivity and density of periodic orbits [2], [3]. Thus, the future behavior of a chaotic system is fully determined by its initial state. Any arbitrarily tiny change in the initial state results in a totally different orbit. With these significant properties, chaos theory has wide applications in different fields of science and engineering [4]–[7], especially in cryptography and communication [8]–[11]. This is due to the facts that many properties of chaotic behavior can be found similar counterparts in cryptography and the synchronization of chaos is extremely suitable for designing secure communication systems [12]–[15].

A dynamical system with chaotic attractors is globally stable but locally unstable. This means that arbitrarily close states diverge from each other but never depart from the attractor. However, the phase plane of finite precision platforms cannot have infinite number of states. When chaotic behavior is simulated in a finite precision platform, the arbitrarily close states will overlap, and thus the chaotic behavior will degrade to periodic behavior [16]–[18]. If states of a chaotic attractor are more concentrated, the extremely close ones are more possible to overlap. Thus, a chaotic system with good ergodicity is desired in real applications. On the other hand, with the development of discerning chaos technologies, some chaotic systems with simple definitions and behaviors can be easily attacked using different methods [19]. Recently, many studies are performed to predict chaotic behaviors by estimating their states [20], identifying their chaotic signals [21], [22], or deducing their initial conditions [23], [24]. If the future behavior of a chaotic system is successfully predicted, its corresponding chaos-based applications may have the high probability of crashing [25], [26].

Recently, a wide body of research has devoted to developing new dynamical systems with complex behaviors. These studies can be classified into two catalogs: designing specific chaotic maps and developing methodologies of generating a series of chaotic maps. The former aims to produce well-defined chaotic maps with clear mathematical definitions, such as the Lü attractor [27], the multiwing chaotic attractors [28]–[30] and the multiscroll chaotic attractors [31], [32]. The latter is to propose a framework or a system that can generate a series of chaotic maps, such as the coupling scheme [33]–[35] and the hyperchaotic system generation methodology [36].

To generate new one-dimensional (1D) discrete-time chaotic maps with better performance, our previous works have designed four nonlinear operations: cascade [37], modulation [38], switching [39] and fusion [40]. However, these previous works discussed only the properties of individual nonlinear operations and failed to consider the relationship among different nonlinear operations. To address this problem, this paper proposes a 1D nonlinear model (1D-NLM) to discuss the relationship among different nonlinear operations and to investigate the properties and chaotic behaviors of different combinations of these nonlinear operations. New

Manuscript received December 4, 2016; revised April 25, 2017; accepted June 12, 2017. Date of publication July 18, 2017; date of current version January 5, 2018. This work was supported in part by the Macau Science and Technology Development Fund under Grant FDCT/016/2015/A1, and in part by the Research Committee at the University of Macau under Grant MYRG2014-00003-FST and Grant MYRG2016-00123-FST, and in part by the Shenzhen Science and Technology Innovation Council under Grant JCYJ20170307150704051. This paper was recommended by Associate Editor P. P. Sotiriadis. *(Corresponding author: Yicong Zhou.)*

Z. Hua is with the School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen 518055, China (e-mail: huazyum@gmail.com).

Y. Zhou is with the Department of Computer and Information Science, University of Macau, Macau 999078, China (e-mail: yicongzhou@umac.mo).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TCSI.2017.2717943

chaotic maps can be generated by arbitrarily combining these nonlinear operations or by directly using them individually. Thus, users have great flexibility to select arbitrary nonlinear operations and any existing chaotic maps as seed maps to produce a large number of new chaotic maps. The main contributions of this work are as follows:

1) We propose 1D-NLM. It contains six basic nonlinear operations, including four nonlinear operations developed in our previous works and two newly introduced ones. These operations can be arbitrarily combined together to form new complicated operations;
2) We propose two new nonlinear operations for 1D-NLM and theoretically analyze their chaotic behaviors. To investigate the relationship among these basic operations, we comprehensively analyze the properties of different combinations of these basic operations and their chaotic behaviors;
3) As examples, four new chaotic maps are generated by two proposed basic nonlinear operations and combinations of basic operations in 1D-NLM. We study their dynamics properties from following three aspects: equilibrium point, stability and bifurcation diagram;
4) We quantitatively evaluate these newly generated chaotic maps using the Lyapunov exponent, Shannon entropy, correlation dimension and initial state sensitivity.
5) To demonstrate the performance of 1D-NLM in practical applications, we use a pseudo-random number generator (PRNG) as an example to compare one of our new chaotic maps with existing chaotic maps.

The rest of this paper is organized as follows. Section II reviews three existing 1D chaotic maps and four developed nonlinear operations as background. Section III introduces 1D-NLM and its chaotic behavior is discussed in Section IV. Section V presents four examples of new chaotic maps generated using 1D-NLM and their performance is evaluated in Section VI. Section VII use a chaos-based PRNG to compare the performance of new and existing chaotic maps. Section VIII concludes this paper.

## II. Background

This section briefly reviews three widely used 1D chaotic maps and four developed nonlinear operations. The existing 1D chaotic maps will be used as seed maps to demonstrate the proposed 1D-NLM in Section V and the four nonlinear operations are components of the model.

### A. Existing 1D Chaotic Maps

*1) Logistic Map:* The Logistic map is a first-order difference equation that widely arises in the economic, social and biological sciences [41]. It is represented as

$$x_{i+1} = \mathcal{L}(x_i) = 4px_i(1 - x_i).$$

Its parameter $p \in [0, 1]$ and variable $x_i$ is limited into the interval $[0, 1]$.

Equilibrium point (or fixed point) is the element of a function's domain that maps to itself. The Logistic map's equilibrium point $\tilde{x}$ satisfies the equation

$$\tilde{x} = 4p\tilde{x}(1 - \tilde{x}). \tag{1}$$

Solve Eq. (1), we can get that the Logistic map has two equilibrium points, i.e. $\tilde{x}_1 = 0$ and $\tilde{x}_2 = 1 - 1/(4p)$. Fig. 1(a) plots the two equilibrium points and bifurcation diagram of the Logistic map with the change of its parameter $p$. Observed from the bifurcation diagram, we can get that the Logistic is chaotic when $p \in [0.9, 1]$.

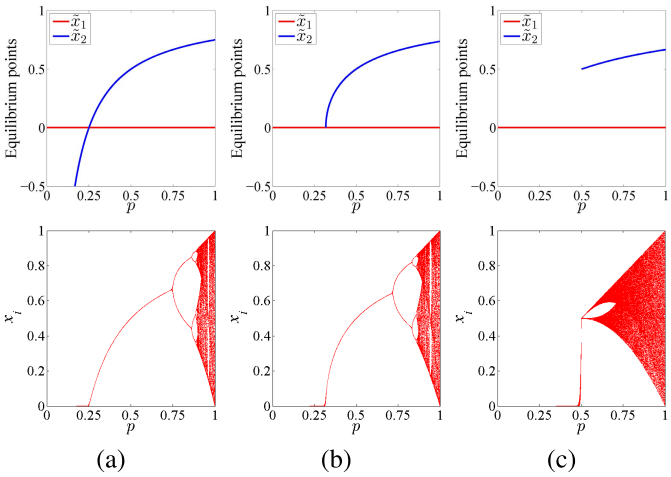


Fig. 1. Equilibrium points and bifurcation diagrams of the (a) Logistic map, (b) Sine map and (c) Tent map.

*2) Sine Map:* The Sine map is derived from the Sine function that maps the input angle within interval $[0, 1]$ into the same interval. Mathematically, the Sine map is defined as

$$x_{i+1} = \mathcal{S}(x_i) = p \sin(\pi x_i),$$

where the control parameter $p \in [0, 1]$. To find out the Sine map's equilibrium point $\tilde{x}$, we set

$$\tilde{x} = p \sin(\pi \tilde{x}). \tag{2}$$

Solve Eq. (2), we obtain that the Sine map has equilibrium point $\tilde{x}_1 = 0$ in the whole parameter range and another equilibrium point $\tilde{x}_2$ when its parameter $p > 0.3184$. Fig. 1(b) shows its equilibrium points and bifurcation diagram. The Sine map has chaotic behavior when $p \in [0.87, 1]$.

*3) Tent Map:* The Tent map is a piecewise function that either scales or folds the input value based on its range. Mathematically, its generalized form can be defined as

$$x_{i+1} = \mathcal{T}(x_i) = \begin{cases} 2px_i, & \text{for } x_i < 0.5, \\ 2p(1 - x_i), & \text{for } x_i \geq 0.5, \end{cases}$$

where the parameter $p \in [0, 1]$. To find out its equilibrium point $\tilde{x}$, we set

$$\tilde{x} = 2p \min\{\tilde{x}, 1 - \tilde{x}\}. \tag{3}$$

From Eq. (3), we calculate out that the Tent map has equilibrium point $\tilde{x}_1 = 0$ in the whole parameter range and equilibrium point $\tilde{x}_2 = (2p)/(2p+1)$ in the range $p \in [0.5, 1]$. The two equilibrium points and bifurcation diagram of the Tent map are plotted in Fig. 1(c). The Tent map has chaotic behavior when $p \in (0.5, 1)$.

