IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received October 7, 2019, accepted October 24, 2019, date of publication October 30, 2019, date of current version November 14, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2950457

Dynamics and Optimization Control of a Robust Chaotic Map

CHUNLAI LI[1], KUN QIAN[1], SHAOBO HE[2], HONGMIN LI[1], AND WEI FENG[1]
[1]College of Physics and Electronics, Hunan Institute of Science and Technology, Yueyang 414006, China
[2]School of Physics and Electronics, Central South University, Changsha 410083, China

Corresponding authors: Chunlai Li (hnistlichl@163.com) and Shaobo He (heshaobo_123@163.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61901530, in part by the Hunan Provincial Natural Science Foundation of China under Grant 2019JJ40109, in part by the Research Foundation of Education Bureau of Hunan Province of China under Grant 18A314, in part by the Science and Technology Program of Hunan Province under Grant 2016TP1021, in part by the China Postdoctoral Science Foundation under Grant 2019M652791, and in part by the Postdoctoral Innovative Talents Support Program under Grant BX2018038.

ABSTRACT Robust chaos in the discrete system is suggested to have practical as well as theoretical importance since it can obtain reliable operation in the chaotic mode. However, it receives only moderate attention and only focuses on a finite chaotic parameter space and small Lyapunov exponents. This paper introduces a two-dimensional smooth map and studies its robustness of chaos in the infinite parameter space. Then, a compound operation-based optimization control method is introduced to increase the map complexity in the measure of Lyapunov exponent. The introduced method is simple and provides a new pathway for exploring the robustness and complexity of discrete chaotic system. Finally, we design a chaos-based pseudo-random number generator (CPNG) based on the optimized robust chaotic map, and the careful analysis shows that the proposed CPNG has high quality of randomness and has passed the rigorous National Institute of Standards and Technology (NIST) test.

INDEX TERMS Discrete map, dynamics, parameter space, Lyapunov exponent.

I. INTRODUCTION

With the rapid development of network communication, the data security and encryption have been paid more and more attention by engineers and scientists [1], [2]. Compared with traditional schemes, chaotic information encryption technology is suggested to have higher security and rapidity [3], [4]. The complex dynamic behavior of chaotic systems is of great importance to the security in chaotic encryption communication system [5]–[8]. It is generally known that the running time will increase significantly when discretizing a continuous chaotic system. In contrast, discrete chaotic maps are more attractive in digital applications for less computing time [9]. However, most discrete chaotic systems, such as Sine map, Logistic map, Cubic map and Tent map, have relatively small key space in parameter and relatively small Lyapunov exponents, which make the generated chaotic sequences weak in security [10]–[13]. To enlarge the key space in parameter, Zhou *et al.* [14] obtained a discrete system by combining different one-dimensional chaotic maps in a non-linear way, but the Lyapunov exponent of the system is small and the sequence complexity is not high. Then to avoid this deficiency, Wang and Yuan [15], Zhou *et al.* [16] and Yuan *et al.* [17] introduced the cascading method for constructing discrete chaotic system, which can enlarge both the maximum Lyapunov exponent and the system parameter range of chaos. In addition, some other methods, such as dimension expansion [18]–[20], closed-loop modulation [21]–[23], cascade modulation [24], modeling [25] and mixed operation [26]–[28], are proposed to improve the performance of chaotic maps. However, these methods lack the theoretical consideration of pure chaos and larger Lyapunov exponent in the parameter space.

A chaotic system is called robust if there is no periodic window or any coexisting attractor within some parameter space. In other words, chaos is the unique dynamical behavior within this parameter range. Therefore, small disturbance of parameter cannot destroy the chaotic feature of robust chaotic system. In 1998, Banerjee *et al.* [29] originally discovered the existence of robust chaos when studying the current mode

The associate editor coordinating the review of this manuscript and approving it for publication was Parul Garg.

controlled boost converter, and gave a sufficient condition for generating robust chaos. Banerjee and Grebogi [30] also found the existence of robust chaos in buck converter and proposed the conditions of robust chaos in this two-dimensional (2D) piecewise smooth map. Han [31] proposed a chaos robustness criterion for a kind of two-dimensional piecewise smooth maps, theoretically based on Banerjee's method. Andrecut and Ali [32] found robust chaos in a family of one-dimensional continuous piecewise smooth maps and demonstrated it by the theory of bifurcation structure. Patraa and Banerjee [33] confirmed the robust chaos in 3D piecewise linear maps and derived the occurrence conditions by analyzing the interplay between the stable and unstable manifolds. However, these works only concern the robust chaos phenomenon of discrete map system within limited parameter range, which has limited the practical application.

