Two-Dimensional Parametric Polynomial Chaotic System

Zhongyun Hua, *Member, IEEE*, Yongyong Chen, Han Bao, *Graduate Student Member, IEEE*,
and Yicong Zhou, *Senior Member, IEEE*

Abstract—When used in engineering applications, most existing chaotic systems may have many disadvantages, including discontinuous chaotic parameter ranges, lack of robust chaos, and easy occurrence of chaos degradation. In this article, we propose a two-dimensional (2-D) parametric polynomial chaotic system (2D-PPCS) as a general system that can yield many 2-D chaotic maps with different exponent coefficient settings. The 2D-PPCS initializes two parametric polynomials and then applies modular chaotification to the polynomials. Setting different control parameters allows the 2D-PPCS to customize its Lyapunov exponents in order to obtain robust chaos and behaviors with desired complexity. Our theoretical analysis demonstrates the robust chaotic behavior of the 2D-PPCS. Two illustrative examples are provided and tested based on numeral experiments to verify the effectiveness of the 2D-PPCS. A chaos-based pseudorandom number generator is also developed to illustrate the applications of the 2D-PPCS. The experimental results demonstrate that these examples of the 2D-PPCS can achieve robust and desired chaos, have better performance, and generate higher randomness pseudorandom numbers than some representative 2-D chaotic maps.

Index Terms—Chaotic system, discrete-time system, nonlinear system, pseudorandom number generator (PNG), robust chaos.

I. INTRODUCTION

NONLINEAR dynamical systems have been attracting increasing attention in many research fields [1]–[3]. A chaotic system is a typical type of nonlinear system and it has many unique characteristic properties, including the initial condition sensitivity, unpredictability, and periodic orbits density [4], [5]. Because of these significant properties, chaotic systems are suitable for many practical applications [4], [6], [7]. In particular, chaotic systems are used widely in secure communications [8]–[10] and as pseudorandom number generators (PNGs) [11], [12] because the synchronization of a chaotic system is suitable for carrying secret data [13], [14], and the chaotic systems and PNGs have similar properties in terms of the unpredictability and initial condition sensitivity [6], [15].

Essentially, chaotic systems are mathematical models for describing natural or unnatural phenomena that exhibit chaotic behaviors [16]. The Lorenz system was first built by the meteorologist E. N. Lorenz to simulate the unpredictability of long-term weather changes [17] and many chaotic systems were designed subsequently [18], [19]. The Hénon map and logistic map are two classical chaotic systems [20], where the former is a minimal normal form for describing stretching and folding chaos dynamics, and the latter simulates population growth. These classical chaotic systems have obvious dynamic properties and have been studied widely in many applications [21], [22].

However, due to the rapid increment of computational capacity and the development of technology for discerning chaos, many researchers have shown that some classical chaotic systems have performance shortcomings in practical applications [23]. First, the chaotic behaviors of some chaotic systems can be estimated using various methods, especially artificial intelligence techniques [24], [25]. These chaos estimation techniques predict chaotic behaviors by directly predicting their chaotic time series [24], estimating their control parameters [26], or identifying their initial conditions [27]. Second, these chaotic systems exhibit frail chaos. The phrase frail chaos denotes that the chaotic dynamics are not robust and tiny changes in the system parameters may result in the disappearance of chaos [28]. For example, the chaotic range of the logistic map is discontinuous and many periodic windows exists [29]. The control parameter may fall into the periodic windows when it undergoes a small disturbance, which leads to the disappearance of the logistic map's chaos. Finally, many classical chaotic systems have serious security flaws due to the problem of dynamical degradation [30], [31]. This is because their structures and behaviors are very simple [18]. When simulated on finite-precision platforms, chaos degradation readily occurs [32]. These shortcomings cause defects in many chaos-based applications [33].

Many new chaotic systems have been designed to accommodate chaos-based applications [34], [35]. These new chaotic systems can be divided into two categories. The first category is designed on the basis of existing chaotic systems [34], [35]. For example, Hua and Zhou [36] designed a chaotic framework that generates new chaotic maps with much better performance by using two chaotic maps to be control and seed maps. The other category of new chaotic systems is constructed from linear or nonlinear equations [2], [37]. For example, Wang *et al.* [37] designed a high-dimensional digital chaotic system based on *m* iteration functions. The complex dynamic behavior of the system was demonstrated based on theoretical and experimental results. Compared with classical chaotic systems, these newly obtained chaotic systems result in more complex dynamic properties and better chaos performance, and thus they may be more suitable for some engineering applications. However, these new chaotic systems also have various shortcomings and they cannot satisfy some requirements of many chaos-based applications. In particular, the chaotic behaviors of these systems do not exhibit robust chaos. The phrase robust chaos indicates the nonexistence of periodic windows for the space of system parameter [28]. Thus, the chaotic ranges of these new chaotic systems have periodic windows [36] and small changes to the parameters may make them fall into the periodic windows when used in certain applications. In addition, these new chaotic systems exhibit behaviors with different complexities when different parameter values are used and their chaotic dynamics cannot be controlled, so users cannot obtain the desired chaotic dynamics by specifying their parameters [2]. Thus, designing new chaotic systems with robust chaos and the desired dynamic complexity is attractive and meaningful.

In this study, we present a two-dimensional (2-D) parametric polynomial chaotic system (2D-PPCS), which is directly constructed from general polynomials. The 2D-PPCS is a new 2-D system and totally different from existing ones. It is a general system that can yield many new 2-D chaotic maps with robust chaos and desired complexity of behaviors. Theoretical analysis, experiment results, and application show the superiority of the 2D-PPCS. The main novelty and contributions of this work are summarized as follows.

1) We propose a new 2-D chaotic system, the 2D-PPCS. It is a general system that can yield a large number of 2-D chaotic maps using different exponent coefficient settings. To the best of our knowledge, this is the first time that 2-D chaotic maps are directly generated from general polynomials.

2) Theoretical analysis results demonstrate that the 2D-PPCS can generate robust chaos and behaviors with desired complexity, and has late chaos degradation, and it is able to overcome the disadvantages of existing chaotic systems in discontinuous chaotic parameter ranges.

3) To demonstrate the effectiveness of the 2D-PPCS, we generate two illustrative examples of the 2D-PPCS called 2-D Quadric and 2-D Cubic maps. The property analysis and numeral experiments demonstrate that the 2-D Quadric and 2-D Cubic maps can exhibit robust and desired chaotic behaviors, and they perform better than representative 2-D chaotic maps, such as the Lorenz, Hénon, 2D-LSMCL, and 2D-SLM maps.

4) We apply the 2-D Quadric and 2-D Cubic maps to a PNG to investigate the potential applications of the 2D-PPCS. The simulation results show that they outperform most existing 2-D chaotic maps in this application.

The remainder of this article is organized as follows. In Section II, we review several representative 2-D chaotic maps, as well as discussing their properties. In Section III, we propose the 2D-PPCS and prove its robust chaotic behavior. We provide two illustrative examples of 2D-PPCS in Section IV, and numerical analyses and performance comparisons are presented in Section V. In Section VI, we investigate the application of the 2D-PPCS in a PNG. Finally, we give our conclusions in Section VII.

II. EXISTING 2-D CHAOTIC MAPS

In this section, we introduce four existing 2-D chaotic maps comprising two classical and two recently developed ones.

A. Four 2-D Chaotic Maps

The discrete Lorenz map is the 2-D discrete-time form of the Lorenz system, which is a widely studied three-dimensional (3-D) chaotic systems [38]. The mathematical equation for the discrete Lorenz map is written as

$$\begin{cases} x_{i+1} = (1+ab)x_i - bx_iy_i \\ y_{i+1} = (1-b)y_i + bx_i^2 \end{cases} \quad (1)$$

where *a* and *b* are two system parameters. The discrete Lorenz map exhibits obvious chaotic behavior when its parameters $a = 1.05$ and $b = 0.75$.

The Hénon map is named after M. Hénon [18] and its mathematical definition is written as

$$\begin{cases} x_{i+1} = 1 - ax_i^2 + y_i \\ y_{i+1} = bx_i \end{cases} \quad (2)$$

where *a* and *b* are two system parameters. The Hénon map is also a commonly studied prototype for 2-D chaotic system and it exhibits obvious chaotic behavior when $a = 1.4$ and $b = 0.3$.

The 2-D-logistic-modulated-sine-coupling-logistic chaotic (2D-LSMCL) map is a new chaotic map which is developed from the classical logistic and sine maps [39]. The 2D-LSMCL map was generated by first modulating the sine map using the logistic map, and then coupling the outputs from the logistic and sine maps, and finally extending the phase plane of trajectory from one-dimensional (1-D) to 2-D. Mathematically, the 2D-LSMCL map is defined as

$$\begin{cases} x_{i+1} = (\sin(4\pi ay_i(1-y_i)) + b)x_i(1-x_i) \\ y_{i+1} = (\sin(4\pi ax_{i+1}(1-x_{i+1})) + b)y_i(1-y_i) \end{cases} \quad (3)$$

where *a* and *b* are system parameters. The 2D-LSMCL map exhibits obvious chaotic behavior when $a = 0.75$ and $b = 3$.