TABLE I
DEFINITIONS OF SIX BASIC NONLINEAR OPERATIONS IN 1D-NLM

| Operations | Descriptions | Definitions |
|---|---|---|
| Cascade ($\circledcirc$) | $\mathcal{C}(x) = f(x) \circledcirc g(x)$ | $x_{i+1} = g(f(x_i))$ |
| Modulation ($\odot$) | $\mathcal{M}(x) = f(x) \odot g(x)$ | $x_{i+1} = g(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f(y_i)$ |
| Switching ($\circledast$) | $\mathcal{W}(x) = f_1(x) \circledast f_2(x) \circledast \cdots \circledast f_l(x)$ | $x_{i+1} = f_{q_i}(x_i)$, where $q_i \in \{1, 2, \cdots, l\}$ |
| Fusion ($\oplus$) | $\mathcal{P}(x) = f(x) \oplus g(x)$ | $x_{i+1} = (f(x_i) + g(x_i)) \mod 1$ |
| Scalar cascade($\widetilde{\circledcirc}$) | $\mathcal{U}(x) = c \mathbin{\widetilde{\circledcirc}} f(x)$ | $\mathcal{U}(x) = \underbrace{f(x) \circledcirc f(x) \circledcirc \cdots \circledcirc f(x)}_{c}$ |
| Scalar modulation ($\widetilde{\odot}$) | $\mathcal{D}(x) = c \mathbin{\widetilde{\odot}} f(x)$ | $\mathcal{D}(x) = \underbrace{f(x) \odot f(x) \odot \cdots \odot f(x)}_{c}$ |

### B. Existing Nonlinear Operations

Here, we recall four nonlinear operations of generating 1D chaotic maps developed in our previous works.

*1) Cascade:* The cascade operation for generating new chaotic maps was proposed in [37]. It connects two 1D chaotic maps in series. The definition of the cascade operation is given in Table I. $f(x)$ and $g(x)$ are two 1D chaotic maps that are used as seed maps. The output of $f(x)$ is fed into the input of $g(x)$, and the output of $g(x)$ is the iterative value, and also feeds back into the input of $f(x)$ for next iteration.

*2) Modulation:* The modulation operation uses the output of a chaotic map to dynamically control the parameter of another chaotic map to exhibit chaotic behaviors [38]. Its definition is shown in Table I, in which $f(x)$ and $g(x)$ are two 1D chaotic maps, the transformation $R(x)$ is to linearly transform the output of $f(x)$ into $g(x)$'s chaotic range, and $g(x)$ uses the dynamically changed parameter to generate trajectories.

*3) Switching:* The switching operation utilizes a wheel switch to select one of seed maps to execute in each iteration [39]. It contains $l$ 1D normalized chaotic maps as seed maps and a controlling wheel switch $\mathbf{q}$. According to the pre-defined rules in $\mathbf{q}$, one seed map is selected to generate chaotic orbit in each iteration. Its definition is shown in Table I. As can be seen, $f_1(x), f_2(x), \cdots, f_l(x)$ are $l$ normalized chaotic maps and $\mathbf{q} = \{q_1, q_2, \cdots, q_l\}$ is the wheel switch, in which $q_i \in \{1, 2, \cdots, l\}$. In the $i$-th iteration, the $q_i$-th seed map $f_{q_i}(x)$ is selected to execute.

*4) Fusion:* The fusion operation generates new chaotic maps by mixing the dynamics of two seed maps in a nonlinear way [40]. Its definition is shown in Table I. In each iteration, the input is concurrently fed into two seed maps, and then the outputs of the two seed maps are combined by the modular arithmetic.

## III. PROPOSED 1D-NLM

When designing digital circuit systems, complex circuit systems can be constructed by combining several basic circuit units. Motivated by the concept of circuit design, this section introduces the 1D nonlinear model (1D-NLM). It contains six basic nonlinear operations, including four developed nonlinear operations presented in Section II-B and two newly introduced ones. These nonlinear operations can be arbitrarily combined together to form new complicated operations. Each of the six basic nonlinear operations is designed using the concept that complex circuit systems are a combination of basic circuit units, while the complicated operations correspond to the combined structures of complex circuit systems.

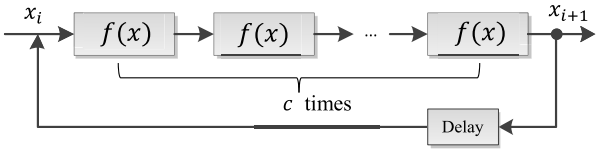


Fig. 2. The scalar cascade operation.

### A. New Nonlinear Operations

Here, we introduce two nonlinear operations. Each operation can use existing chaotic maps as seed maps to generate new ones.

*1) Scalar Cascade:* The scalar cascade operation generates chaotic maps by cascading a chaotic map with itself several times. Its definition is shown in Table I and its structure is demonstrated in Fig. 2. The integer $c$ indicates how many times the seed map $f(x)$ is cascaded with itself. The scalar cascade operation has all the properties of the cascade operation.

*2) Scalar Modulation:* The scalar modulation is defined in Table I and its structure is shown in Fig. 3. The $c$ is an integer and $c \geq 2$. The first $c-1$ maps are control maps and the last one is the seed map. When $c = 2$, the scalar modulation degrades to the modulation operation that the outputs of a chaotic map is used to dynamically control the parameter of itself. When $c > 2$, the outputs of a control map are used to dynamically control the parameter of the next control map, and the outputs of the last control map $f(y^{(c-1)})$ are used to dynamically control the parameter of the seed map $f(x)$ to generate iterative values. The transformation $R(x)$ maps the output of a control map into the chaotic range of the next control map or the seed map $f(x)$.

All the six basic nonlinear operations can generate a large number of new chaotic maps using existing chaotic maps as

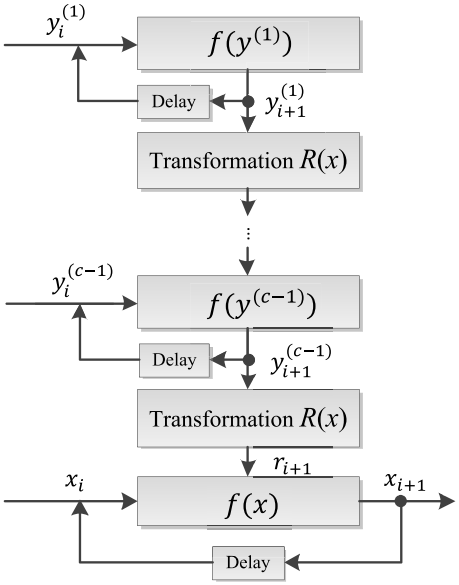


Fig. 3. The scalar modulation operation.

seed maps. These new chaotic maps usually have much more complex behaviors than their corresponding seed maps.

### *B. Combinations of Basic Nonlinear Operations*

The basic nonlinear operations in 1D-NLM can be arbitrarily combined to form new complicated operations. For $N$ seed maps $f_1(x)$, $f_2(x)$, $\cdots$, $f_N(x)$, a combination of basic operations can be defined as

$$\mathcal{CO}(x) = f_1(x) \maltese f_2(x) \maltese \cdots \maltese f_N(x), \tag{4}$$

where $\maltese$ represents one of the six basic nonlinear operations listed in Table I. Note that if $\maltese$ represents the scalar cascade or scalar modulation, $f_i(x)$ on the left of $\maltese$ is an integer constant instead of a chaotic map. In Eq. (4), any chaotic maps and basic nonlinear operations can be arbitrarily selected to generate a large number of new chaotic maps.

To better demonstrate the properties of the complicated operations, we set $N = 3$ and the two basic nonlinear operations as the cascade operation $\circledcirc$ and modulation operation $\odot$ as examples. A totally number of 12 different combinations can be obtained and they are shown in Table II. According to the order of the cascade and modulation operations, these complicated operations can be divided into two kinds. One first does modulation and then performs cascade. The other first does cascade and then performs modulation. For the two kinds of complicated operations, we separately take one example to analyze their chaotic behaviors. The two examples are

$$\mathcal{CO}_1(x) = f_1(x) \odot f_2(x) \circledcirc f_3(x), \tag{5}$$

and

$$\mathcal{CO}_2(x) = f_1(x) \circledcirc f_2(x) \odot f_3(x). \tag{6}$$

*1) Structure of $\mathcal{CO}_1(x)$:* The structure of $\mathcal{CO}_1(x)$ is shown as Fig. 4. The seed maps $f_1(x)$, $f_2(x)$ and $f_3(x)$ are three existing chaotic maps. First, do cascade operation to $f_1(x)$ and $f_2(x)$. Then, perform modulation operation to the cascade result and $f_3(x)$. Changing the positions of $f_1(x)$, $f_2(x)$ and $f_3(x)$ can result in totally different combinations, which can be seen in the first six rows of Table II.