In recent years, we have found that robust chaos exists in continuous chaotic systems with infinite parameter space. These parameters can regularly control the amplitude of system signal, and the Lyapunov exponent remains invariable [34]–[36]. Therefore, this type of system provides a significant candidate for the practical application of chaotic encryption and chaotic communication. However, to the best of our knowledge, there is no research on robust chaos of discrete map with infinite parameter space reported in the literature so far, which is still open and challenging.

So, aiming at the dilemma of existing discrete maps, we attempt to find some solution by introducing a two-dimensional smooth map and an optimization scheme. First, by exploring the relationship of system parameters and scale transformation of state variables, we find that the Lyapunov exponents of this discrete map remains invariable and the signal amplitudes change regularly following some functional relationship when some parameters vary in infinite real space. Then, a compound operation-based optimization control method of complexity is introduced using the matching condition of iteration range and the definition of Lyapunov exponent. Theoretical analysis shows that the values of Lyapunov exponent will increase in logarithmic form when the control parameters vary in real space. Thus the complexity of the chaotic sequence increases. Finally, we introduce a CPNG based on the optimized chaotic map, careful analysis shows that the proposed CPNG has high randomness and has passed the rigorous NIST test. The main contribution of this work includes the following parts: The introduced method can theoretically guarantee an infinite parameter range of robust chaos and large Lyapunov exponents. What's more, the introduced method is simple and can be extended to one-dimensional or high-dimensional discrete chaotic systems. Therefore, this work provides a kind of effective way for exploring the robustness and complexity of discrete systems.

The rest of this paper is organized as follows. In Section II, we introduce two-dimensional chaotic map and analyze the basic dynamic characteristics. In Section III, we introduce a control scheme of complexity optimization for the 2D chaotic map. In Section IV, we introduce a CPNG based on the optimized robust chaotic map. Finally, the conclusion is provided in Section V.

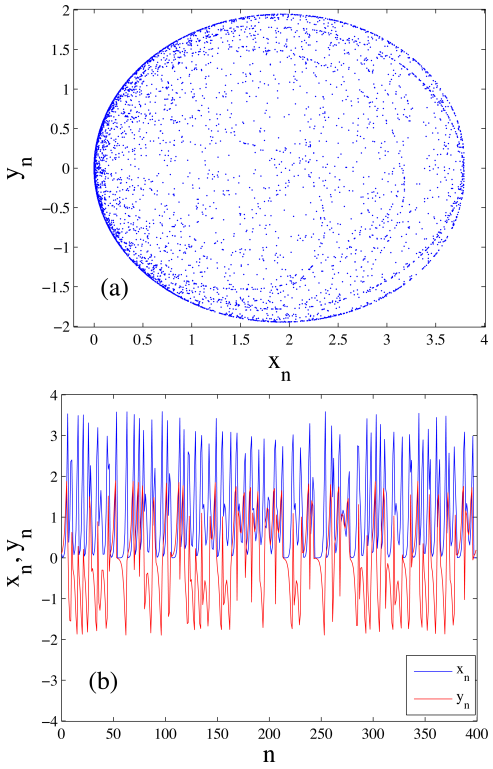


FIGURE 1. (a) Phase portrait and (b) time sequences of map (1) with $a = 1$, $b = 1.98$, $c = 1.0$, $x_0 = 0.1$, $y_0 = 0.1$.

II. THE TWO-DIMENSIONAL ROBUST CHAOTIC MAP

A. MODEL DESCRIPTION

The two-dimensional chaotic map is evolved from the parabolic discrete map, described by

$$\begin{cases} x_{n+1} = ay_n^2 \\ y_{n+1} = by_n - cx_n y_n \end{cases} \tag{1}$$

where x, y are state variables; a, b, c are positive parameters. When the parameters are set as $a = 1$, $b = 1.98$, $c = 1.0$ and the initial condition is designated to be $x_0 = 0.1$, $y_0 = 0.1$, map (1) is chaotic, as is diagrammed in Fig.1 by the phase portrait and time trajectories.