A 2-D chaotic system called 2D-SLM map is also developed on the basis of the logistic and sine maps [40]. First, the sine map is combined with a parameter *b*. Then, the output from the logistic map is then modulated by using this combination
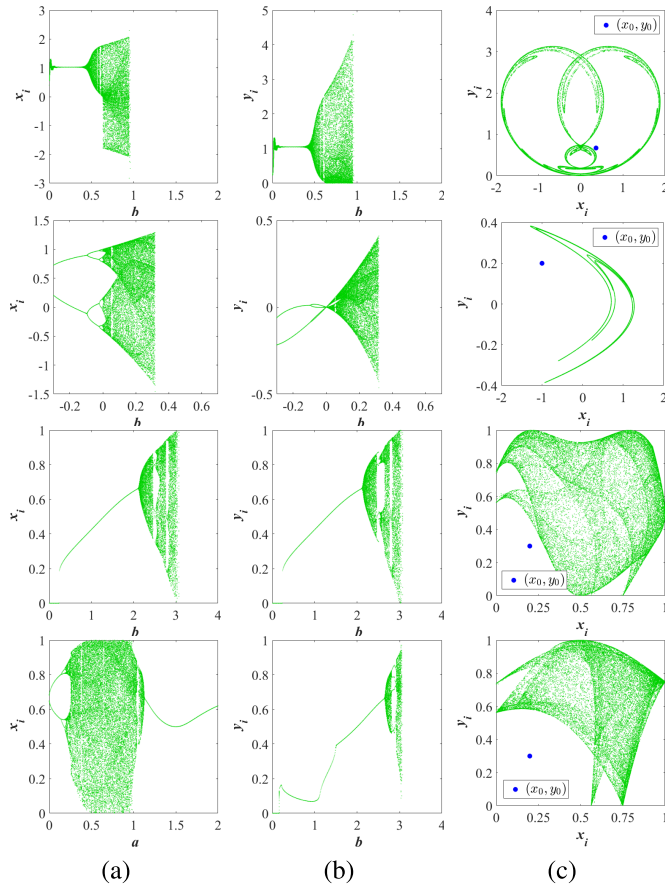
Fig. 1. Bifurcation diagrams and trajectories obtained for existing types of 2-D chaotic maps. From top to bottom, the four plots show the (a) bifurcation diagrams for variable x_i, (b) bifurcation diagrams for variable y_i, and (c) trajectories of (x_i, y_i) for the discrete Lorenz map, Hénon map, 2D-LSMCL map, and 2D-SLM map, respectively.

to improve its nonlinearity. Finally, the outputs are extended to 2-D from 1-D. The 2D-SLM map is mathematically written as

$$\begin{cases} x_{i+1} = a(\sin(\pi y_i) + b)x_i(1 - x_i) \\ y_{i+1} = a(\sin(\pi x_{i+1}) + b)y_i(1 - y_i) \end{cases} \quad (4)$$

where a and b are system parameters. The 2D-SLM map exhibits obvious chaotic behavior when $a = 1$ and $b = 3$.

B. Analysis of Dynamics

For a 2-D dynamical system, a bifurcation diagram plots its variable x_i or y_i as the control parameters change, and the trajectory represents the variables (x_i, y_i) by setting its parameters as fixed values. Fig. 1 demonstrates these bifurcation diagrams and trajectories for the discrete Lorenz, Hénon, 2D-LSMCL, and 2D-SLM maps. To illustrate the dynamics properties for these 2-D chaotic maps in a straightforward manner, the bifurcation diagrams were plotted while changing one parameter b and keeping the other parameter a as a fixed value, thereby making the related chaotic system exhibit obvious chaotic behavior. In particular, the parameter a was set as 1.05, 1.4, 0.75, and 1 in the discrete Lorenz, Hénon, 2D-LSMCL, and 2D-SLM maps, respectively. The trajectories of these 2-D chaotic maps were plotted by setting their parameters as fixed values. In particular, the parameters (a, b) were set

as $(1.05, 0.75)$, $(1.4, 0.3)$, $(0.75, 3)$, and $(1, 3)$ in the discrete Lorenz, Hénon, 2D-LSMCL, and 2D-SLM maps, respectively. Clearly, these 2-D chaotic maps have some obvious properties. First, their chaotic behaviors occur only in very narrow data ranges and their chaotic parameter ranges exist many periodic windows and thus are discontinuous. Small disturbances to the parameters may make them fall into the periodic windows and thus cause disappearance of chaos. Second, the outputs of the chaotic maps are distributed over a quite small data range and they have obvious patterns, thereby indicating that the outputs do not exhibit high randomness. Additionally, the complexity of the chaotic dynamics cannot be controlled. Thus, users cannot obtain desired and stable chaotic dynamics by predefining the control parameters. These properties cause defects in many chaos-based applications [23], [41].

III. 2D-PPCS AND ITS CHAOTIC BEHAVIOR

A. 2D-PPCS

We present the 2D-PPCS for generating chaotic maps with robust chaos and behaviors with the desired complexity. Modular operation can fold any value into a fixed range, so modular chaotification is employed to generate the 2D-PPCS from nonlinear polynomials. First, we initialize two parametric polynomials $F(x, y) = ax + cy^\gamma$ and $G(x, y) = by$. Modular chaotification is then applied to $F(x, y)$ and $G(x, y)$ to obtain two 2-D equations. After writing the 2-D equations in discrete time forms, we can obtain the 2D-PPCS as

$$\begin{cases} x_{i+1} = (ax_i + cy_i^\gamma) \mod \beta \\ y_{i+1} = by_i \mod \beta \end{cases} \quad (5)$$

where x_i and y_i are two variables at the ith observation time, a, b, and c are control parameters, γ indicates the exponent coefficient, and β is the modular coefficient.

It is well known that linear equations cannot generate chaos, whereas nonlinear polynomials contain sufficient nonlinear operations to exhibit complex nonlinear properties. Thus, many chaotic systems are built from nonlinear polynomials, including the logistic map and Lorenz system family. However, these chaotic systems exist some obvious shortcomings. First, they can achieve chaotic behaviors with only a small number of parameter settings. For example, the logistic map produces chaotic behavior only in the parameter range of $[3.57, 4]$ [36]. Second, many periodic windows occur in their parameter space, which leads to frail chaotic behaviors that readily disappear when the parameters are disturbed. Finally, the complexity of the chaotic dynamics cannot be controlled, and thus we may not obtain desired and stable chaotic dynamics by predefining the control parameters. These happen because these chaotic systems are all built from nonlinear polynomials with special structures and their control parameters can only have some small values. When the control parameters are specified as some large values, the phase planes become uncompacted and their trajectories diverge to infinity.

The modular operation can always fold the phase plane for any input and it is a bounded nonlinear transform. When it is employed to generate chaos from nonlinear polynomials, the control parameters can be any large value and the system structures can be specified. Thus, the proposed 2D-PPCS can

exhibit the following properties: 1) the exponent coefficient γ determines the complexity of the nonlinear polynomials in the 2D-PPCS. Thus, setting γ to different values can obtain different chaotic maps; 2) the control parameters can be very large values for the 2D-PPCS; and 3) the 2D-PPCS can exhibit robust chaos and behaviors with desired complexity by predefining its control parameters. These properties are theoretically proved in Section III-B and experimental verifications are presented in Section V.

B. Proof of Chaotic Behavior

The 2D-PPCS constructed according to (5) can achieve robust chaos and dynamical behaviors with desired complexity. We use the Lyapunov exponent (LE) to prove this property. The LE is a commonly used measurement for indicating whether the chaos exist or not [42]. The LE metric defines chaos by characterizing the separation rate of two extremely close trajectories of a nonlinear system. A multidimensional dynamical system has several LEs that describe the separation of close phase plane trajectories from different directions. The LE number for a multidimensional dynamical system equals to the dimensionality of its phase plane. Thus, the 2D-PPCS has two LEs for describing the separation rate of the system in two directions.

1) Definition of Chaos: Let the 2-D discrete-time differentiable dynamical system be

$$\mathbf{C}(x, y) : \begin{cases} x_{i+1} = C_1(x_i, y_i) \\ y_{i+1} = C_2(x_i, y_i) \end{cases}$$

and the two LEs can be calculated as [42]

$$LE_j = \lim_{t \to \infty} \frac{1}{t} \ln \lambda_j(\mathbf{J}) \tag{6}$$

where $j = 1$ or 2, $\lambda_1(\mathbf{J})$ and $\lambda_2(\mathbf{J})$ are the two eigenvalues for the 2-D matrix $\mathbf{J}$, and $\mathbf{J} = \mathbf{J}(x_0, y_0)\mathbf{J}(x_1, y_1) \cdots \mathbf{J}(x_{t-1}, y_{t-1})$. $\mathbf{J}(x_i, y_i)$ is the Jacobian matrix for the dynamical system $\mathbf{C}(x, y)$ at the iteration i and

$$\mathbf{J}(x_i, y_i) = \begin{pmatrix} \frac{\partial C_1(x,y)}{\partial x}\Big|_{(x_i,y_i)} & \frac{\partial C_1(x,y)}{\partial y}\Big|_{(x_i,y_i)} \\ \frac{\partial C_2(x,y)}{\partial x}\Big|_{(x_i,y_i)} & \frac{\partial C_2(x,y)}{\partial y}\Big|_{(x_i,y_i)} \end{pmatrix}.$$

If a dynamical system has a positive LE, then its close trajectories will diverge with each unit time. If a nonlinear system can achieve two or more positive LEs, then its close trajectories diverge in multi dimensions. A larger positive LE denotes that the extremely close phase plane trajectories of the system diverge more quickly. The definition of chaos can be described according to Definition 1 [42].

Definition 1: A nonlinear system has chaotic behavior in the sense of LE if: 1) it has at least one positive LE and 2) it has the globally bounded phase plane.
Using Definition 1, we can decide whether a 2-D dynamical system exhibits chaotic behavior.

2) Chaos of the 2D-PPCS: First, we give Proposition 1 to show the chaotic behaviors of the constructed 2D-PPCS.

Proposition 1: The 2D-PPCS in (5) has chaotic behavior if its two system parameters a and b satisfy that $|a \cdot b| > 1$.