TABLE II
TWELVE DIFFERENT COMBINATIONS OF BASIC NONLINEAR OPERATIONS

| Operations | Definitions |
|---|---|
| $f_1(x) \odot f_2(x) \circledcirc f_3(x)$ | $x_{i+1} = f_3(f_2(r_{i+1}, x_i))$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_1(y_i)$ |
| $f_1(x) \odot f_3(x) \circledcirc f_2(x)$ | $x_{i+1} = f_2(f_3(r_{i+1}, x_i))$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_1(y_i)$ |
| $f_2(x) \odot f_1(x) \circledcirc f_3(x)$ | $x_{i+1} = f_3(f_1(r_{i+1}, x_i))$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_2(y_i)$ |
| $f_2(x) \odot f_3(x) \circledcirc f_1(x)$ | $x_{i+1} = f_1(f_3(r_{i+1}, x_i))$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_2(y_i)$ |
| $f_3(x) \odot f_1(x) \circledcirc f_2(x)$ | $x_{i+1} = f_2(f_1(r_{i+1}, x_i))$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_3(y_i)$ |
| $f_3(x) \odot f_2(x) \circledcirc f_1(x)$ | $x_{i+1} = f_1(f_2(r_{i+1}, x_i))$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_3(y_i)$ |
| $f_1(x) \circledcirc f_2(x) \odot f_3(x)$ | $x_{i+1} = f_3(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_2(f_1(y_i))$ |
| $f_1(x) \circledcirc f_3(x) \odot f_2(x)$ | $x_{i+1} = f_2(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_3(f_1(y_i))$ |
| $f_2(x) \circledcirc f_1(x) \odot f_3(x)$ | $x_{i+1} = f_3(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_1(f_2(y_i))$ |
| $f_2(x) \circledcirc f_3(x) \odot f_1(x)$ | $x_{i+1} = f_1(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_3(f_2(y_i))$ |
| $f_3(x) \circledcirc f_1(x) \odot f_2(x)$ | $x_{i+1} = f_2(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_1(f_3(y_i))$ |
| $f_3(x) \circledcirc f_2(x) \odot f_1(x)$ | $x_{i+1} = f_1(r_{i+1}, x_i)$, where $r_{i+1} = R(y_{i+1})$, $y_{i+1} = f_2(f_3(y_i))$ |

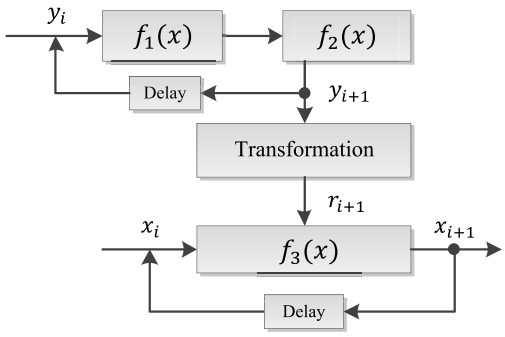


Fig. 4. The structure of $\mathcal{CO}_1(x)$.

*2) Structure of $\mathcal{CO}_2(x)$:* Fig. 5 displays the structure of $\mathcal{CO}_2(x)$. Different from $\mathcal{CO}_1(x)$, $\mathcal{CO}_2(x)$ first does modulation operation to $f_1(x)$ and $f_2(x)$, and then performs cascade

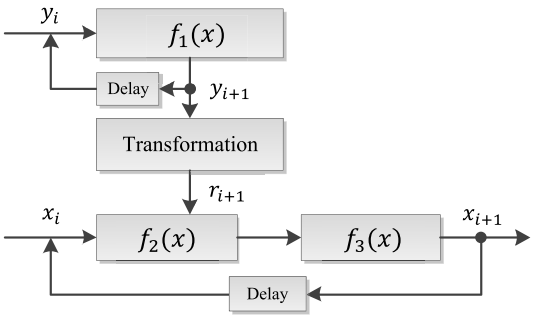


Fig. 5. The structure of $\mathcal{CO}_2(x)$.

to the modulation result and $f_3(x)$. Changing the positions of $f_1(x)$, $f_2(x)$ and $f_3(x)$ in $\mathcal{CO}_2(x)$ also result in totally different chaotic maps. All the different combinations with different positions of $f_1(x)$, $f_2(x)$ and $f_3(x)$ are shown in the last six rows of Table II.

## IV. Chaotic Behavior Analysis

Among all the methods of detecting the existence of chaos, the Lyapunov exponent (LE) developed in [42] is a widely accepted indictor, which denotes the average divergence of two close trajectories of a dynamical system. The LE of a differentiable equation $x_{i+1} = f(x_i)$ can be defined as,

$$\lambda_{f(x)} = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|\right\}. \tag{7}$$

A positive LE denotes that the two close trajectories of a dynamical system exponentially diverge in each unit time and they will be totally different eventually. Thus, a dynamical system $x_{i+1} = f(x_i)$ is considered to own chaotic behavior if $\lambda_{f(x)} > 0$.

The chaotic behaviors of the cascade, modulation, switching and fusion operations have been analyzed in the previous works in [37]–[40]. The analysis results demonstrated their complex chaotic behaviors.

### A. Chaotic Behavior of Scalar Cascade

For the scalar cascade operation $\mathcal{U}(x) = c \mathbin{\widetilde{\circledcirc}} f(x)$, when $c = 2$, its iterative form can be rewritten as $x_{i+1} = f(f(x_i))$. Based on the definition of LE in Eq. (7), its LE can be written as

$$\begin{aligned}\lambda_{\mathcal{U}(x)} &= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|(f(f(x_i)))'\right|\right\}\\ &= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(f(x_i))f'(x_i)\right|\right\}\\ &= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(f(x_i))\right|\right\}\\ &\quad+\lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|\right\}\\ &= 2\lambda_{f(x)}.\end{aligned}$$

When $c = k$, it is not difficult to calculate out that $\lambda_{\mathcal{U}(x)} = k\lambda_{f(x)}$. Thus, $\lambda_{\mathcal{U}(x)} > 0$ if $\lambda_{f(x)} > 0$. This means that if the seed map $f(x)$ has chaotic behavior, the scalar cascade result is chaotic and has larger LE than its seed map.

### B. Chaotic Behavior of Scalar Modulation

Based on the definition of LE in Eq. (7), the LE of the scalar modulation shown in Fig. 3 can be written as

$$\lambda_{\mathcal{D}(x)} = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(r_{i+1}, x_i)\right|\right\}, \tag{8}$$

where $x_i$ is the iteration value and $r_{i+1}$ is the transform result of $(c-1)$-th control map's output that is used to control the parameter of $f(x)$ in each iteration. LE of the scalar modulation result can be analyzed from the following ways:

- When the attractors of the $(c-1)$-th control map $f(y_i^{(c-1)})$ are an equilibrium point, after transforming, the obtained $r_{i+1}$ is also fixed and within the chaotic range of $f(x)$. Thus,
$$\lambda_{\mathcal{D}(x)} > 0.$$
- When the attractors of $f(y_i^{(c-1)})$ are a limit cycle, namely, $f(y_i^{(c-1)})$ has a periodic orbit and its outputs are a finite number of different points, suppose $\{o_j \mid j = 1, 2, \cdots, k\}$. After transforming, the periodic sequence $\{o_j \mid j = 1, 2, \cdots, k\}$ is transformed as $\{r_j \mid j = 1, 2, \cdots, k\}$, which is also a periodic sequence and $r_j$ $(j = 1, 2, \cdots, k)$ is in the chaotic range of $f(x)$. Because $k$ is a finite number, when the iteration number $n$ increases to $\infty$, the number of each point of the periodic sequence $\{r_j \mid j = 1, 2, \cdots, k\}$ approaches to $n/k$. Thus, Eq. (8) can be rewritten as
$$\begin{aligned}\lambda_{\mathcal{D}(x)} &= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n/k-1}\ln\left|(f'(r_1, x_i)\right|\right\}+\cdots\\ &\quad+\lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n/k-1}\ln\left|(f'(r_k, x_i)\right|\right\}.\end{aligned} \tag{9}$$
Because $k$ is a finite number and $n \to \infty$, then $(n/k) \to \infty$. Thus,
$$\begin{aligned}&\lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n/k-1}\ln\left|(f'(r_j, x_i)\right|\right\}\\ &\quad= \frac{1}{k}\lim_{(n/k)\to\infty}\left\{\frac{1}{n/k}\sum_{i=0}^{n/k-1}\ln\left|(f'(r_j, x_i)\right|\right\}\\ &\quad= \frac{1}{k}\lambda_{f(r_j,x)},\end{aligned}$$
where $j = 1, 2, \cdots, k$. Then Eq. (9) becomes
$$\begin{aligned}\lambda_{\mathcal{D}(x)} &= \frac{1}{k}\lambda_{f(r_1,x)}+\frac{1}{k}\lambda_{f(r_2,x)}+\cdots+\frac{1}{k}\lambda_{f(r_k,x)}\\ &= \frac{1}{k}\sum_{j=1}^{k}\lambda_{f(r_j,x)}.\end{aligned}$$

Because $r_j$ $(j = 1, 2, \cdots, k)$ is in the chaotic range of $f(x)$, $\lambda_{f(r_j,x)} > 0$ for $\forall j \in \{1, 2, ..., k\}$. Thus,

$$\lambda_{\mathcal{D}(x)} = \frac{1}{k}\sum_{j=1}^{k} \lambda_{f(r_j,x)} > 0.$$

- When $f(y_i^{(c-1)})$ has chaotic attractor, $f(y_i^{(c-1)})$ is chaotic and $r_{i+1}$ is dynamical. In this case, the seed map $f(x)$ achieves a different control parameter in each unit time, which makes the iterative outputs different and unpredictable.

From the discussions above, the scalar modulation result is able to achieve chaotic behavior if the seed map $f(x)$ has continuous chaotic range. However, the scalar modulation result may lose its chaotic behavior if the chaotic range of $f(x)$ is discontinuous. This occurs when the control map $f(y^{(c-1)})$ is not chaotic and the fixed output(s) of $f(y^{(c-1)})$ happen(s) to be transformed into the nonchaotic ranges of $f(x)$.