The fixed points of map (1) can be calculated by the transformed equations $x_n = ay_n^2$ and $y_n = by_n - cx_n y_n$. It is well known that map (1) has one fixed point $P_0 = (0, 0)$ when $b \leq 1$; and map (1) has three fixed point when $b > 1$, depicted as $P_0 = (0, 0)$, $P_1 = \left(\frac{-1+b}{c}, -\frac{\sqrt{-1+b}}{\sqrt{ac}}\right)$ and $P_2 = \left(\frac{-1+b}{c}, \frac{\sqrt{-1+b}}{\sqrt{ac}}\right)$. The characteristic equation evaluated at fixed point (x, y) is

$$\lambda^2 - (b - cx)\lambda - 2acy^2 = 0 \tag{2}$$

Considering fixed point P_0, we obtain $\lambda_1 = 0$, $\lambda_2 = b$. Thus, we have that fixed point P_0 is stable when $b < 1$ since

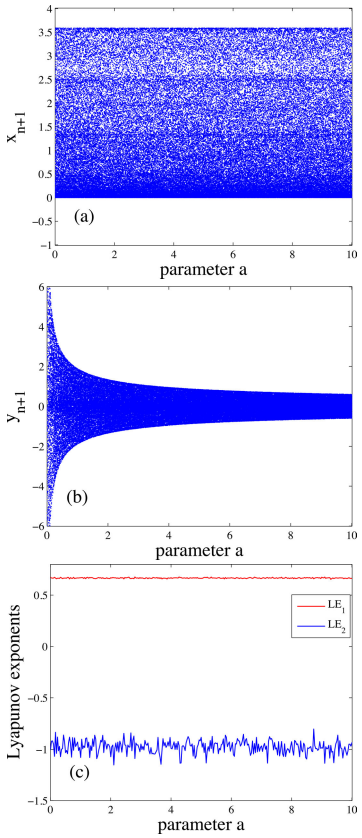


FIGURE 2. (a), (b) Bifurcation diagram and (c) Lyapunov exponent spectrum versus parameter *a*.

the characteristic values satisfy $|\lambda_{1,2}| < 1$. When $b > 1$, we have $|\lambda_1| < 1$ and $|\lambda_2| > 1$, thus, fixed point P_0 is an unstable saddle point.

When considering the fixed points P_1 and P_2, we obtain the corresponding characteristic values as $\lambda_1 = \frac{1}{2} - \frac{\sqrt{9-8b}}{2}$, $\lambda_2 = \frac{1}{2} + \frac{\sqrt{9-8b}}{2}$. Accordingly, we have

(I) when $1 < b \leq 1.125$, it yields $0 \leq 9 - 8b < 1$ and $|\lambda_{1,2}| < 1$. Therefore, P_1 and P_2 are stable nodes.

(II) when $1.125 < b < 1.5$, it yields $-3 < 9 - 8b < 0$, λ_1 and λ_2 are a pair of conjugate complex roots satisfying $|\lambda_{1,2}| < 1$. Therefore, P_1 and P_2 are stable foci.

(III) when $b > 1.5$, it yields $9 - 8b < -3$, λ_1 and λ_2 are a pair of conjugate complex roots satisfying $|\lambda_{1,2}| > 1$. Therefore, P_1 and P_2 are unstable foci.

B. ROBUST CHAOS

We set $b = 1.98$, $c = 1.0$, while take a as the bifurcation parameter varying in the interval [0, 10]. Fig.2 (a) and (b) depict the bifurcation of map (1) by adopting continuation diagram of the state variable x and y respectively. Fig.2 (c) displays the corresponding spectrums of Lyapunov exponent with QR decomposition method. It's known that with the increasing of a, the signal amplitude adjusts in certain pattern, and the spectrums of Lyapunov exponent keep constant.

The significance of fixed point of discrete nonlinear map can be interpreted as a point with zero velocity in phase space. When the trajectory in phase space is rescaled, the nonzero fixed point will correspondingly deviate from the original position. Conversely, when the nonzero fixed point deviates from the original position, the signal amplitude of trajectory in phase space may be rescaled. It can be found from the expression of nonzero fixed points that parameters a and c of map (1) can control the location of fixed points P_1 and P_2. According, parameters a and c may rescale the amplitude of signal x and y. In fact, when taking the scale transformations $x = \hat{x}$ and $y = a^{-0.5}\hat{y}$, we get the resulting system of map (1), as below

$$\begin{cases} \hat{x}_{n+1} = \hat{y}_n^2 \\ \hat{y}_{n+1} = b\hat{y}_n - c\hat{x}_n\hat{y}_n \end{cases} \tag{3}$$

Thus, the coefficient of y^2 is normalized with the scale transformations [35]. Therefore, when parameter a increases successively, the amplitude of y changes by the power function with an index of $-1/2$, but the amplitude of x keeps in the same range, as depicted in Fig.2 (a) and (b) respectively.