Proof: The Jacobian matrix of the 2D-PPCS in (5) at the observation i is

$$\mathbf{J}(x_i, y_i) = \begin{pmatrix} a & c \cdot \gamma \cdot y_i^{\gamma-1} \\ 0 & b \end{pmatrix}.$$

Then, the multiplications of the Jacobian matrices from observation 0 to observation $t - 1$ is calculated as

$$\begin{aligned} \mathbf{J} &= \mathbf{J}(x_0, y_0)\mathbf{J}(x_1, y_1) \ldots \mathbf{J}(x_{t-1}, y_{t-1}) \\ &= \begin{pmatrix} a & c \cdot \gamma \cdot y_0^{\gamma-1} \\ 0 & b \end{pmatrix} \times \cdots \times \begin{pmatrix} a & c \cdot \gamma \cdot y_{t-1}^{\gamma-1} \\ 0 & b \end{pmatrix} \\ &= \begin{pmatrix} a^t & A(a, b, c, \gamma, y_0, y_1, \ldots, y_{t-1}) \\ 0 & b^t \end{pmatrix} \end{aligned}$$

where $A(a, b, c, \gamma, y_0, y_1, \ldots, y_{t-1})$ is a certain value represented by $a, b, c, \gamma, y_0, y_1, \ldots, y_{t-1}$. Let $\lambda_1(\mathbf{J})$ and $\lambda_2(\mathbf{J})$ be the two eigenvalues of $\mathbf{J}$. It is obvious that the $\lambda_1(\mathbf{J})$ and $\lambda_2(\mathbf{J})$ are independent from $A(a, b, c, \gamma, y_0, y_1, \ldots, y_{t-1})$ and can be obtained as $\lambda_1(\mathbf{J}) = a^t$ and $\lambda_2(\mathbf{J}) = b^t$. According to the LE definition shown in (6), the two LEs of the 2D-PPCS are

$$\begin{aligned} LE_1 &= \lim_{t \to \infty} \frac{1}{t} \ln \lambda_1(\mathbf{J}) \\ &= \lim_{t \to \infty} \frac{1}{t} \ln(a^t) \\ &= \ln(a) \end{aligned} \tag{7}$$

and

$$\begin{aligned} LE_2 &= \lim_{t \to \infty} \frac{1}{t} \ln \lambda_2(\mathbf{J}) \\ &= \lim_{t \to \infty} \frac{1}{t} \ln(b^t) \\ &= \ln(b). \end{aligned} \tag{8}$$

Since $|a \cdot b| > 1$, at least one of $|a|$ and $|b|$ is larger than 1. Then one can deduce that at least one of LE_1 and LE_2 is larger than 0. Then the condition 1) in Definition 1 has been satisfied.

Additionally, because the modular operation can always fold any input to a fixed range, the 2D-PPCS in (5) has a globally bounded phase plane. Then the condition 2) in Definition 1 has also been satisfied and thus the 2D-PPCS has chaotic behavior. This does the proof. ∎

Proposition 1 states that the 2D-PPCS always exhibits chaotic behavior when its two parameters a and b have $|a \cdot b| > 1$. Table I lists the two LEs for the 2D-PPCS with several settings for a and b. The 2D-PPCS has two positive LEs with these settings of parameters, thereby indicating that it can achieve hyperchaotic behavior. From (7) and (8), the two LEs for the 2D-PPCS are totally determined by its parameters, a and b.

C. Discussions

Because the two LEs of the 2D-PPCS are directly determined by its parameters, a and b. Users can customize the LEs for the 2D-PPCS by setting the two parameters a and b to specific values. Thus, the 2D-PPCS can achieve the following advantages.

TABLE I
TWO LEs OF THE 2D-PPCS WITH VARIOUS PARAMETERS a AND b

| a	LE_1	b	LE_2
2	$LE_1 = \ln(a) = 0.6931$	2	$LE_2 = \ln(b) = 0.6931$
3	$LE_1 = \ln(a) = 1.0986$	3	$LE_2 = \ln(b) = 1.0986$
4	$LE_1 = \ln(a) = 1.3863$	4	$LE_2 = \ln(b) = 1.3863$
5	$LE_1 = \ln(a) = 1.6094$	5	$LE_2 = \ln(b) = 1.6094$
6	$LE_1 = \ln(a) = 1.7918$	6	$LE_2 = \ln(b) = 1.7918$
7	$LE_1 = \ln(a) = 1.9459$	7	$LE_2 = \ln(b) = 1.9459$
8	$LE_1 = \ln(a) = 2.0794$	8	$LE_2 = \ln(b) = 2.0794$
9	$LE_1 = \ln(a) = 2.1972$	9	$LE_2 = \ln(b) = 2.1972$
10	$LE_1 = \ln(a) = 2.3026$	10	$LE_2 = \ln(b) = 2.3026$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

Fig. 2. Top row shows the bifurcation diagrams for the variable x_i in the 2-D Quadric map with the parameter pairs: (a) $a, b \in (1, 100)$, (b) $a, c \in (1, 100)$, and (c) $b, c \in (1, 100)$; and bottom row shows the corresponding bifurcation diagrams for the variable y_i.
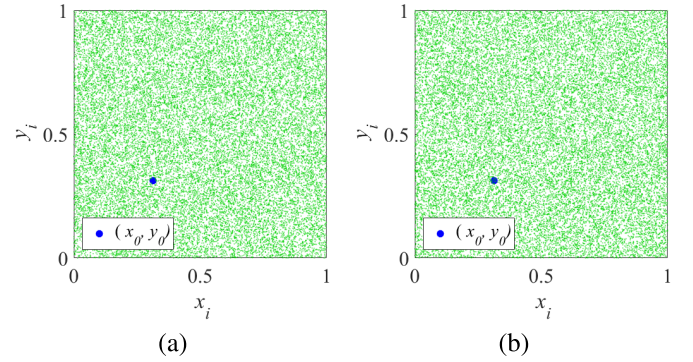

Fig. 3. Trajectories of the (a) 2-D Quadric map and (b) 2-D Cubic map with control parameters comprising $(a, b, c) = (49, 49, 49)$.

1) Because the state space in digital platforms cannot have infinite states, all self-evolved systems without external disturbance will finally result in periodic behaviors [30]. Thus, all chaotic systems unavoidably have chaos degradation if the evolution time is long enough. However, the 2D-PPCS has late chaos degradation for the two reasons: 1) it has continuous chaotic ranges, which is proved by Proposition 1 and experiments in Fig. 5(e) and 2) its output states cannot overlap in a long iteration, which is verified by the experiment results in Table VI.

2) The proposed 2D-PPCS has robust chaos. However, most existing chaotic systems do not have this property. The robust chaos is defined as the inexistence of periodic windows in the neighborhood of parameter space and it is a strongly desired property for many chaos-based applications [28].

3) The 2D-PPCS has more complex dynamics properties than some representative 2-D chaotic maps, which can be seen from the comparisons in Section V.

4) The 2D-PPCS is more suitable for many chaos-based applications than representative 2-D chaotic maps. For example, the PNG application. This will be verified by the test results in Table VI. This is because the 2D-PPCS generates robust behaviors with desired complexity by setting its two parameters as specific values. However, other 2-D chaotic maps do not have this property.

Using the same construction method, 3-D or even higher-dimensional polynomial chaotic systems can be generated. However, high-dimensional chaotic systems have more control parameters. To obtain robust chaos and behaviors with desired complexity, the relationship between these parameters should be reconsidered.

IV. TWO ILLUSTRATIVE EXAMPLES

The exponent coefficient γ in (5) determines the complexity of the nonlinear polynomials in the 2D-PPCS. Setting γ at various values can obtain different 2-D chaotic maps with diverse levels of complexity. In the following, we consider two illustrative examples of the 2D-PPCS where γ is set as two and three. The modular coefficient β is set to one but users can set it to other values.
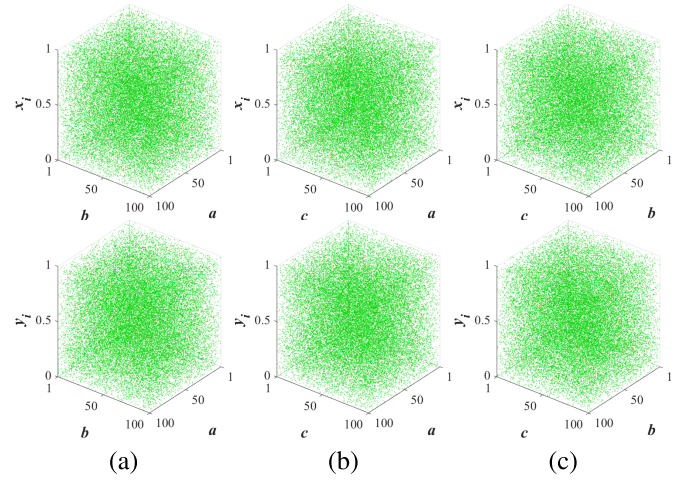
A. 2-D Quadric Map

1) Definition: When the exponent coefficient γ is set at two, the 2D-PPCS in (5) becomes a 2-D Quadric map and its definition is

$$\begin{cases} x_{i+1} = (ax_i + cy_i^2) \mod 1 \\ y_{i+1} = by_i \mod 1 \end{cases} \tag{9}$$

where a, b, and c are system parameters for the 2-D Quadric map. According to Proposition 1, the 2-D Quadric map exhibits chaotic behavior when its control parameters $|a \cdot b| > 1$. Thus, we investigated the behavior of the 2-D Quadric map when its parameters comprised $a, b, c \in (1, 100)$.