### C. Chaotic Behaviors of Complicated Operations

As arbitrary numbers of basic nonlinear operations can be selected to form complicated operations in Eq. (4), we take $\mathcal{CO}_1(x)$ in Eq. (5) and $\mathcal{CO}_2(x)$ in Eq. (6) as examples to demonstrate the chaotic behaviors of complicated operations.

*1) Chaotic Behavior of $\mathcal{CO}_1(x)$:* The example $\mathcal{CO}_1(x)$ first performs the modulation to $f_1(x)$ and $f_2(x)$, and then cascades the modulation result and $f_3(x)$. Suppose $\mathcal{M}(x) = f_1(x) \odot f_2(x)$. According to the analysis in [38, Section III-C] that if the seed map $f_2(x)$ has continuous chaotic range, the modulation result $\mathcal{M}(x)$ always has chaotic behavior. This means that $\lambda_{\mathcal{M}(x)} > 0$.

The example $\mathcal{CO}_1(x)$ can be rewritten as $\mathcal{CO}_1(x) = \mathcal{M}(x) \circledcirc f_3(x)$, namely $x_{i+1} = f_3(\mathcal{M}(x_i))$. Based on the definition of LE in Eq. (7), the LE of $\mathcal{CO}_1(x)$ can be defined as

$$\begin{aligned}
\lambda_{\mathcal{CO}_1(x)} &= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|(f_3(\mathcal{M}(x_i)))'\right|\right\} \\
&= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f_3'(\mathcal{M}(x_i))\mathcal{M}'(x_i)\right|\right\} \\
&= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f_3'(\mathcal{M}(x_i))\right|\right\} \\
&\quad + \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|\mathcal{M}'(x_i)\right|\right\} \\
&= \lambda_{f_3(x)} + \lambda_{\mathcal{M}(x)}.
\end{aligned}$$

Thus, the LE of $\mathcal{CO}_1(x)$ is the combination of those of $\mathcal{M}(x)$ and $f_3(x)$. Because $\lambda_{\mathcal{M}(x)} > 0$, $\lambda_{\mathcal{CO}_1(x)} > 0$ if $\lambda_{\mathcal{M}(x)} > -\lambda_{f_3(x)}$.

*2) Chaotic Behavior of $\mathcal{CO}_2(x)$:* The example $\mathcal{CO}_2(x)$ first cascades $f_1(x)$ and $f_2(x)$, and then performs modulation to the cascade result and $f_3(x)$. Suppose $\mathcal{C}(x) = f_1(x) \circledcirc f_2(x)$, then $\mathcal{CO}_2(x) = \mathcal{C}(x) \odot f_3(x)$. Based on the definition of LE in Eq. (7), the LE of $\mathcal{CO}_2(x)$ can be written as

$$\lambda_{\mathcal{CO}_2(x)} = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f_3'(r_{i+1}, x_i)\right|\right\}, \tag{10}$$

where $x_i$ is the iteration value and $r_{i+1}$ is the transformation result of $\mathcal{C}(x)$'s output that is used to control the parameter of $f_3(x)$ in each iteration. Based on the chaotic behavior analysis of modulation operation in [38, Section III-C], when the seed map has continuous chaotic range, the modulation result always has chaotic behavior whether the control map is chaotic or not. Then, $\lambda_{\mathcal{CO}_2(x)} > 0$ and $\mathcal{CO}_2(x)$ has chaotic behavior.

## V. Examples of New Chaotic Maps

To show the effectiveness and usability of 1D-NLM, this section demonstrates four examples of new chaotic maps generated by two proposed basic nonlinear operations and the complicated operations of 1D-NLM, and studies their dynamics properties.

### A. $\mathcal{E}_1$

First, we demonstrate the scalar cascade operation $\widetilde{\circledcirc}$. The constant $c$ is set as 3 and the seed map is selected as the Sine map $\mathcal{S}(x)$, then a chaotic map $\mathcal{E}_1$ can be generated. Mathematically, it is represented as

$$\begin{aligned}
x_{i+1} &= 3 \,\widetilde{\circledcirc}\, \mathcal{S}(x_i) \\
&= p_1 \sin(\pi p_2 \sin(\pi p \sin(\pi x_i))),
\end{aligned}$$

where $p$, $p_1$, $p_2$ are control parameters within the range $[0, 1]$. For simplicity, we set the parameters $p_1 = 1$, $p_2 = 1$ and investigate the chaotic behavior of $\mathcal{E}_1$ with the change of its parameter $p$. Then,

$$x_{i+1} = \sin(\pi \sin(\pi p \sin(\pi x_i))). \tag{11}$$

*1) Equilibrium Point and Stability:* To find out the equilibrium points of $\mathcal{E}_1$, we set $x_{i+1} = x_i$ and the equilibrium points of $\mathcal{E}_1$ are the roots of the equation

$$\tilde{x} - \sin(\pi \sin(\pi p \sin(\pi \tilde{x}))) = 0. \tag{12}$$

Obviously, $\tilde{x}_1 = 0$ is one equilibrium point of $\mathcal{E}_1$. Solving Eq. (12), we can find out that $\mathcal{E}_1$ has more equilibrium points when its control parameter $p$ increases within the range $[0, 1]$. When $p > 0.0323$, Eq. (12) has another root $\tilde{x}_2$ and thus $\mathcal{E}_1$ has two equilibrium points; When $p > 0.3063$, $\mathcal{E}_1$ has four equilibrium points; When $p > 0.6831$, $\mathcal{E}_1$ has six equilibrium points; When $p > 0.9460$, the number of equilibrium points increases to eight.

The equilibrium point of a dynamical system has two states: stable and unstable. Its stability is dependent on the slope of the system' curve at the point. When the slope is within the range $(-1, 1)$, the equilibrium point is stable and it attracts all its neighboring trajectories to make them converge to the point eventually; otherwise, the equilibrium point is unstable and its neighboring trajectories escape from it as the time increases.

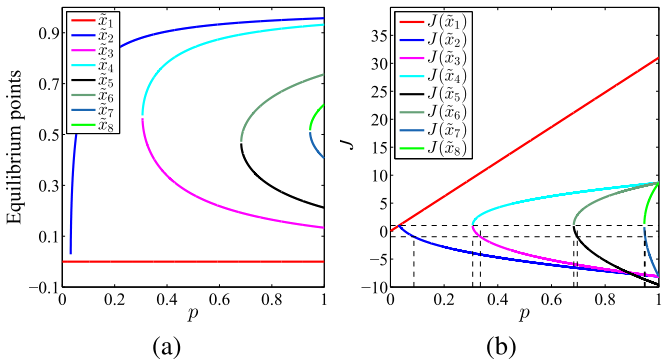


Fig. 6. (a) Equilibrium points of $\mathcal{E}_1$; (b) Jacobian values of the equilibrium points of $\mathcal{E}_1$.

TABLE III
EQUILIBRIUM POINTS OF $\mathcal{E}_1$ AND THEIR STABILITY

| Equilibrium points | Occurrence intervals | Stable intervals |
|---|---|---|
| $\tilde{x}_1$ | $[0, 1]$ | $[0, 0.0323]$ |
| $\tilde{x}_2$ | $[0.0323, 1]$ | $[0.0323, 0.0875]$ |
| $\tilde{x}_3$ | $[0.3063, 1]$ | $[0.3063, 0.3352]$ |
| $\tilde{x}_4$ | $[0.3063, 1]$ | unstable |
| $\tilde{x}_5$ | $[0.6831, 1]$ | $[0.6831, 0.6961]$ |
| $\tilde{x}_6$ | $[0.6831, 1]$ | unstable |
| $\tilde{x}_7$ | $[0.9460, 1]$ | $[0.9460, 0.9490]$ |
| $\tilde{x}_8$ | $[0.9460, 1]$ | unstable |

The Jacobian matrix can be used to calculate the slope of a curve and that of $\mathcal{E}_1$ is given by

$$J = \frac{d_{\mathcal{E}_1}}{d_{x_i}} = \cos(\pi \sin(\pi p \sin(\pi x_i))) \times \pi \cos(\pi p \sin(\pi x_i))\pi p \cos(\pi x_i)\pi.$$

The equilibrium point is stable if the Jacobian value at the point is within the range $(-1, 1)$; otherwise, it is unstable.

Fig. 6 plots the equilibrium points of $\mathcal{E}_1$ and their Jacobian values with different parameter settings. Table III lists the occurrence and stable intervals of these equilibrium points. As can be seen from the table, we can achieve that $\mathcal{E}_1$ has stability when $p \in [0, 0.0875] \cup [0.3063, 0.3352] \cup [0.6831, 0.6961] \cup [0.9460, 0.9490]$.