When we replace the fixed point (x, y) in the characteristic equation (2) with P_0, it yields $\lambda^2 - b\lambda = 0$; and when we put the fixed point P_1 or P_2 in the characteristic equation (2), it yields $\lambda^2 - \lambda + b - 1 = 0$. Thus, we have eliminated the influence of a on the characteristic equation, and the characteristic roots are indifferent with a. Consequently, the Lyapunov exponent spectrum remains invariable when parameter a varies in real space, as depicted in Fig.2 (c). And we find from Fig.2 (c) that there exist one positive and one negative Lyapunov exponents, in which the positive Lyapunov exponent means the divergence degree of the system trajectory in the long time motion, and the negative Lyapunov exponent means the convergence degree of the system trajectory in the long time motion. Therefore, the map system (1) is chaotic.

Then, we set $a = 1$, $b = 1.98$, while take c as the bifurcation parameter varying in the region [0, 10]. The corresponding bifurcation diagram and Lyapunov exponent spectrum are depicted in Fig.3, by adopting continuation diagram and QR decomposition method respectively. It's known that with the increasing of c, the signal amplitude adjusts in certain pattern, and the spectrums of Lyapunov exponent keep constant. It follows analogously that when taking the scale transformations $x = c^{-1}\hat{x}$ and $y = c^{-0.5}\hat{y}$, we get the resulting system of map (1), as depicted by

$$\begin{cases} \hat{x}_{n+1} = a\hat{y}_n^2 \\ \hat{y}_{n+1} = b\hat{y}_n - \hat{x}_n\hat{y}_n \end{cases} \tag{4}$$

Thus, the coefficient of xy is normalized with the scale transformations [35].Therefore, when parameter c increases successively, the amplitude of x changes by the power function with an index of -1, the amplitude of y changes by the power function with an index of $-1/2$, as depicted in Fig.3 (a) and (b) respectively. It's also found that we can eliminate the influence of c on the characteristic equation by considering P_0, P_1 or P_2, denoting the Lyapunov exponent

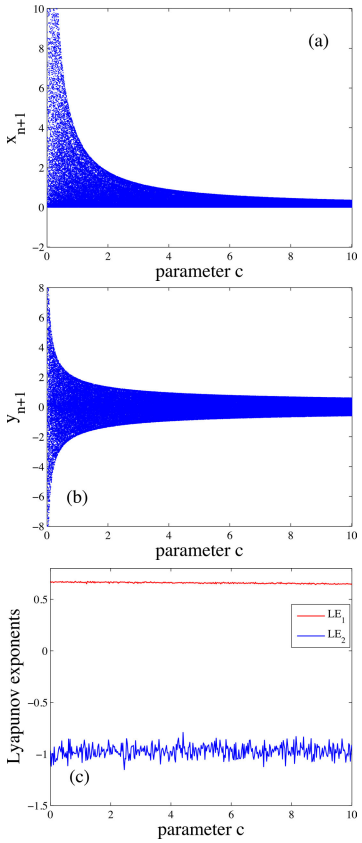


FIGURE 3. (a), (b) Bifurcation diagram and (c) Lyapunov exponent spectrum versus parameter c.

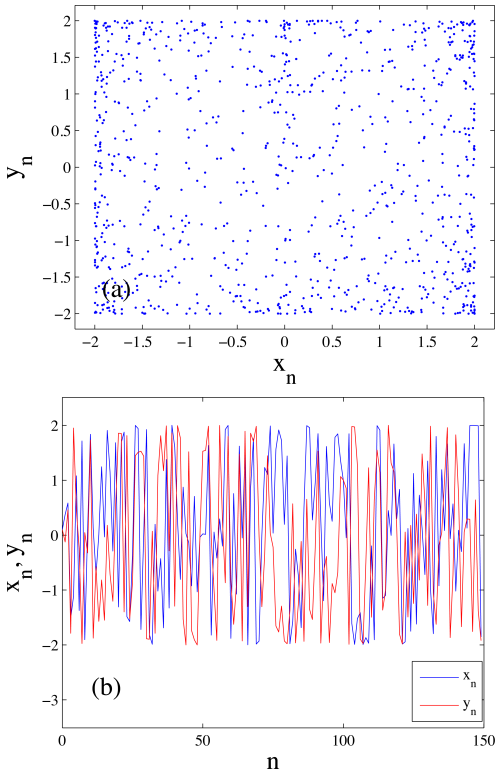


FIGURE 4. (a) Phase portrait and (b) time sequences of map (10) with parameter set p and $x_0 = 0.1$, $y_0 = 0.1$.

spectrum remains invariable when parameter c varies in real space, as depicted in Fig.3 (c).