2) Bifurcation Diagram and Trajectory: The bifurcation diagram and phase plane trajectory of the 2-D Quadric map are investigated to understand its dynamical behavior with different parameters. Fig. 2 plots the bifurcation diagrams for the 2-D Quadric map from a 3-D viewpoint. According to these diagrams, the variables x_i and y_i are uniformly distributed throughout the whole data range with different parameter settings. Fig. 3(a) shows the trajectory for the 2-D Quadric map under a fixed parameter setting. The trajectory could also randomly visit or approach all the areas of the data range, which indicates that the 2-D Quadric map can output uniform states and exhibit robust chaotic behavior.

3) Equilibrium Point and Stability: An equilibrium point describes that a dynamical system's domain exists an element that allows the system map to the element. In particular, x demonstrates an equilibrium point of f if it satisfies that $f(\ldots f(x)\ldots) = x$. All the equilibrium points of the 2-D Quadric map are the solutions of the equation as follows:

$$\begin{cases} x = (ax + cy^2) \mod 1 \\ y = by \mod 1. \end{cases} \tag{10}$$

By solving the equation above, we can find that the 2-D Quadric map owns various numbers of equilibrium points with different control parameters. An equilibrium point can indicate an unstable or stable state. An unstable equilibrium point repels the neighboring states and makes the system unstable, whereas a stable equilibrium point attracts the neighboring states of the trajectories in the phase plane and the system will become stable as the time increases. Thus, a system will remain locally stable over a long period if its equilibrium point is stable. The system is locally unstable if all the equilibrium points are unstable. Furthermore, a locally unstable system is considered to exhibit chaotic behavior if it is also globally stable. The stability can be indicated by the eigenvalues of the system's Jacobian matrix. Let the two eigenvalues of a 2-D dynamical system's Jacobian matrix be λ_1 and λ_2. Then, the system is locally stable if $|\lambda_1| < 1$ and $|\lambda_2| < 1$, whereas it is locally unstable if $|\lambda_1| > 1$ or (and) $|\lambda_2| > 1$. The Jacobian matrix for the 2-D Quadric map is calculated as

$$\mathbf{J} = \begin{pmatrix} a & 2 \cdot c \cdot y_i \\ 0 & b \end{pmatrix}.$$

Clearly, the two eigenvalues of the 2-D Quadric map's Jacobian matrix are $\lambda_1 = a$ and $\lambda_2 = b$, and they are independent of the observation state of the 2-D Quadric map. Thus, when $a, b \in (1, 100)$, the two eigenvalues always satisfy that $|\lambda_1| > 1$ and $|\lambda_2| > 1$, which denotes that all these equilibrium points have unstable state. According to (10), the 2-D Quadric map has an equilibrium point at $(0, 0)$ for any parameter setting. It also has many nonzero equilibrium points on $I \in [0, 1)$ with different parameter settings. Table II lists the nonzero equilibrium points and their eigenvalues for the Jacobian matrix under two parameter settings. All the eigenvalues are larger than one, thereby indicating the unstable state of the 2-D Quadric map.

B. 2-D Cubic Map

1) Definition: When we set the exponent coefficient γ to three, the 2D-PPCS in (5) yields a 2-D Cubic map, which is defined by

$$\begin{cases} x_{i+1} = (ax_i + cy_i^3) \mod 1 \\ y_{i+1} = by_i \mod 1 \end{cases} \tag{11}$$

where a, b, and c are also system parameters. The 2-D Cubic map can also exhibit chaotic behavior when its parameters satisfy $|a \cdot b| > 1$. We set the control parameters in the same ranges as those for the 2-D Quadric map, i.e., $a, b, c \in (1, 100)$.

2) Bifurcation Diagram and Trajectory: Fig. 4 depicts the bifurcation diagrams for the 2-D Cubic map from a 3-D viewpoint. Each diagram plots the states visited by the variable

TABLE II
NONZERO EQUILIBRIUM POINTS OF THE 2-D QUADRIC MAP AND EIGENVALUES OF THE JACOBIAN MATRIX UNDER TWO PARAMETER SETTINGS

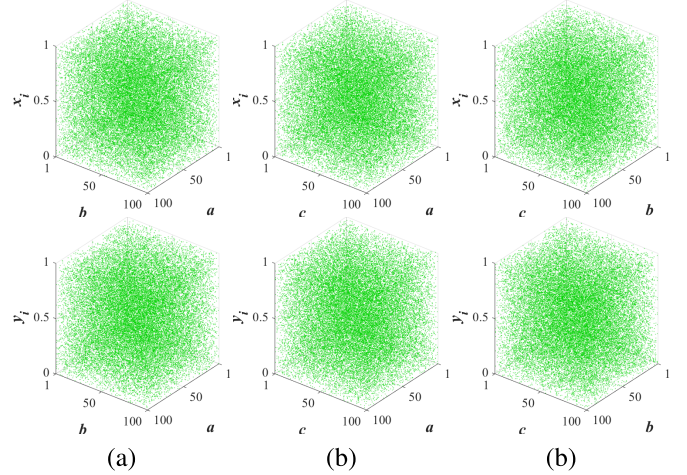| (a, b, c)	Equilibrium points $(\tilde{x}, \tilde{y})$	Eigenvalues
$(4, 4, 4)$	$(0.185, 0.333)$, $(0.519, 0.333)$ $(0.852, 0.333)$, $(0.073, 0.667)$ $(0.407, 0.667)$, $(0.740, 0.667)$	$\lambda_1 = 4$ $\lambda_2 = 4$
$(6, 5, 5)$	$(0.137, 0.250)$, $(0.422, 0.250)$ $(0.538, 0.250)$, $(0.738, 0.250)$ $(0.937, 0.250)$, $(0.938, 0.250)$ $(0.150, 0.500)$, $(0.350, 0.500)$ $(0.550, 0.500)$, $(0.750, 0.500)$ $(0.950, 0.500)$, $(0.038, 0.750)$ $(0.237, 0.750)$, $(0.437, 0.750)$ $(0.438, 0.750)$, $(0.637. 0.750)$ $(0.838, 0.750)$	$\lambda_1 = 6$ $\lambda_2 = 5$
$\vdots$	$\vdots$	$\vdots$

Fig. 4. Top row shows the bifurcation diagrams for the variable x_i in the 2-D Cubic map with the parameter pairs: (a) $a, b \in (1, 100)$, (b) $a, c \in (1, 100)$, and (c) $b, c \in (1, 100)$; and bottom row shows the corresponding bifurcation diagrams for the variable y_i.

x_i or y_i when the parameter pairs are (a, b), (a, c), or (b, c). Clearly, under different parameter settings, the results show that the variables x_i and y_i are always uniformly distributed throughout the whole data range. This indicates that the 2-D Cubic map can exhibit complex chaotic behaviors in the whole parameter space and its chaotic range is continuous. However, observed from Fig. 1, the four existing 2-D chaotic maps show chaotic behaviors only in small parameter spaces and their outputs cannot distribute uniformly. Besides, their chaotic ranges are discontinuous. With uniformly distributed outputs, the 2-D Cubic map is more suitable for many applications. This will be verified by the PNG application in Section VI.

Fig. 3(b) plots the phase plane trajectory of the 2-D Cubic map for the parameter settings of $(a, b, c) = (49, 49, 49)$. It is obvious that the variable pair (x_i, y_i) of the 2-D Cubic map can also randomly visit all the areas of the 2-D phase plane, which is similar with that of the 2-D Quadric map in Fig. 3(a). This is because both the 2-D Quadric and 2-D Cubic maps
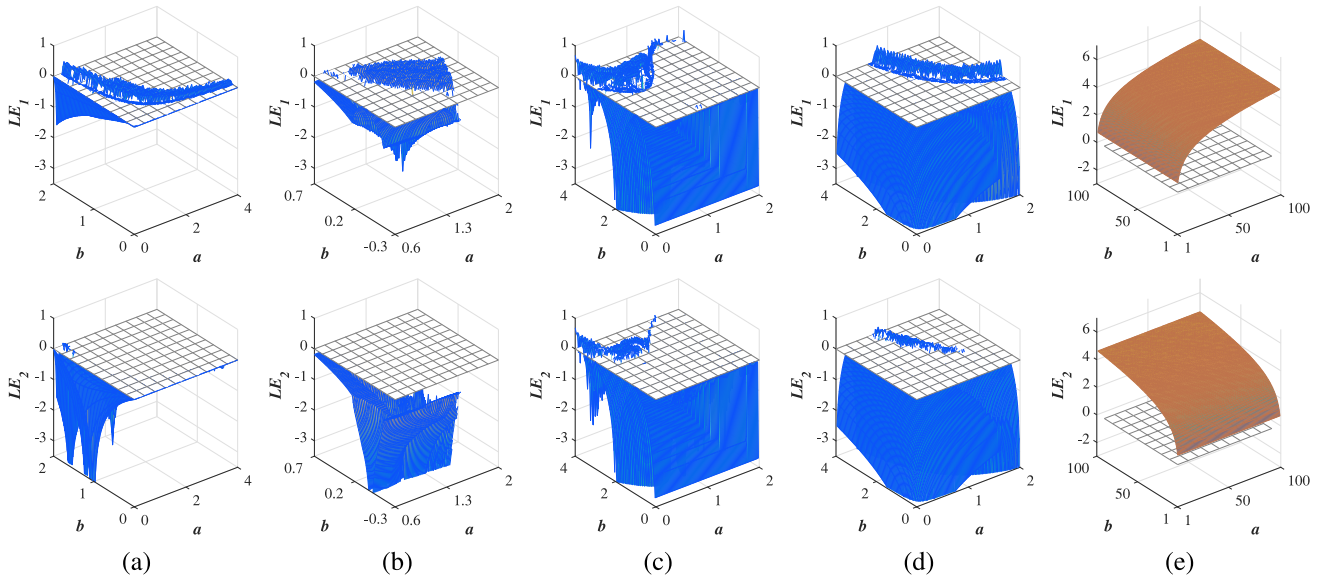
Fig. 5. Two LEs for the (a) discrete Lorenz map, (b) Hénon map, (c) 2D-LSMCL map, (d) 2D-SLM map, and (e) 2-D Quadric and 2-D Cubic maps.

have complex behaviors and their trajectories can randomly visit all the areas of the phase plane. However, even the two chaotic maps have similar trajectories in the global view, their trajectories are completely different in the local view.