*2) Bifurcation Diagram:* As can be observed from Fig. 6(b), when the control parameter $p$ increases to 0.0875, the equilibrium point $\tilde{x}_2 = 0.6708$ becomes unstable. At the same time, the Jacobian value at this point reduces to -1. Once this happens, the equilibrium point $\tilde{x}_2$ becomes two new stable points. When $p$ increases to 0.1109, the period-two stable points lose their stability and generate period-four stable points; When $p$ increases to 0.1172, the period-four stable points lose their stability and generate eight stable points. For example, when $p = 0.1185$, the eight stable points are 0.3521, 0.8554, 0.4890, 0.9095, 0.3217, 0.8274, 0.5646, 0.9002. By this principle, the stable points doubly increase and a critical value $\tilde{p}$ is finally achieved. When $p$ is slightly less than $\tilde{p}$, the outputs of the system are periodic with a large period. When $p$ is slightly larger than $\tilde{p}$, these points start to become aperiodic and the system eventually routes to chaos, which is called period-doubling bifurcation. Numerical result shows that $\hat{p} = 0.1190$. When $p$ increases to 0.3063, 0.6831 or 0.9460, $\mathcal{E}_1$ obtains the stable equilibrium points $\tilde{x}_3$, $\tilde{x}_5$, $\tilde{x}_7$, respectively. Then, it returns back to stable state. When $p$ increases to 0.3352, 0.6961 or 0.9490, $\tilde{x}_3$, $\tilde{x}_5$ and $\tilde{x}_7$ lose their stability and $\mathcal{E}_1$ starts to route to chaos again. The bifurcation diagram of $\mathcal{E}_1$ is plotted in Fig. 7.

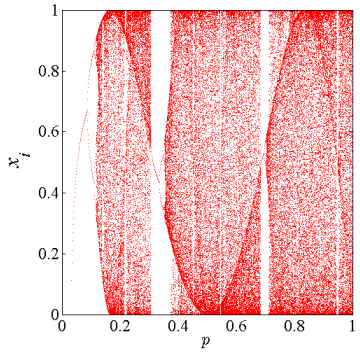


Fig. 7. The bifurcation diagram of $\mathcal{E}_1$.

## B. $\mathcal{E}_2$

Here, we give an example of chaotic map generated by the scalar modulation operation $\widetilde{\odot}$. The coefficient $c$ is set as 3 and the seed map is also selected as the Sine map $\mathcal{S}(x)$, then a chaotic map $\mathcal{E}_2$ can be generated by

$$\begin{aligned} x_{i+1} &= 3 \,\widetilde{\odot}\, \mathcal{S}(x_i) \\ &= r_{i+1} \sin(\pi x_i), \end{aligned} \tag{13}$$

where

$$\begin{aligned} r_{i+1} &= 1 - 0.13 y_{i+1}^{(2)}, \\ y_{i+1}^{(2)} &= p_{i+1} \sin(\pi y_i^{(2)}), \\ p_{i+1} &= 1 - 0.13 y_{i+1}^{(1)}, \\ y_{i+1}^{(1)} &= p \sin(\pi y_i^{(1)}), \end{aligned}$$

where $p$ is the control parameter and $p \in [0, 1]$.

Fig. 8 shows the bifurcation diagram of $\mathcal{E}_2$. Theoretically, if the seed map $f(x)$ has a continuous chaotic range, the scalar modulation result has chaotic behavior for all the parameter settings. This has been proved in Section IV-B. However, if the chaotic range of $f(x)$ is not continuous, the scalar modulation result may lose its chaotic behavior in some parameter settings. This occurs when the fixed outputs of a control map happen to be transformed into the non-chaotic ranges of the next control map or seed map, such as the white space in the chaotic ranges of the Logistic and Sine maps (see Figs. 1(a) and (b)). As the seed map in $\mathcal{E}_2$ is the Sine map, $\mathcal{E}_2$ losses its chaotic behavior in few parameter settings, which can be observed from Fig. 8.

## C. $\mathcal{E}_3$

This example demonstrates the complicated operation $\mathcal{CO}_1(x) = f_1(x) \odot f_2(x) \circledcirc f_3(x)$ in Table II. $f_1(x)$ is selected

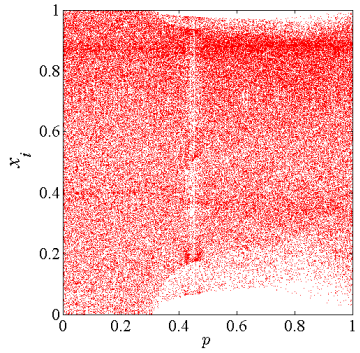


Fig. 8. The bifurcation diagram of $\mathcal{E}_2$.

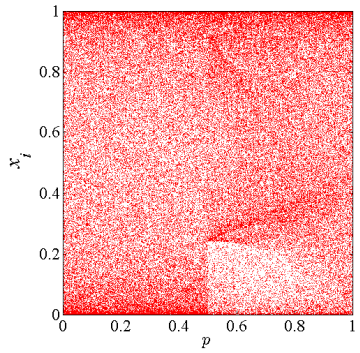


Fig. 9. The bifurcation diagram of $\mathcal{E}_3$.

as the Tent map $\mathcal{T}(x)$; $f_2(x)$ is selected as the Sine map $\mathcal{S}(x)$; and $f_3(x)$ is selected as the Logistic map $\mathcal{L}(x)$. Then, $\mathcal{E}_3$ is defined by

$$\mathcal{E}_3(x) = \mathcal{T}(x) \odot \mathcal{S}(x) \circledcirc \mathcal{L}(x).$$

First, Tent map controls the parameter of the Sine map to generate a new chaotic map $\mathcal{M}(x)$. Then, $\mathcal{M}(x)$ is cascaded by the Logistic map to obtain $\mathcal{E}_3$. The iterative form of $\mathcal{E}_3$ is represented as

$$x_{i+1} = 4r_{i+1}\sin(\pi x_i)(1 - r_{i+1}\sin(\pi x_i)), \tag{14}$$

where $r_{i+1}$ is the transformation result of $y_{i+1}$, which is defined as

$$r_{i+1} = 1 - 0.13y_{i+1},$$

where $y_{i+1}$ is the output of the Tent map,

$$y_{i+1} = \begin{cases} 2py_1, & \text{for } y_i < 0.5, \\ 2p(1 - y_i), & \text{for } y_i \geq 0.5, \end{cases}$$

where the control parameter $p \in [0, 1]$.

We use the numerical result to investigate the chaotic properties of $\mathcal{E}_3$. It is obvious that $\tilde{x}_1 = 0$ is an equilibrium point of $\mathcal{E}_3$. In the generation procedure of $\mathcal{E}_3$, the parameter of Sine map is modulated by the Tent map. When $p \in [0, 0.5]$, the Tent map has fixed point, which is transformed into the chaotic range of Tent map by the following transformation; When $p \in (0.5, 1]$, the Tent map has chaotic attractors and the Sine map gets a dynamically changed parameter in each iteration. After cascading with the Logistic map, the obtained $\mathcal{E}_3$ is dissipated in the whole parameter range [0, 1], which is also verified by its bifurcation diagram shown in Fig. 9.

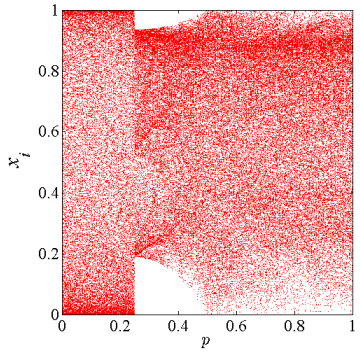


Fig. 10. The bifurcation diagram of $\mathcal{E}_4$.

### D. $\mathcal{E}_4$

The example $\mathcal{E}_4$ demonstrates the complicated operation $\mathcal{CO}_2(x) = f_1(x) \circledcirc f_2(x) \odot f_3(x)$ in Table II. As any different of same chaotic maps can be selected in the combination operation, we select $f_1(x)$ and $f_2(x)$ both as the Tent map $\mathcal{T}(x)$ and choose $f_3(x)$ as the Sine map $\mathcal{S}(x)$. Then, $\mathcal{E}_4$ is defined by

$$\mathcal{E}_4(x) = \mathcal{T}(x) \circledcirc \mathcal{T}(x) \odot \mathcal{S}(x).$$

First, Tent map is cascaded to itself to generate a new chaotic map, namely $\mathcal{C}(x) = \mathcal{T}(x) \circledcirc \mathcal{T}(x)$. Then, $\mathcal{C}(x)$ is to dynamically control the parameter of the Sine map to obtain $\mathcal{E}_4$. The iterative definition of $\mathcal{E}_4$ can be represented by

$$x_{i+1} = r_{i+1}\sin(\pi x_i), \tag{15}$$

where $r_{i+1}$ is the transformation result of $y_{i+1}$, which is defined as

$$r_{i+1} = 1 - 0.13y_{i+1},$$

where $y_{i+1}$ is the output of $\mathcal{C}(x)$.

The bifurcation diagram of $\mathcal{E}_4$ is shown in Fig. 10, from which we can observe that $\mathcal{E}_4$ also has chaotic behavior in the whole parameter range.

## VI. Performance Analysis

This section evaluates the performance of the four new chaotic maps from four aspects: Lyapunov exponent (LE) [42], Shannon entropy (SE) [43], [44], correlation dimension (CD) [45] and initial state sensitivity.