III. OPTIMIZATION CONTROL OF THE ROBUST CHAOTIC MAP

A. THE OPTIMIZATION CONTROL SCHEME

As a numerical characteristic of nonlinear system, the Lyapunov exponent indicates the average exponential divergence rate of adjacent trajectories in phase space. The Lyapunov exponent of the discrete chaotic map $x_{n+1} = f(x_n)$ is defined by

$$LE_f = \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f'(x_i)\right|\right\} \tag{5}$$

In general, negative Lyapunov exponent represents the state of fixed point, nonpositive Lyapunov exponent represents the state of period or limit cycle, and positive Lyapunov exponent means the chaotic behavior. What's more, larger Lyapunov exponent corresponds to higher sensitivity to the initial condition. Therefore, the Lyapunov exponent provides a useful measure to quantitatively determine the randomness performance of a chaotic system. Accordingly, an effective and direct method for improving the randomness of a chaotic system is to increase the Lyapunov exponent value. In this section, to increase the complexity of the chaotic sequence, an optimization scheme will be designed for the robust chaotic map based on the measure of Lyapunov exponent.

The Sine map is a commonly used chaotic map depicted by $x_{n+1} = S(x) = a\sin(\pi x_n)$, which is chaotic when $a \in [0.867, 1]$. And the robust chaotic maps are expressed by $f_1(x), f_2(x), \ldots, f_k(x)$ respectively. Then the compound operation-based optimization scheme for the robust chaotic map is represented as

$$x_{n+1} = P(x) = a\sin\left(\pi(f_1(x) + f_2(x) + \cdots f_k(x))\right) \tag{6}$$

The advantage of choosing Sine map for compound operation is that it is not necessary to consider the iterative matching problem between the range and the definition domain of the subsystem.

Thus, the Lyapunov exponent of the compound map is

$$\begin{aligned} LE_P &= \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|P'(x_i)\right|\right\} \\ &= LE_S + \lim_{n\to\infty}\left\{\frac{1}{n}\sum_{i=0}^{n-1}\ln\left|f_1'(x_i)+f_2'(x_i)+\cdots f_k'(x_i)\right|\right\} \\ &\geq LE_S + LE_{f_i} > 0 \end{aligned} \tag{7}$$

In (7), $LE_S > 0$ is the Lyapunov exponent of Sine map, $LE_{f_i} > 0$ is the Lyapunov exponent of some robust chaotic map $f_i(x)$. We can find that the Lyapunov exponent of the compound map is larger than that of any robust chaotic maps. As a consequence, the dynamic performance of robust chaotic map is improved.

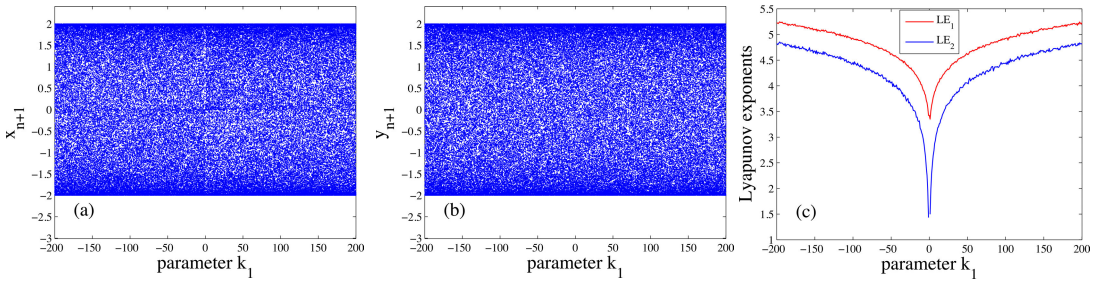


FIGURE 5. (a), (b) Bifurcation diagram and (c) Lyapunov exponent spectrum versus parameter k_1.

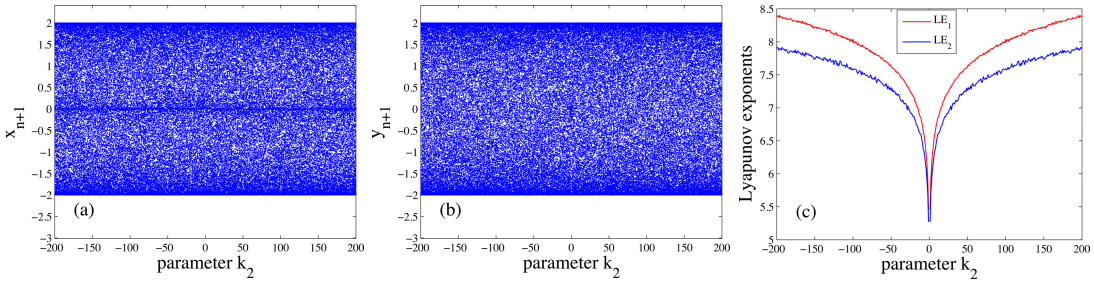


FIGURE 6. (a), (b) Bifurcation diagram and (c) Lyapunov exponent spectrum versus parameter k_2.