3) Equilibrium Points and Stability: The equilibrium points for the 2-D Cubic map are the solutions of the equation

$$\begin{cases} x = (ax + cy^3) \mod 1 \\ y = by \mod 1. \end{cases} \quad (12)$$

Clearly, the point $(0, 0)$ is a solution of the equation above. The 2-D Cubic map has many nonzero equilibrium points for different settings of parameters. The Jacobian matrix for the 2-D Cubic map can be obtained as

$$\mathbf{J} = \begin{pmatrix} a & 3 \cdot c \cdot y_i^2 \\ 0 & b \end{pmatrix}.$$

The two eigenvalues for the Jacobian matrix are also $\lambda_1 = a$ and $\lambda_2 = b$, and they are independent of the observation states, x_i and y_i. When $a, b \in (1, 100)$, the two eigenvalues always have $|\lambda_1| > 1$ and $|\lambda_2| > 1$, and all these equilibrium points show unstable for the 2-D Cubic map. Table III lists the nonzero equilibrium points for the 2-D Cubic map and the eigenvalues of the Jacobian matrix with two-parameter settings. All the eigenvalues are larger than one, which indicates the locally unstable property of the 2-D Cubic map.

V. NUMERAL EXPERIMENTS

To demonstrate the robust chaotic behaviors and desired dynamics properties of the 2-D Quadric and 2-D Cubic maps, we numerically analyzed the chaotic behaviors of the two 2-D chaotic maps based on the LE, Kolmogorov entropy (KE), correlation dimension (CD), and initial state sensitivity. The chaotic behaviors and dynamic properties of the 2-D Quadric and 2-D Cubic maps are determined by their parameters a and b, and we set the parameter $c = 49$ in our experiments.

TABLE III
NONZERO EQUILIBRIUM POINTS FOR THE 2-D CUBIC MAP AND EIGENVALUES OF THE JACOBIAN MATRIX UNDER TWO PARAMETER SETTINGS

(a, b, c)	Equilibrium points $(\tilde{x}, \tilde{y})$	Eigenvalues
$(4, 4, 4)$	$(0.284, 0.333)$, $(0.617, 0.333)$ $(0.951, 0.333)$, $(0.271, 0.667)$ $(0.604, 0.667)$, $(0.938, 0.667)$	$\lambda_1 = 4$ $\lambda_2 = 4$
$(6, 5, 5)$	$(0.184, 0.250)$, $(0.384, 0.250)$ $(0.584, 0.250)$, $(0.784, 0.250)$ $(0.984, 0.250)$, $(0.075, 0.500)$ $(0.275, 0.500)$, $(0.475, 0.500)$ $(0.675, 0.500)$, $(0.875, 0.500)$ $(0.178, 0.750)$, $(0.378, 0.750)$ $(0.578, 0.750)$, $(0.778, 0.750)$ $(0.978, 0.750)$	$\lambda_1 = 6$ $\lambda_2 = 5$
$\vdots$	$\vdots$	$\vdots$

A. LE

As described in Section III-B, the LE is an indicator of chaotic behavior and a larger positive LE value indicates more rapid divergence of the neighboring trajectories of a system. A dynamical system exhibits chaotic behavior if it has positive LE(s) and its phase plane is globally stable.

To demonstrate the superior performance of the constructed 2-D Quadric and 2-D Cubic maps, we compared their LEs with those for the four 2-D chaotic maps presented in Section II, comprising two classical maps, i.e., the discrete Lorenz map [38] and Hénon map [18], and two recently developed chaotic maps, i.e., the 2-D LSMCL map [39] and 2-D SLM map [40]. In our experiments, we used the LE calculation toolbox LET[1] to calculate the LEs of different chaotic maps. Fig. 5 compares

[1] https://ww2.mathworks.cn/matlabcentral/fileexchange/233-let?requestedDomain=zh

the LE values for these 2-D chaotic maps. The two LEs for the 2-D Quadric and 2-D Cubic maps are shown in the same figures because their LEs are the same when they have same parameters, as shown by (7) and (8). The results demonstrate that the discrete Lorenz, Hénon, 2-D LSMCL, and 2-D SLM maps can achieve positive LEs only with a few parameter values, and they have discontinuous chaotic ranges. Small changes to the control parameters can cause the disappearance of their chaos. By contrast, the 2-D Quadric and 2-D Cubic maps can achieve two positive LEs over the whole parameter range, where their LEs are much larger and the chaotic ranges are continuous and much wider compared with those for the four other 2-D chaotic maps. These findings indicate that the 2-D Quadric and 2-D Cubic maps exhibit robust hyperchaotic behavior and they can obtain better performance compared with these other 2-D chaotic maps.

B. KE

The KE is a type of entropy metric that provides a theoretical explanation for the distribution of finite states. This entropy can describe the required information to forecast the current output of a chaotic system from its previous t outputs. The KE is defined according to Definition 2 [43].

Definition 2: The phase plane is divided into D-dimensional hypercubes with content ϵ^D and $P(i_0, \ldots, i_n)$ is the probability that a phase plane trajectory is in hypercube i_0 at $t = 0$, i_1 at $t = T$, $\ldots$, i_n at $t = nT$. Then, the KE is defined as

$$K = \lim_{T \to 0} \lim_{\epsilon \to 0^+} \lim_{N \to \infty} \frac{1}{NT} \sum_{n=0}^{N-1} (K_{n+1} - K_n) \quad (13)$$

where $K_{n+1} - K_n$ is the required information to forecast that the phase plane trajectory of the hypercube at $(n+1)T$ given the trajectories up to nT, and K_n can be calculated as

$$K_n = -\sum_{i_0, \ldots, i_n} P(i_0, \ldots, i_n) \ln P(i_0, \ldots, i_n). \quad (14)$$

A positive KE indicates that extra information is required to forecast the trajectory of a nonlinear system and a larger KE denotes that more information is required. Thus, a nonlinear system owning a positive KE is considered to own unpredictability and a larger KE the denotes better performance of unpredictability.

In our experiments, we used the 12000 states of a system's trajectory to calculate the KEs for different 2-D chaotic maps and Fig. 6 demonstrates the results obtained. The parameters for these 2-D chaotic maps are the same as those employed in the LE experiments. Clearly, the 2-D Quadric and 2-D Cubic maps yielded from the 2D-PPCS have positive KEs within all the parameters, and they have much larger KEs than the other four 2-D chaotic maps. These results are the same as the results in LE experiment and they demonstrate the robust chaotic behavior of the 2-D Quadric and 2-D Cubic maps.

C. CD

As a kind of fractal dimension, the CD measures the occupied space dimensionality of a time series [44]. The time series

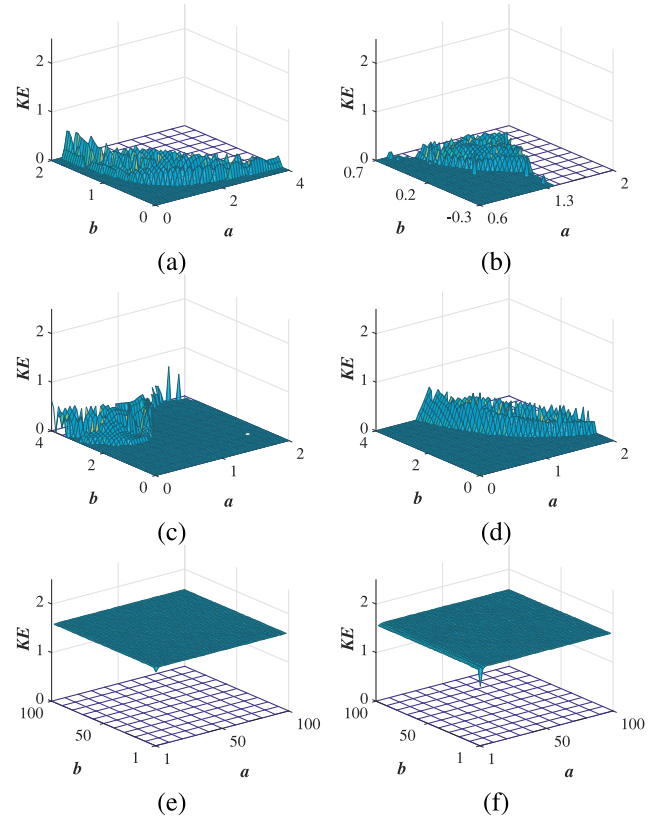

Fig. 6. KEs of the (a) discrete Lorenz map, (b) Hénon map, (c) 2-D-LSMCL map, (d) 2DSLM map, (e) 2-D Quadric map, and (f) 2-D Cubic map.

of a nonlinear system is regarded to own chaotic dynamics if its CD obtained is larger than 0 and a larger CD denotes a higher space dimensionality occupied by the time series. The CD is defined according to Definition 3.