### A. Lyapunov Exponent

As discussed in Section IV that LE is a widely accepted indictor to measure the existence of chaotic behavior. A dynamical system with at least one positive LE shows complicated dynamics and bigger positive LE means that the two close trajectories of a dynamical system diverge faster. Fig. 11 plots the LEs of different chaotic maps with the change of their parameters. As can be observed from the figure, $\mathcal{E}_1$ and $\mathcal{E}_2$ have positive LEs in most parameter settings while $\mathcal{E}_3$ and $\mathcal{E}_4$ have positive LEs in the whole parameter ranges. This is consistent with their bifurcation diagrams in Figs. 7, 8, 9 and 10. Compared with their corresponding

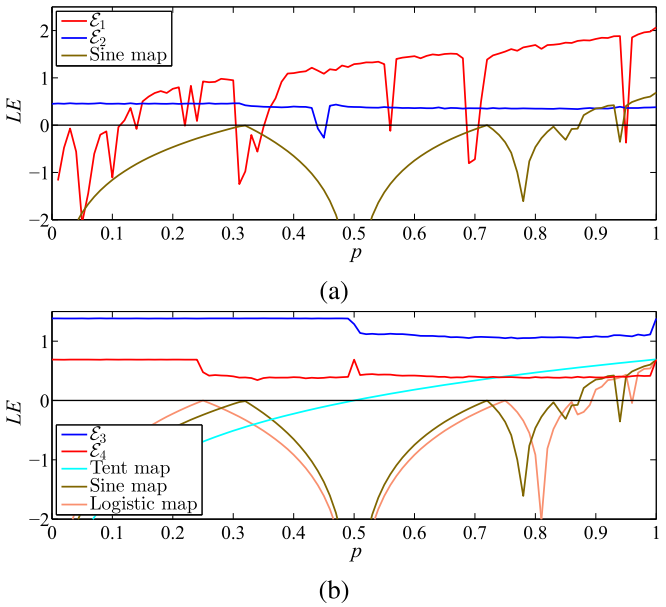


Fig. 11. (a) LE comparisons of $\mathcal{E}_1$, $\mathcal{E}_2$ and Sine map; (b) LE comparisons of $\mathcal{E}_4$, $\mathcal{E}_3$, Tent, Sine and Logistic maps.

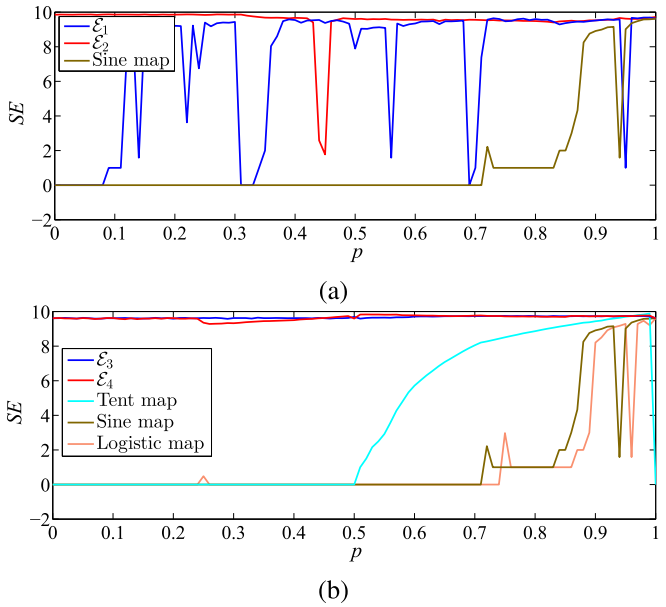


Fig. 12. (a) SE comparisons of $\mathcal{E}_1$, $\mathcal{E}_2$ and Sine map; (b) SE comparisons of $\mathcal{E}_4$, $\mathcal{E}_3$, Tent, Sine and Logistic maps.

seed maps used in the generation procedures, $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ and $\mathcal{E}_4$ have bigger positive LEs in most parameter settings. This means that 1D-NLM can generate chaotic maps with more complicated behaviors.

### B. Shannon Entropy

The SE is a widely used standard to measure the randomness of a data sequence or a signal. To test the randomness of outputs of different chaotic maps, we designed the following experiments for each chaotic map: 1) obtain a time series $\mathbf{z}$ with length 10,000 for different parameter settings; 2) uniformly divide interval $(0, 1)$ into $2^{10}$ sub-intervals and $Pr(i)$ is the frequency of occurrence of $\mathbf{z}$ in the $i$-th sub-interval; 3) calculate SE of $\mathbf{z}$. Fig. 12 plots SEs of different chaotic maps with different parameter settings. We can see that $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ and $\mathcal{E}_4$ have much bigger SEs than the Sine, Tent and Logistic maps in most parameter settings. Moreover, $\mathcal{E}_3$ and $\mathcal{E}_4$ have quite large SEs in the whole parameter settings that are close to the theoretical maximum value 10. With a larger SE, the outputs of a chaotic map distribute more random in the interval $(0, 1)$. The average SEs of different chaotic maps in their respective chaotic ranges are listed in Table IV, from which we can also observe that the new chaotic maps have better ergodicity than their seed maps.

TABLE IV
AVERAGE MEASURE RESULTS OF DIFFERENT CHAOTIC MAPS WITHIN THEIR RESPECTIVE CHAOTIC RANGES

| Chaotic maps | SE | CD |
|---|---|---|
| Sine | 9.150352 | 0.904162 |
| $\mathcal{E}_1$ | **9.269728** | **0.925160** |
| $\mathcal{E}_2$ | **9.662937** | **1.613083** |
| Logistic | 9.072545 | 0.902477 |
| Sine | 9.150352 | 0.904162 |
| Tent | 7.389761 | 0.876820 |
| $\mathcal{E}_3$ | **9.663178** | **1.103635** |
| $\mathcal{E}_4$ | **9.641178** | **1.455635** |

### C. Correlation Dimension

The CD is a type of fractal dimensions and describes the dimensionality of the space occupied by a set of points [46]. It can be used to measure the strangeness of chaotic attractor.

The method proposed in [46] is used to calculate the CDs of different chaotic maps. Fig. 13 plots the experimental results. As can be seen from the figures, the four new chaotic maps have much bigger CDs than their corresponding seed maps in most parameter settings. These seed maps have very small CDs that are close to 0 in many parameter settings. This means that their attractors have low degree of freedom. The average CDs of different chaotic maps in their respective chaotic ranges are listed in the third column of Table IV, in which we can get that $\mathcal{E}_1$, $\mathcal{E}_2$, $\mathcal{E}_3$ and $\mathcal{E}_4$ have larger CDs on average than their seed maps, which means that their attractors can occupy higher dimensionality in their phase planes to make their behaviors more irregular.

### D. Initial State Sensitivity

The initial state sensitivity of a dynamical system can be measured by the correlation coefficient (CC) [37]. An absolute CC closing to 0 means that the two trajectories have weak correlation.

For each chaotic map, the experiment was designed as follows: 1) apply a tiny change to the initial value and generate two trajectories $\mathbf{s}_1$ and $\mathbf{s}_2$ with the same control parameter; 2) apply to a tiny change to the control parameter and

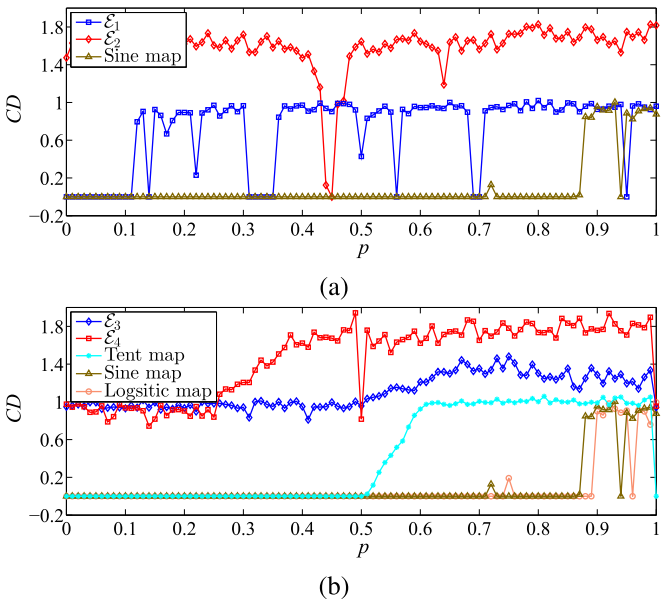


Fig. 13. (a) CD comparisons of $\mathcal{E}_1$, $\mathcal{E}_2$ and Sine map; (b) CD comparisons of $\mathcal{E}_3$, $\mathcal{E}_4$, Tent, Sine and Logistic maps.

TABLE V
AVERAGE ABSOLUTE CCs OF DIFFERENT CHAOTIC MAPS WITHIN THEIR RESPECTIVE CHAOTIC RANGES

| Chaotic maps | CC($\mathbf{s}_1$,$\mathbf{s}_2$) | CC($\mathbf{s}_3$,$\mathbf{s}_4$) |
|---|---|---|
| Sine | 0.173399 | 0.158888 |
| $\mathcal{E}_1$ | **0.037798** | **0.029916** |
| $\mathcal{E}_2$ | **0.178791** | **0.032771** |
| Logistic | 0.201365 | 0.204028 |
| Sine | 0.173399 | 0.158888 |
| Tent | 0.428486 | 0.413691 |
| $\mathcal{E}_3$ | **0.020091** | **0.019763** |
| $\mathcal{E}_4$ | **0.098026** | **0.025788** |

generate two trajectories $\mathbf{s}_3$ and $\mathbf{s}_4$ with the same initial value; 3) calculate CC between $\mathbf{s}_1$ and $\mathbf{s}_2$, and that between $\mathbf{s}_3$ and $\mathbf{s}_4$. Table V lists the average absolute CCs of different chaotic maps in their respective chaotic ranges. As can be seen from the table, the four new chaotic maps have much smaller absolute CCs on average than their seed maps, except for $\mathcal{E}_2$ in applying a tiny change in initial value. Fig. 14 plots the output pairs of $(\mathbf{s}_1, \mathbf{s}_2)$ and $(\mathbf{s}_3, \mathbf{s}_4)$ of these new chaotic maps. These output pairs randomly distribute in the whole phase plane, which straightforwardly display that they have weak correlations.