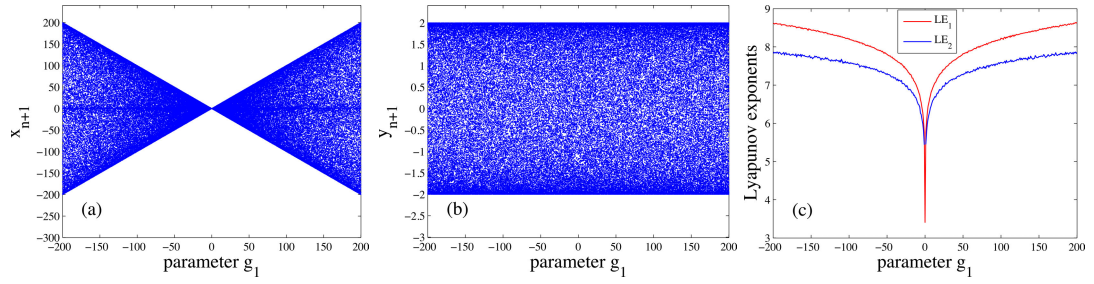


FIGURE 7. (a), (b) Bifurcation diagram and (c) Lyapunov exponent spectrum versus parameter g_1.

If all the robust chaotic maps have the same expression, i.e. $f_1(x) = f_2(x) = \ldots = f_k(x) = f_0(x)$, the compound map can be depicted as

$$x_{n+1} = P(x) = a \sin\left(k\pi f_0(x)\right) \tag{8}$$

More generally, the parameter k can be treated as a positive or negative real number. In this way, the Lyapunov exponent of the compound map is described by

$$LE_P = LE_S + \lim_{n\to\infty} \left\{ \frac{1}{n} \ln \left| k f_0'(x_i) \right| \right\} \tag{9}$$

Thus, the Lyapunov exponent of the compound map varies logarithmically with k, or the parameter k can control the Lyapunov exponent of the compound map by the logarithm function. When $|k| \geq 1$, one further obtains $LE_P > 0$ for $LE_s > 0$ and $LE_{f_i} > 0$.

B. APPLICATION TO THE ROBUST MAP

Based on the introduced optimization scheme, the compound map of 2D chaotic map (1) is constructed as

$$\begin{cases} x_{n+1} = g_1 \sin\left(k_1 \pi a y_n^2\right) \\ y_{n+1} = g_2 \sin\left(k_2 \pi \left(b y_n - c x_n y_n\right)\right) \end{cases} \tag{10}$$

When selecting the parameter set $p = \{a = 1, b = 1.98, c = 1.0, g_1 = 2, g_2 = 2, k_1 = 6, k_2 = 6\}$ and initial condition $x_0 = 0.1$, $y_0 = 0.1$, the chaotic phase portrait and time sequences of map (10) are plotted in Fig.4. Obviously, map (10) has better ergodicity and larger key space since the phase portrait distributes in much larger regions than that of map (1) and the existed maps. It's also found in Fig.4 that the sequences of map (10) are uniformly distributed. Therefore, the time sequences of map (10) have better pseudo-random performance.

From the analysis in section 3.1, we know that the parameters k_1 and k_2 can control the Lyapunov exponent of the

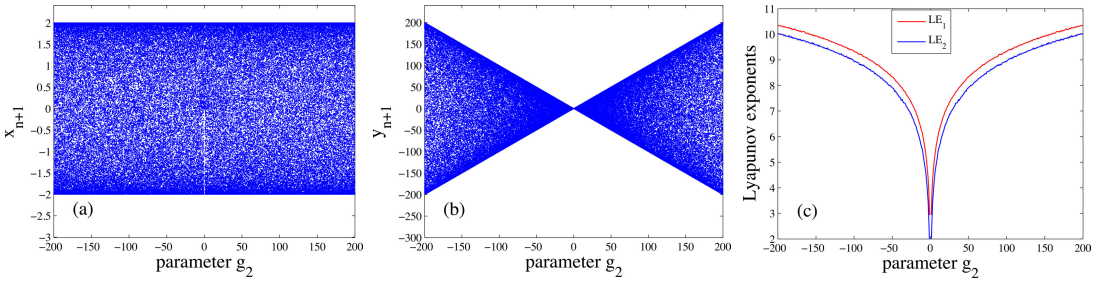


FIGURE 8. (a), (b) Bifurcation diagram and (c) Lyapunov exponent spectrum versus parameter g_2.

TABLE 1. Correlation coefficients of different chaotic maps.