Definition 3: The CD of a time series $\{s_1, s_2, \ldots, s_n, \ldots, \}$ with a given embedding dimension m is defined by

$$d = \lim_{r \to 0} \lim_{N \to \infty} \frac{\log C_m(r)}{\log r}$$

where $C_m(r)$ indicates the correlation integral calculated as

$$C_m(r) = \lim_{N \to \infty} \frac{1}{[N - (m-1)\zeta][N - (m-1)\zeta - 1]}$$
$$\times \sum_{i=1}^{N-(m-1)\zeta} \sum_{j=i+1}^{N-(m-1)\zeta} \theta\left(r - |\bar{s}_i - \bar{s}_j|\right)$$

where $\theta(\omega)$ indicates a step function, with $\theta(\omega) = 0$ for $\omega \leq 0$ and $\theta(\omega) = 1$ for $\omega > 0$; ζ is the time delay, which is typically set to 1; and $\{\bar{s}_1, \bar{s}_2, \ldots, \bar{s}_n, \ldots, \}$ is a new data sequence

$$\bar{s}_t = \left(s_t, s_{t+\zeta}, s_{t+2\zeta}, \ldots, s_{t+(m-1)\zeta}\right)$$
$$t = 1, 2, \ldots, N - (m-1)\zeta.$$

In our experiments, we used the nonlinear time series analysis tool TISEAN 3.0.1[2] to test the CDs for various 2-D chaotic maps and Fig. 7 shows the results obtained. The parameter ranges for these 2-D chaotic maps were the same as those employed in the LE and KE experiments, ensuring that the

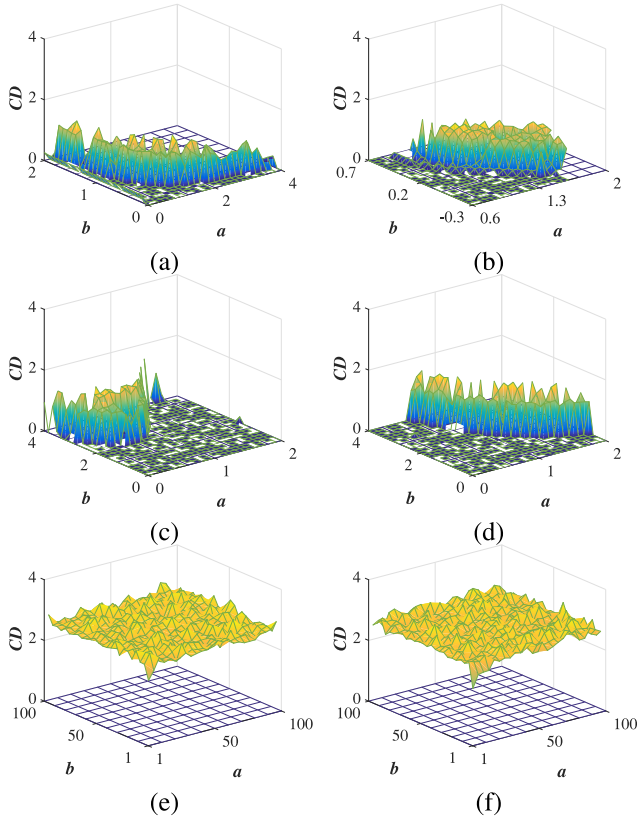[2]https://www.pks.mpg.de/ tisean/archive_3.0.0.html

Fig. 7.   CDs of the (a) discrete Lorenz map, (b) Hénon map, (c) 2D-LSMCL map, (d) 2D-SLM map, (e) 2-D Quadric map, and (f) 2-D Cubic map.

Fig. 8.   First and second rows show the chaotic trajectories of (X_1, X_2) and (Y_1, Y_2), where (X_1, Y_1) and (X_2, Y_2) are generated using the initial states of $(x_0, y_0, a, b) = (0.1, 0.1, 49, 49)$ and $(x_0, y_0, a, b) = (0.100001, 0.100001, 49, 49)$, respectively. The third row shows the differences between X_1 and X_3, and between Y_1 and Y_3, where (X_3, Y_3) are generated using the initial state of $(x_0, y_0, a, b) = (0.1, 0.1, 49.00001, 49.00001)$. (a) 2-D Quadric map and (b) 2-D Cubic map.

experiments are consistent. The results demonstrate that the 2-D Quadric and 2-D Cubic maps have positive CDs within all the settings of parameters, whereas the other four 2-D chaotic maps could only produce positive CDs in narrow parameter ranges. Additionally, the 2-D Quadric and 2-D Cubic maps could produce much larger CDs than the other 2-D chaotic maps. These findings demonstrate that the 2-D Quadric and 2-D Cubic maps is able to generate time series owning a higher space dimensionality than the other four 2-D chaotic maps.

D. Initial State Sensitivity

The initial state sensitivity is the most important and straightforward characteristic of chaos, where it indicates that a chaotic system shows extremely sensitive to the change of its initial state. A small change to its initial state can eventually lead to completely different chaotic signals.

The joint entropy here is used to test the correlation between two chaotic signals of a 2-D chaotic system generated by extremely similar initial states. We divided the values of two chaotic signals comprising S_1 and S_2 into K states. Their joint entropy can be calculated as

$$H(S_1 S_2) = \sum_{i_1=1}^{K} \sum_{i_2=1}^{K} P(b_{i_1} b_{i_2}) \log_2 P(b_{i_1} b_{i_2})$$

where b_{i_1} and b_{i_2} are the i_1th and i_2th states in S_1 and S_2, respectively, and $P(b_{i_1} b_{i_2})$ denotes the joint probability. Clearly, the joint entropy $H(S_1 S_2)$ is always positive. The maximum value of joint entropy could be obtained when the
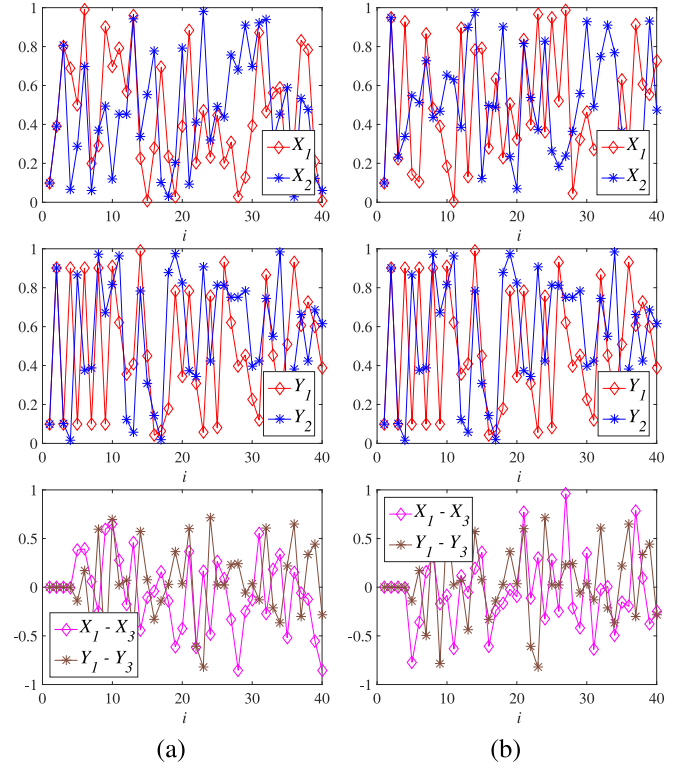
two chaotic signals S_1 and S_2 are completely independent and uniformly distributed, i.e., $P(b_{i_1} b_{i_2}) = P(b_{i_1}) \times P(b_{i_2})$ and $P(b_{i_1}) = P(b_{i_2}) = 1/K$. The maximum joint entropy is calculated as

$$
\begin{aligned}
H(S_1 S_2)_{\max} &= \sum_{i_1=1}^{K} \sum_{i_2=1}^{K} P(b_{i_1} b_{i_2}) \log_2 P(b_{i_1} b_{i_2}) \\
&= \sum_{i_1=1}^{K} \sum_{i_2=1}^{K} (1/K)^2 \log_2 (1/K)^2 \\
&= 2 \log_2 K.
\end{aligned}
$$

For each of the 2-D Quadric and 2-D Cubic maps, our experiments were conducted as follows: 1) set the initial state as $(x_0, y_0, a, b) = (0.1, 0.1, 49, 49)$ and generate the chaotic trajectories X_1 and Y_1; 2) slightly change the initial state to $(x_0, y_0, a, b) = (0.100001, 0.100001, 49, 49)$ and generate the chaotic trajectories X_2 and Y_2; and 3) slightly change the initial state to $(x_0, y_0, a, b) = (0.1, 0.1, 49.00001, 49.00001)$ and generate the chaotic trajectories X_3 and Y_3. Fig. 8 shows the first 40 states for the trajectories X_1, X_2 and Y_1, Y_2, as well as the differences between X_1 and X_3, and between Y_1 and Y_3. As can be seen, with the incasement of iteration number, slightly changing the initial values or parameters could lead to completely different trajectories. Table IV shows the joint entropies for these trajectories starting from slightly different initial values or parameters with the signal state

TABLE IV
JOINT ENTROPIES OF TRAJECTORIES STARTING FROM SLIGHTLY DIFFERENT INITIAL VALUES (TRAJECTORIES (X_1, Y_1) AND (X_2, Y_2)) AND CONTROL PARAMETERS (TRAJECTORIES (X_1, Y_1) AND (X_3, Y_3))

		Number of signal states K							
		2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8
2-D Quadric map	$H(X_1 X_2)$	1.9959	3.9764	5.9909	7.9949	9.9973	11.9986	13.9993	15.9996
	$H(Y_1 Y_2)$	1.9904	3.9765	5.9922	7.9938	9.9973	11.9986	13.9993	15.9996
	$H(X_1 X_3)$	1.9959	3.9826	5.9913	7.9948	9.9973	11.9986	13.9993	15.9996
	$H(Y_1 Y_3)$	1.9943	3.9847	5.9885	7.9950	9.9971	11.9986	13.9993	15.9996
2-D Cubic map	$H(X_1 X_2)$	1.9621	3.9719	5.9905	7.9942	9.9972	11.9986	13.9993	15.9996
	$H(Y_1 Y_2)$	1.9904	3.9765	5.9922	7.9938	9.9973	11.9986	13.9993	15.9996
	$H(X_1 X_3)$	1.9362	3.9881	5.9917	7.9946	9.9973	11.9986	13.9993	15.9996
	$H(Y_1 Y_3)$	1.9943	3.9847	5.9885	7.9950	9.9971	11.9986	13.9993	15.9996
$H(S_1 S_2)_{\max}$		2	4	6	8	10	12	14	16

$K \in \{2^1, \ldots, 2^n, \ldots, 2^8\}$. For each signal state, the first $2^{3 \times (n+1)}$ states are used to calculate the joint entropy. The results show that all the joint entropies approach to the maximum values, and thus the trajectories obtained starting from slightly different initial states exhibit high uncertainty.