## VII. PSEUDO-RANDOM NUMBER GENERATOR

For many chaos-based practical applications, their performance is highly dependent on the chaos performance of their used chaotic maps. Because new chaotic maps generated by the proposed 1D-NLM have better chaos performance than

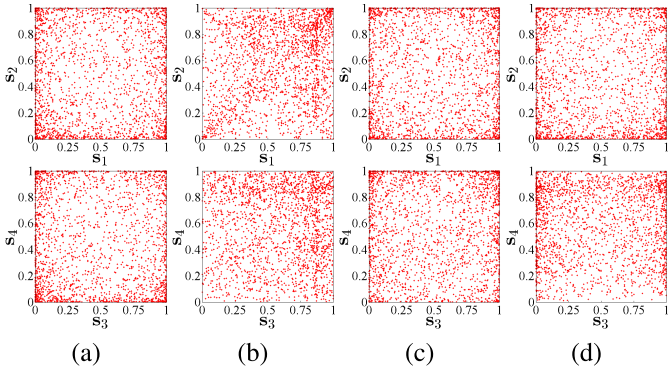


Fig. 14. Output trajectories generated by (a) $\mathcal{E}_1$, (b) $\mathcal{E}_2$, (c) $\mathcal{E}_3$, and (d) $\mathcal{E}_4$ with a tiny change applied to their initial values (the top row) and control parameters (the bottom row).

their seed maps, they are more suitable for many practical applications. To better show this advantage of 1D-NLM, we use a simple chaos-based pseudo-random number generator (PRNG) as an example to compare one of our new chaotic maps with three existing ones.

### A. Chaos-Based PRNG

One widely used method of designing chaos-based PRNGs is to directly use the chaotic trajectories as the random numbers [47]. Suppose sequence $S = \{S(i)|i = 1, 2, \cdots\}$ is a collection of points truncated from a chaotic trajectory. A chaos-based PRNG can be defined as

$$T(t) = Bin\lfloor S(t)\rceil_{32}, \tag{16}$$

where $Bin\lfloor\gamma\rceil_{32}$ is a transformation and truncation function that first converts the float number $\gamma$ into a 52-bit binary string using IEEE 754 Standard [48] and then fetches the $32^{th}$ digital number of the binary string.

In Eq. (16), different chaotic maps can be used to generate the chaotic sequence $S$. Our experiments use the new chaotic map $\mathcal{E}_3$ and three existing 1D chaotic maps (the Logistic, Sine and Tent maps) as the chaotic maps of PRNG. The PRNGs using $\mathcal{E}_3$, Logistic map, Sine map and Tent map are called $\mathcal{E}_3$-based PRNG ($\mathcal{E}_3$-PRNG), Logistic-map-based PRNG (LM-PRNG), Sine-map-based PRNG (SM-PRNG) and Tent-map-based PRNG (TM-PRNG), respectively.

Besides the four chaos-based PRNGs, our experiment also added a PRNG used in MATLAB R2012a software, called MATLAB-PRNG. It uses the built-in function *rand(.)* to generate random numbers and the procedure is shown as

$$T(t) = \begin{cases} 1, & \text{if } rand(1) \geq 0.5 \\ 0, & \text{if } rand(1) < 0.5. \end{cases} \tag{17}$$

### B. Randomness Evaluation

Here, we use the TestU01 to test the randomness of the PRNGs. The TestU01 is a widely used and accepted software library that provides a collection of empirical statistical tests for random numbers [49]. It predefines six test batteries and each test battery contains a collection of statistical tests. Each statistical test is designed to find the non-randomness areas of a

TABLE VI

TESTU01 RESULTS OF DIFFERENT LENGTHS OF BINARY SEQUENCES GENERATED BY VARIOUS PRNGS. $\alpha/\beta$ INDICATES PASSING $\alpha$ OUT OF $\beta$ STATISTICAL TESTS

| Test batteries | *Alphabit* | *BlockAlphabit* | *Rabbit* |
|---|---|---|---|
| $2^{20}$ bits | | | |
| **$\mathcal{E}_3$-PRNG** | **17/17** | **102/102** | **38/38** |
| LM-PRNG | 17/17 | 102/102 | 38/38 |
| SM-PRNG | 17/17 | 102/102 | 38/38 |
| TM-PRNG | 16/17 | 101/102 | 37/38 |
| MATLAB-PRNG | 17/17 | 101/102 | 38/38 |
| $2^{25}$ bits | | | |
| **$\mathcal{E}_3$-PRNG** | **17/17** | **102/102** | **39/39** |
| LM-PRNG | 17/17 | 102/102 | 37/39 |
| SM-PRNG | 15/17 | 91/102 | 34/39 |
| TM-PRNG | 15/17 | 90/102 | 35/39 |
| MATLAB-PRNG | 17/17 | 101/102 | 39/39 |
| $2^{30}$ bits | | | |
| **$\mathcal{E}_3$-PRNG** | **17/17** | **102/102** | **40/40** |
| LM-PRNG | 5/17 | 40/102 | 21/40 |
| SM-PRNG | 0/17 | 6/102 | 10/40 |
| TM-PRNG | 0/17 | 6/102 | 11/40 |
| MATLAB-PRNG | 17/17 | 102/102 | 39/40 |

test sequence from different sides and can generate a $p$-value. The test sequence is considered to pass the statistical test if the obtained $p$-value falls into the interval $[0.001, 0.999]$.

We use the software version of TestU01-1.2.3 provided in [50] to perform our experiments. For each of the five PRNGs, we first randomly generate three binary sequences with lengths $2^{20}$, $2^{25}$ and $2^{30}$ bits, and then use three test batteries, the *Rabbit*, *Alphabit* and *BlockAlphabit* to test the randomness of the three binary sequences. *Alphabit* applies 17 statistical tests. *BlockAlphabit* applies the *Alphabit* test battery repeatedly after reordering the bits by blocks with different sizes 1, 2, 4, 8, 16, 32. Thus, it contains a total number of $17 \times 6 = 102$ statistical tests. *Rabbit* applies 38, 39 and 40 statistical tests for binary sequences with lengths $2^{20}$, $2^{25}$ and $2^{30}$ bits, respectively. Table VI lists the TestU01 results for the four chaos-based PRNGs and MATLAB-PRNG. The LM-PRNG, SM-PRNG and TM-PRGN can pass almost all the statistical tests when the generated binary sequences are of length $2^{20}$ bits. They become to fail some of the statistical tests when the binary sequences increase to $2^{25}$ bits, and they fail to pass most of the statistical tests when the binary sequences increase to $2^{30}$ bits. MATLAB-PRNG fails two tests in *BlockAlphabit* with sequence length as $2^{20}$ and $2^{25}$ bits, and one test in *Rabbit* with sequence length as $2^{30}$ bits. On the other hand, $\mathcal{E}_3$-PRGN can generate different lengths of binary sequences that can pass all the tests. This demonstrates that the new chaotic map $\mathcal{E}_3$ has better randomness and ergodicity, and is more suitable for designing PRNGs.

## VIII. CONCLUSION

This paper introduced 1D-NLM for generating new chaotic maps. It contains six basic nonlinear operations, including four nonlinear operations developed in our previous works and two newly proposed ones. These basic nonlinear operations can be arbitrarily combined to form different complicated operations. The properties of the newly proposed nonlinear operations and complicated operations of 1D-NLM were discussed and their chaotic behaviors were investigated using LE. Four examples of new chaotic maps were generated as examples in 1D-NLM to show its effectiveness and usability. Their dynamics properties were carefully studied and their performance was evaluated in terms of LE, SE, CD and initial state sensitivity. Compared with existing ones, these newly generated chaotic maps have much wider chaotic ranges, their outputs are more random, their attractors have higher degree of freedom, and their initial states are more sensitive. To further demonstrate the effectiveness of 1D-NLM in practical applications, we used chaos-based PRNG as an example to compare one of the new chaotic maps with three existing chaotic maps. Performance test results show that new chaotic map of 1D-NLM is suitable for designing PRNG.

## ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions that greatly contribute to improving the quality of the manuscript.

## REFERENCES

[1] V. G. Ivancevic and T. T. Ivancevic, *Complex Nonlinearity: Chaos, Phase Transitions, Topology Change and Path Integrals*. Berlin, Germany: Springer, 2008.

[2] B. Hasselblatt and A. Katok, *A First Course in Dynamics: With a Panorama of Recent Developments*, 1st ed. Cambridge, U.K.: Cambridge Univ. Press, 2003.

[3] Z. Hua, S. Yi, Y. Zhou, C. Li, and Y. Wu, "Designing hyperchaotic cat maps with any desired number of positive Lyapunov exponents," *IEEE Trans. Cybern.*, to be published.