Discrete maps		Correlation coefficients	
Map	*parameters* *initial condition*	AC (x/y)	CC of x and y
Hénon map $\begin{cases} x_{n+1} = -ax_n^2 + y_n + 1 \\ y_{n+1} = bx_n \end{cases}$	a=1.4, b=0.3 x_0=0.1, y_0=0.1	−0.0125 −0.0136	0.0232
Logistic map $\begin{cases} x_{n+1} = ax_n(1-x_n) + by_n^2 \\ y_{n+1} = cy_n(1-y_n) + d(x_n^2 + x_n y_n) \end{cases}$	a=3.0, b=0.2, c=3.4, d=0.14 x_0=0.1, y_0=0.1	−0.0017 −0.0091	0.0029
Map (1) $\begin{cases} x_{n+1} = ay_n^2 \\ y_{n+1} = by_n - cx_n y_n \end{cases}$	a=1, b=1.98, c=1.0 x_0=0.1, y_0=0.1	0.0088 −0.0165	−0.0088
Map (10) $\begin{cases} x_{n+1} = g_1 \sin\left(k_1 \pi a y_n^2\right) \\ y_{n+1} = g_2 \sin\left(k_2 \pi \left(by_n - cx_n y_n\right)\right) \end{cases}$	a=1, b=1.98, c=1.0, g_1=2, g_2=2, k_1=6, k_2=6 x_0=0.1, y_0=0.1	−0.000323 −0.000169	−0.00058

compound map by the logarithm function, which can be demonstrated by Fig.5 (c) and Fig.6 (c). And it's found from (10) that the signal amplitudes of x and y are equal to g_1 and g_2 respectively, as demonstrated in Fig.5 (a-b), Fig.6 (a-b), Fig.7 (a-b) and Fig.8 (a-b). What's more, it's easy to derive from (9) and (10) that parameter g_1 and g_2 can control the Lyapunov exponent of the compound map by the logarithm function, as depicted in Fig.7 (c) and Fig.8 (c).

The effect of parameter a on the Lyapunov exponent of map (10) is similar to that of k_1. Further, it's found by numerical calculation that parameter c can control the Lyapunov exponent of map (10) approximately in accordance with the logarithm function. The distribution of largest Lyapunov exponent spectrum in two-parameter phase space a vs c is depicted in Fig.9.

The mapping diagram of discrete dynamical system $x_{n+1} = f(x_n)$ describes the discrete sets generated by successive iterations of x_n and x_{n+1}. In Fig.10, we plot the mapping diagrams of Sine map, Hénon map, map (1) and map (10) respectively. As we know that map (1) and map (10) have more complex patterns than Sine map and Hénon map. In particular, map (10) presents a strong chaotic state with full

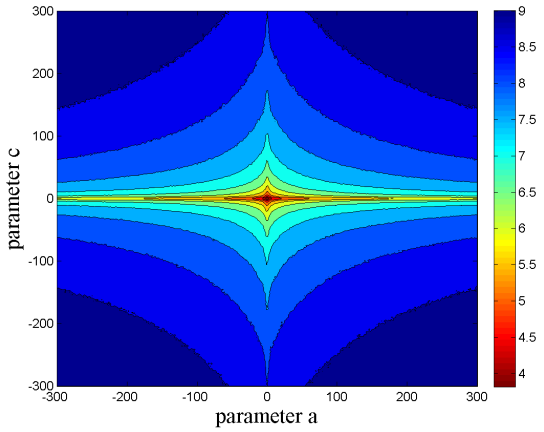


FIGURE 9. Distribution of largest Lyapunov exponent with respect to a and c.

mapping. From the bifurcation diagrams in Fig.5 and Fig.6, we further find that the full mapping ranges for parameter k_1 and k_2 are infinite. Comparing with injective mapping, full mapping corresponds to stronger chaotic intensity and larger iteration interval. When processed by digital system,