VI. PNG

Pseudorandom numbers are employed widely in many practical applications such as industrial applications [12]. Chaotic systems own many unique characteristics, including the initial condition sensitivity, aperiodicity, and unpredictability, and thus they are suitable for designing PNGs.

A. PNG Design

When using a chaotic system to generate pseudorandom numbers, two strategies are commonly employed. The first strategy generates random numbers based on a threshold. A bit 1 is generated when the current chaotic output is bigger than the threshold, whereas a bit 0 is generated for the opposite situation. The second strategy involves directly generating random numbers from the chaotic outputs. It is clear that the performance of a chaos-based PNG is completely determined by the chaotic sequence employed. If a chaotic system easily happens chaos degradation, it cannot generate a long sequence of pseudorandom numbers.

If we assume that $S = \{s_1, s_2, \ldots, s_i, \ldots, \}$ is a chaotic sequence generated by a chaotic system, then a simple chaos-based PNG can be constructed as

$$P = \lfloor s_i \times \alpha \rfloor \mod \beta \tag{15}$$

where α is a large number to scale up the chaotic outputs, β is an integer, the function $\lfloor x \rfloor$ is to get the largest integer that equals to or is smaller than x. Our experiment sets $\alpha = 10^9$ and $\beta = 256$. Clearly, eight bits of random numbers can be obtained from each output state.

B. Randomness Test

An effective PNG should generate a large number of random numbers with aperiodicity and high randomness. The TestU01 is a widely used test standard for measuring the

TABLE V
CONTROL PARAMETERS USED FOR DIFFERENT 2-D CHAOTIC MAPS IN TESTU01 TEST

Chaotic maps	Control parameters
Discrete Lorenz map [38]	$a = 1.0462, b = 0.7481$
Hénon map [18]	$a = 1.3954, b = 0.3135$
2-D LSMCL map [39]	$a = 0.7515, b = 2.9691$
2-D SLM map [40]	$a = 0.9494, b = 2.9247$
2-D Quadric map	$a = 28.9705, b = 1.0221, c = 60.1613$
2-D Cubic map	$a = 49.1742, b = 39.3341, c = 8.8290$

random numbers [45]. It contains many statistical tests and can test a long sequence of random numbers. The TestU01 test standard comprises a set of predefined batteries and each battery is a set of many empirical statistical tests. It includes six widely used batteries, namely *Rabbit*, *Alphabit*, *BlockAlphabit*, *SmallCrush*, *Crush*, and *BigCrush* test suits. These test suits take different lengths of pseudorandom numbers as input. The *Rabbit*, *Alphabit*, and *BlockAlphabit* test suites can take 2^{32} bits as input and contain 17, 102, and 40 statistical tests, respectively. The *SmallCrush* test suite takes about 6 Gb as input and contains 15 statistical tests. The *Crush* test suite takes about 1 Tb as input and contains 144 statistical tests. The *BigCrush* test suite is the most stringent statistical test suit. It uses 160 statistical tests and can test a sequence with about 10 Tb, which is larger than 2^{43} bits. Thus, the TestU01 is an all-sided test standard that aims to determine the nonrandomness and defective areas from various viewpoints. To the best of our knowledge, it contains the most statistical tests and its tested random numbers are the longest, compared with other test standards. The maximum tested bit length can reach to 10 Tb. In our experiments, we used the open-source software TestU01[3] to ensure that neutral test results were obtained.

To demonstrate the superior performance of our proposed 2-D Quadric and 2-D Cubic maps, we separately used the discrete Lorenz, Hénon, 2D-LSMCL, 2D-SLM, and 2-D

[3]http://simul.iro.umontreal.ca/testu01/tu01.html

TABLE VI
RESULTS OF TESTU01 TEST STANDARD FOR DIFFERENT LENGTHS OF PSEUDORANDOM NUMBERS PRODUCED BY 2-D CHAOTIC MAPS. p/q SHOWS
THAT p OF q STATISTICAL TESTS ARE PASSED. THE DETAILED TEST REPORTED ARE GIVE ON
HTTP://WWW.HUAZHONGYUN.CN/EXPRES/TESTU01.HTM

Test suites	*Rabbit*	*Alphabit*	*BlockAlphabit*	*SmallCrush*	*Crush*	*BigCrush*
	2^{32} bits			about 6 Gb	about 1 Tb	about 10 Tb
Discrete Lorenz map [38]	39/40	17/17	101/102	15/15	140/144	157/160
Hénon map [18]	38/40	17/17	102/102	15/15	133/144	133/160
2-D LSMCL map [39]	40/40	17/17	102/102	15/15	144/144	160/160
2-D SLM map [40]	40/40	17/17	101/102	15/15	144/144	159/160
2-D Quadric map	40/40	17/17	102/102	15/15	144/144	160/160
2-D Cubic map	40/40	17/17	102/102	15/15	144/144	160/160

Quadric and 2-D Cubic maps as chaotic generators for the PNG, and tested the generated pseudorandom numbers using TestU01. The initial states for all the tested chaotic maps were set to $x_0 = 0.1$ and $y_0 = 0.1$. The iteration states x_i and y_i are set as the IEEE 754 double-precision. As discussed in Section II, these existing chaotic maps show classical chaotic behaviors under fixed parameter settings. To keep a same precision for different chaotic maps, their control parameters are randomly selected around these fixed settings. The control parameters of the 2-D Quadric and 2-D Cubic maps are randomly selected from a continuous chaotic range (1, 100). All the control parameters are take four decimal places. Table V shows the utilized control parameters of all the tested chaotic maps.

Table VI demonstrates the test results of the pseudorandom numbers generated by using different 2-D chaotic maps as the chaotic generator. For the discrete Lorenz and Hénon maps, when the bit length is 2^{32}, they fall to pass one or two statistical tests in the *Rabbit* or *BlockAlphabit* test suite. When the bit length increases to 1 Tb and 10 Tb, they fall to pass more statistical tests in the *Crush* and *BigCrush* test suites. The 2-D SLM map fall to pass one statistical test in the *BlockAlphabit* and *BigCrush* test suites, respectively. On the constat, the 2-D LSMCL, 2-D Quadric, and 2-D Cubic maps can pass all the statistical tests of all the six test suites. This means that they do not occur chaos degradation when generating 10 Tb of random numbers. However, the proposed 2-D Quadric and 2-D Cubic maps have much simpler structure than the existing 2-D LSMCL map, which can be seen from their definitions. Besides, the 2-D Quadric and 2-D Cubic maps have continuous chaotic ranges but the 2-D LSMCL map do not have, which can be observed from Proposition 1 and Fig. 5. Then the 2-D LSMCL map cannot overcome the chaos degradation caused by the discontinuous chaotic ranges. Since the maximum bit length that can be measured by the TestU01 is about 10 Tb, the bitstream larger than 10 Tb cannot be directly tested. In our future work, we will investigate how to test the randomness properties of much longer random numbers.

VII. CONCLUSION

Many engineering applications demand chaotic systems to have robust chaos, continuous chaotic parameter ranges, and late chaos degradation. Nevertheless, many existing chaotic systems do not have these properties. To address these shortcomings, we proposed a 2D-PPCS that can yield 2-D chaotic maps with robust chaos and desired dynamic properties. The 2D-PPCS is constructed from nonlinear polynomials and a modular chaotification is performed to compact the phase plane. Our theoretical analysis demonstrated that the 2D-PPCS can achieve chaotic behavior and its two LEs are determined completely by its two control parameters. Thus, we can customize the LEs by specifying the control parameters of the 2D-PPCS in order to obtain robust chaos and desired dynamic properties. We provided two illustrative examples of the 2D-PPCS by setting the highest exponent of the polynomial as two and three. Numeral experiments demonstrated that these two examples of the 2D-PPCS exhibit robust and desired chaotic behaviors, and they also perform much better than some representative 2-D chaotic maps. We applied these two examples of the 2D-PPCS to a PNG to demonstrate the utility of the 2D-PPCS and the experimental results verified the superior performance of the 2D-PPCS. Our future work will investigate how to test the randomness properties of random numbers with much longer and the generation of high-dimensional polynomial chaotic systems with robust chaos.

REFERENCES

[1] B. Kaviarasan, O.-M. Kwon, M. J. Park, and R. Sakthivel, "Integrated synchronization and anti-disturbance control design for fuzzy model-based multiweighted complex network," *IEEE Trans. Syst., Man, Cybern., Syst.*, early access, Jan. 8, 2020, doi: 10.1109/TSMC.2019.2960803.