[4] H. Yang, W. K. S. Tang, G. Chen, and G. P. Jiang, "System design and performance analysis of orthogonal multi-level differential chaos shift keying modulation scheme," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 1, pp. 146–156, Jan. 2016.

[5] C. Shen, S. Yu, J. Lü, and G. Chen, "A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 3, pp. 854–864, Mar. 2014.

[6] P. Ping, F. Xu, and Z. J. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Process.*, vol. 105, no. 12, pp. 419–429, 2014.

[7] Q. Wang, S. Yu, C. Li, J. Lü, X. Fang, C. Guyeux, and J. M. Bahi, "Theoretical design and FPGA-based implementation of higher-dimensional digital chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 3, pp. 401–412, Mar. 2016.

[8] G. Millerioux, J. M. Amigo, and J. Daafouz, "A connection between chaotic and conventional cryptography," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 55, no. 6, pp. 1695–1703, Jul. 2008.

[9] K. Cho and T. Miyano, "Chaotic cryptography using augmented lorenz equations aided by quantum key distribution," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 62, no. 2, pp. 478–487, Feb. 2015.

[10] H. G. Chou, C. F. Chuang, W. J. Wang, and J. C. Lin, "A fuzzy-model-based chaotic synchronization and its implementation on a secure communication system," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 12, pp. 2177–2185, Dec. 2013.

[11] H. Dimassi and A. Loria, "Adaptive unknown-input observers-based synchronization of chaotic systems for telecommunication," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 58, no. 4, pp. 800–812, Apr. 2011.

[12] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.
[13] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using DNA sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[14] Y. Zhang, D. Xiao, Y. Shu, and J. Li, "A novel image encryption scheme based on a linear hyperbolic chaotic system of partial differential equations," *Signal Process., Image Commun.*, vol. 28, no. 3, pp. 292–300, 2013.
[15] P. Ashwin, "Nonlinear dynamics: Synchronization from chaos," *Nature*, vol. 422, no. 6930, pp. 384–385, 2003.
[16] C. Li, S. Li, M. Asim, J. Nunez, G. Alvarez, and G. Chen, "On the security defects of an image encryption scheme," *Image Vis. Comput.*, vol. 27, no. 9, pp. 1371–1381, 2009.
[17] K.-W. Wong, Q. Lin, and J. Chen, "Simultaneous arithmetic coding and encryption using chaotic maps," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 2, pp. 146–150, Feb. 2010.
[18] C. Zhu, L. Zhang, Y. Wang, J. Liu, and L. Mao, "Periodic performance of the chaotic spread spectrum sequence on finite precision," *J. Syst. Eng. Electron.*, vol. 19, no. 4, pp. 672–678, Aug. 2008.
[19] A. N. Srivastava and S. Das, "Detection and prognostics on low-dimensional systems," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 39, no. 1, pp. 44–54, Jan. 2009.
[20] M. Liu, S. Zhang, Z. Fan, and M. Qiu, "$H_\infty$ state estimation for discrete-time chaotic systems based on a unified model," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 42, no. 4, pp. 1053–1063, Aug. 2012.
[21] L. Cong, W. Xiaofu, and S. Songgeng, "A general efficient method for chaotic signal estimation," *IEEE Trans. Signal Process.*, vol. 47, no. 5, pp. 1424–1428, May 1999.
[22] Z. Zhu and H. Leung, "Identification of linear systems driven by chaotic signals using nonlinear prediction," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 49, no. 2, pp. 170–180, Feb. 2002.
[23] Z. Chen, X. Yuan, Y. Yuan, H. H. C. Iu, and T. Fernando, "Parameter identification of chaotic and hyper-chaotic systems using synchronization-based parameter observer," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 63, no. 9, pp. 1464–1475, Sep. 2016.
[24] L. Lin, M. Shen, H. C. So, and C. Chang, "Convergence analysis for initial condition estimation in coupled map lattice systems," *IEEE Trans. Signal Process.*, vol. 60, no. 8, pp. 4426–4432, Aug. 2012.
[25] A. Skrobek, "Cryptanalysis of chaotic stream cipher," *Phys. Lett. A*, vol. 363, nos. 1–2, pp. 84–90, 2007.
[26] T. Yang, L.-B. Yang, and C.-M. Yang, "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett. A*, vol. 245, no. 6, pp. 495–510, 1998.
[27] J. Lü and G. Chen, "A new chaotic attractor coined," *Int. J. Bifurcation Chaos*, vol. 12, no. 3, pp. 659–661, 2002.
[28] Y. Huang, P. Zhang, and W. Zhao, "Novel grid multiwing butterfly chaotic attractors and their circuit design," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 62, no. 5, pp. 496–500, May 2015.
[29] S. Yu, J. Lü, G. Chen, and X. Yu, "Generating grid multiwing chaotic attractors by constructing heteroclinic loops into switching systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 58, no. 5, pp. 314–318, May 2011.
[30] Z. Chen, Y. Yang, and Z. Yuan, "A single three-wing or four-wing chaotic attractor generated from a three-dimensional smooth quadratic autonomous system," *Chaos, Solitons, Fractals*, vol. 38, no. 4, pp. 1187–1196, 2008.
[31] J. Lü, G. Chen, X. Yu, and H. Leung, "Design and analysis of multiscroll chaotic attractors from saturated function series," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 51, no. 12, pp. 2476–2490, Dec. 2004.
[32] T. Zuo, K. Sun, X. Ai, and H. Wang, "High-order grid multiscroll chaotic attractors generated by the second-generation current conveyor circuit," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 10, pp. 818–822, Oct. 2014.
[33] X. Wang and Z. Cheng, "Synchronization of coupled discrete-time harmonic oscillators with rational frequency," *IEEE Trans. Autom. Control*, vol. 58, no. 6, pp. 1573–1579, Jun. 2013.
[34] R. Pagliari and A. Scaglione, "Scalable network synchronization with pulse-coupled oscillators," *IEEE Trans. Mobile Comput.*, vol. 10, no. 3, pp. 392–405, Mar. 2011.
[35] S. Nkomo, M. R. Tinsley, and K. Showalter, "Chimera states in populations of nonlocally coupled chemical oscillators," *Phys. Rev. Lett.*, vol. 110, no. 24, pp. 244102-1–244102-5, 2013.
[36] C. Shen, S. Yu, J. Lu, and G. Chen, "Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 8, pp. 2380–2389, Aug. 2014.
[37] Y. Zhou, Z. Hua, C. M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.
[38] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.
[39] Y. Wu, Y. Zhou, and L. Bao, "Discrete wheel-switching chaotic system and applications," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 12, pp. 3469–3477, Dec. 2014.
[40] Y. Zhou, L. Bao, and C. L. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, pp. 172–182, Apr. 2014.
[41] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.
[42] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.
[43] J. Lin, "Divergence measures based on the Shannon entropy," *IEEE Trans. Inf. Theory*, vol. 37, no. 1, pp. 145–151, Jan. 1991.
[44] Y. Wu, Z. Hua, and Y. Zhou, "*n*-dimensional discrete Cat map generation using Laplace expansions," *IEEE Trans. Cybern.*, vol. 46, no. 11, pp. 2622–2633, Nov. 2016.
[45] P. Grassberger and I. Procaccia, "Characterization of strange attractors," *Phys. Rev. Lett.*, vol. 50, no. 5, pp. 346–349, 1983.
[46] A. M. Albano, J. Muench, C. Schwartz, A. I. Mees, and P. E. Rapp, "Singular-value decomposition and the Grassberger-Procaccia algorithm," *Phys. Rev. A*, vol. 38, no. 6, pp. 3017–3026, 1988.
[47] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*, 1st ed. Boulder, CO, USA: Westview, 2001.
[48] *IEEE Standard for Floating-Point Arithmetic*, IEEE Standard 754-2008, 2008, pp. 1–70.
[49] P. L'Ecuyer and R. Simard, "Testu01: AC library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, p. 22, 2007.
[50] P. L'Ecuyer. (2009). *TestU01*, accessed on Apr. 13, 2017. [Online]. Available: http://simul.iro.umontreal.ca/testu01/tu01.html

**Zhongyun Hua** (S'14–M'16) received the B.S. degree from Chongqing University, Chongqing, China, in 2011, and the M.S. and Ph.D. degrees from the University of Macau, Macau, China, in 2013 and 2016, respectively, all in software engineering.

He is currently an Assistant Professor with the School of Computer Science and Technology, Harbin Institute of Technology Shenzhen Graduate School, Shenzhen, China. His research interests include chaotic system, chaos-based applications, and multimedia security.

**Yicong Zhou** (M'07–SM'14) received the B.S. degree from Hunan University, Changsha, China, and the M.S. and Ph.D. degrees from Tufts University, MA, USA, all in electrical engineering.

He is currently an Associate Professor and the Director of the Vision and Image Processing Laboratory, Department of Computer and Information Science, University of Macau, Macau, China. His research interests include chaotic systems, multimedia security, image processing and understanding, and machine learning.

Dr. Zhou was a recipient of the Third Price of the Macau Natural Science Award in 2014. He serves as a Leading Co-Chair of the Technical Committee on Cognitive Computing in the IEEE Systems, Man, and Cybernetics Society. He serves as an Associate Editor of *Neurocomputing* and the *Journal of Visual Communication and Image Representation*.