[2] S. Chen, S. Yu, J. Lü, G. Chen, and J. He, "Design and FPGA-based realization of a chaotic secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2359–2371, Sep. 2018.

[3] L. Yin, Z. Deng, B. Huo, and Y. Xia, "Finite-time synchronization for chaotic gyros systems with terminal sliding mode control," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 6, pp. 1131–1140, Jun. 2019.

[4] S. Gao, Y. Yu, Y. Wang, J. Wang, J. Cheng, and M. Zhou, "Chaotic local search-based differential evolution algorithms for optimization," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 51, no. 6, pp. 3954–3967, Jun. 2021, doi: 10.1109/TSMC.2019.2956121.

[5] T. H. Lee and J. H. Park, "New methods of fuzzy sampled-data control for stabilization of chaotic systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 12, pp. 2026–2034, Dec. 2018.

[6] P. Z. Wieczorek and K. Gołofit, "True random number generator based on flip-flop resolve time instability boosted by random chaotic source," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 4, pp. 1279–1292, Apr. 2018.

[7] B. Niu, C. K. Ahn, H. Li, and M. Liu, "Adaptive control for stochastic switched nonlower triangular nonlinear systems and its application to a one-link manipulator," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 48, no. 10, pp. 1701–1714, Oct. 2018.

[8] Y. Zhao, W. Zhang, H. Su, and J. Yang, "Observer-based synchronization of chaotic systems satisfying incremental quadratic constraints and its application in secure communication," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 50, no. 12, pp. 5221–5232, Dec. 2020.

[9] X. Zhang, S. Yu, P. Chen, J. Lü, J. He, and Z. Lin, "Design and ARM-embedded implementation of a chaotic secure communication scheme based on H.264 selective encryption," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 1949–1965, 2017.

[10] H. Yang, G.-P. Jiang, and J. Duan, "Phase-separated DCSK: A simple delay-component-free solution for chaotic communications," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 12, pp. 967–971, Dec. 2014.

[11] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 57, no. 12, pp. 996–1000, Dec. 2010.

[12] M. Bakiri, C. Guyeux, J.-F. Couchot, L. Marangio, and S. Galatolo, "A hardware and secure pseudorandom generator for constrained devices," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3754–3765, Aug. 2018.

[13] R. Bassily and S. Ulukus, "Deaf cooperation and relay selection strategies for secure communication in multiple relay networks," *IEEE Trans. Signal Process.*, vol. 61, no. 6, pp. 1544–1554, Mar. 2013.

[14] S. Gong, C. Xing, S. Chen, and Z. Fei, "Secure communications for dual-polarized MIMO systems," *IEEE Trans. Signal Process.*, vol. 65, no. 16, pp. 4177–4192, Aug. 2017.

[15] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Boulder, CO, USA: Westview Press, 2014.

[16] H. G. Schuster and W. Just, *Deterministic Chaos: An Introduction*. Weinheim, Germany: Wiley, 2006.

[17] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmospher. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[18] S. Vaidyanathan and C. Volos, *Advances and Applications in Chaotic Systems*. Heidelberg, Germany: Springer, 2016.

[19] R. L. Devaney, *An Introduction to Chaotic Dynamical Systems*, 2nd ed. Boulder, CO, USA: Westview Press, 2003.

[20] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos*, vol. 2. New York, NY, USA: Springer, 2003,

[21] A. E. Elfiqi, H. S. Khallaf, S. F. Hegazy, A. Elsonbaty, H. M. Shalaby, and S. S. A. Obayya, "Chaotic polarization-assisted L DPSK-MPPM modulation for free-space optical communications," *IEEE Trans. Wireless Commun.*, vol. 18, no. 9, pp. 4225–4237, Sep. 2019.

[22] R. S. T. Lee, "Chaotic type-2 transient-fuzzy deep neuro-oscillatory network (CT2TFDNN) for worldwide financial prediction," *IEEE Trans. Fuzzy Syst.*, vol. 28, no. 4, pp. 731–745, Apr. 2020.

[23] S. Ergün, "On the security of chaos based 'true'random number generators," *IEICE Trans. Fund. Electron. Commun. Comput. Sci.*, vol. 99, no. 1, pp. 363–369, 2016.

[24] M. Han, R. Zhang, T. Qiu, M. Xu, and W. Ren, "Multivariate chaotic time series prediction based on improved grey relational analysis," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 49, no. 10, pp. 2144–2154, Oct. 2019.

[25] H. Zhao, S. Gao, Z. He, X. Zeng, W. Jin, and T. Li, "Identification of nonlinear dynamic system using a novel recurrent wavelet neural network based on the pipelined architecture," *IEEE Trans. Ind. Electron.*, vol. 61, no. 8, pp. 4171–4182, Aug. 2014.

[26] J. A. Lazzús, M. Rivera, and C. H. López-Caraballo, "Parameter estimation of Lorenz chaotic system using a hybrid swarm intelligence algorithm," *Phys. Lett. A*, vol. 380, nos. 11–12, pp. 1164–1171, 2016.

[27] 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.

[28] E. Zeraoulia, *Robust Chaos and Its Applications*, vol. 79. Singapore: World Sci., 2012.

[29] Z. Hua and Y. Zhou, "Image encryption using 2D Logistic-adjusted-Sine map," *Inf. Sci.*, vol. 339, pp. 237–253, Apr. 2016.

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

[31] 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.

[32] Y. Deng, H. Hu, N. Xiong, W. Xiong, and L. Liu, "A general hybrid model for chaos robust synchronization and degradation reduction," *Inf. Sci.*, vol. 305, pp. 146–164, Jun. 2015.

[33] C. Li, D. Lin, J. Lü, and F. Hao, "Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography," *IEEE MultiMedia*, vol. 25, no. 4, pp. 46–56, Oct./Dec. 2018.

[34] Z. Hua, Y. Zhang, and Y. Zhou, "Two-dimensional modular chaotification system for improving chaos complexity," *IEEE Trans. Signal Process.*, vol. 68, pp. 1937–1949, Mar. 2020.

[35] H. Li, Z. Hua, H. Bao, L. Zhu, M. Chen, and B. Bao, "Two-dimensional memristive hyperchaotic maps and application in secure communication," *IEEE Trans. Ind. Electron.*, vol. 68, no. 10, pp. 9931–9940, Oct. 2021.

[36] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.

[37] Q. Wang et al., "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.

[38] N. H. T. Anh, D. Van Liet, and S. Kawamoto, "Nonlinear dynamics of two-dimensional chaos map and fractal set for snow crystal," *Chaotic Model. Simulat.*, vol. 1, no. 1, pp. 21–31, Nov. 2015.

[39] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.

[40] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D Sine Logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[41] R. Zhang and S. Yang, "Robust chaos synchronization of fractional-order chaotic systems with unknown parameters and uncertain perturbations," *Nonlinear Dyn.*, vol. 69, no. 3, pp. 983–992, 2012.

[42] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Physica D Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.

[43] P. Grassberger and I. Procaccia, "Estimation of the Kolmogorov entropy from a chaotic signal," *Phys. Rev. A*, vol. 28, no. 4, pp. 2591–2593, 1983.

[44] L. Lacasa and J. Gómez-Gardeñes, "Correlation dimension of complex networks," *Phys. Rev. Lett.*, vol. 110, Apr. 2013, Art. no. 168703.

[45] P. L'Ecuyer and R. Simard, "TestU01: A C library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, p. 22, 2007.

Zhongyun Hua (Member, IEEE) received the B.S. degree in software engineering from Chongqing University, Chongqing, China, in 2011, and the M.S. and Ph.D. degrees in software engineering from the University of Macau, Macau, China, in 2013 and 2016, respectively.

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

Yongyong Chen received the B.S. and M.S. degrees in information and computing science from the Shandong University of Science and Technology, Qingdao, China, in 2014 and 2017, respectively, and the Ph.D. degree in computer science from the University of Macau, Macau, China, in 2020.

He is currently an Assistant Professor with the School of Computer Science and Technology, Harbin Institute of Technology Shenzhen, Shenzhen, China. His research interests include image processing, data mining, and computer vision.

Han Bao (Graduate Student Member, IEEE) received the B.S. degree in landscape design from the Jiangxi University of Finance and Economics, Nanchang, China, in 2015, and the M.S. degree in art and design from Changzhou University, Changzhou, China, in 2018. He is currently pursuing the Ph.D. degree in nonlinear system analysis and measurement technology with the Nanjing University of Aeronautics and Astronautics, Nanjing, China, and is undergoing a one-year joint training with Changzhou University.

In 2019, he visited the Department of Computer Science, University of Auckland, Auckland, New Zealand. His research interests include memristive neuromorphic circuit, nonlinear circuits and systems, and artificial intelligence.

Yicong Zhou (Senior Member, IEEE) received the B.S. degree in electrical engineering from Hunan University, Changsha, China, in 1992, and the M.S. and Ph.D. degrees in electrical engineering from Tufts University, Medford, MA, USA, in 2008 and 2010, respectively.

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

Dr. Zhou received the Third Price of Macao Natural Science Award as a Sole Winner in 2020 and a co-recipient in 2014. He has been a leading Co-Chair of Technical Committee on Cognitive Computing in the IEEE Systems, Man, and Cybernetics Society since 2015. He serves as an Associate Editor for IEEE TRANSACTIONS ON NEUTRAL NETWORKS AND LEARNING SYSTEMS, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, IEEE TRANSACTIONS ON GEOSCIENCE AND REMOTE SENSING, and four other journals. He was recognized as "World's Top 2% Scientists" in the Stanford University Releases List in 2019 and as the "Highly Cited Researcher" in the Web of Science in 2020. He is a Fellow of the Society of Photo-Optical Instrumentation Engineers.