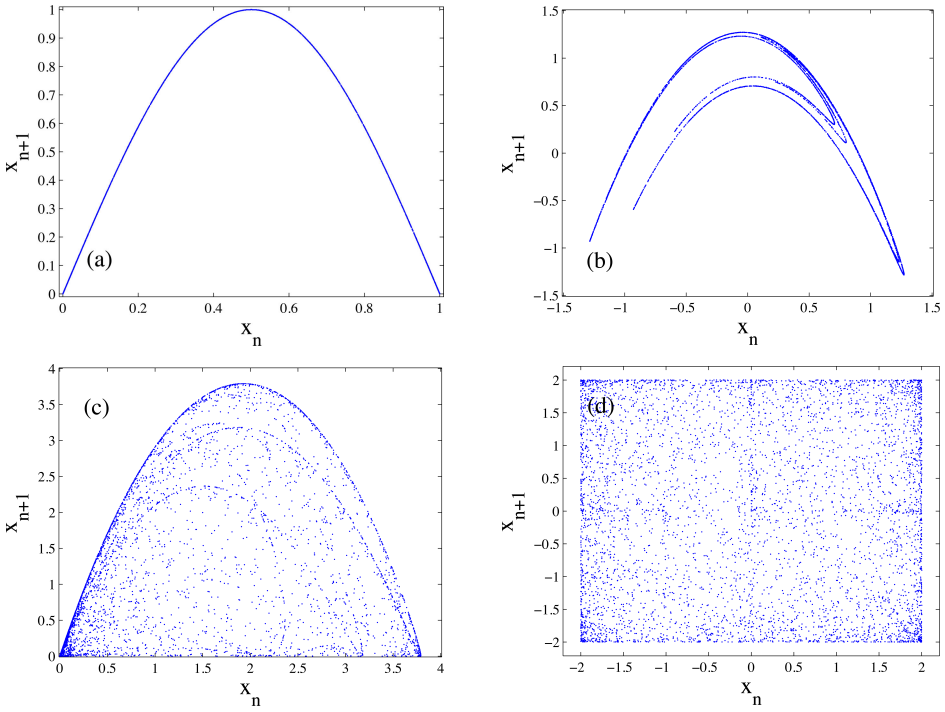


FIGURE 10. Mapping diagram of (a) Sine map; (b) Hénon map; (c) map (1) and (d) map (10).

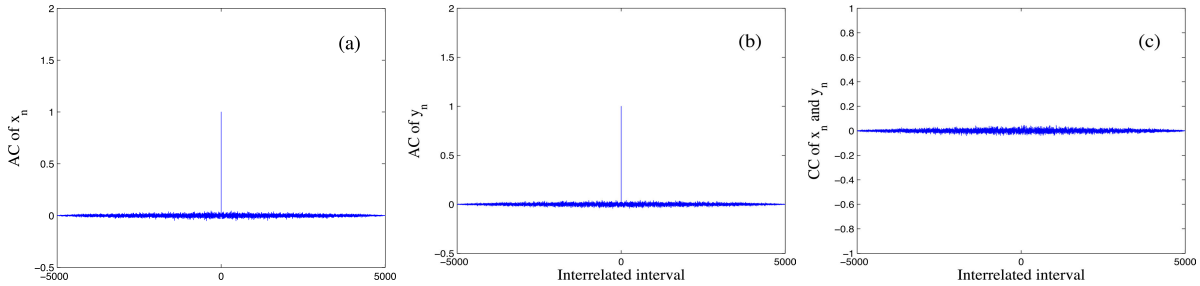


FIGURE 11. (a) Autocorrelation of x; (b) autocorrelation of y; (c) cross correlation between x and y.

the full mapping system takes up a larger digital space, and the iteration value is not easy to approximate the previous one. Therefore, the period of chaotic digital sequence can be extended and the dynamic degradation of chaotic sequence can be improved.

From Fig.11, we know that the autocorrelations of x and y in map (10) trend closer to the delta function and the cross correlation between x and y is approximated to zero. The quantitative comparisons of correlation coefficients for different maps in Table 1 show that the output sequences of map (10) have smaller absolute correlation values. Therefore, it's further indicated that the time sequences of map (10) have better pseudo-random performance.

IV. PSEUDO-RANDOM NUMBER GENERATOR

A. DESIGN OF THE CPNG

The pseudo-random number generator (PRNG) is widely applied in the fields of cryptographic system and information technology. Chaotic map is fit for the design of PRNG for the properties of sensitivity, ergodicity and unpredictability. Recently, many design methods of CPNG were proposed.

TABLE 2. Design scheme of CPNG.

Algorithm 1 CPNG Process
Step 1: Generate chaotic sequences x_1, y_1 by map (10) with initial condition (x_0, y_0).
Step 2: Generate pseudo-random sequence $T_1(s)$ according to $T_1(s_1) = \mathrm{mod}\left(floor\left(\frac{s_1 - \min(s_1)}{\max(s_1) - \min(s_1)} \cdot 10^{10} \right), 256 \right)$ $s_1 = X_1 + Y_1 + X_1 Y_1$ $X_1 = \{x_1(n) \mid n = 1,2, \quad M\}, \quad Y_1 = \{y_1(n) \mid n = 1,2, \quad M\}$
Step 3: Convert sequence T_1 into 8-bit binary sequence B_1.
Step 4: Similarly, generate pseudo-random sequence $T_2(s)$ and its 8-bit binary sequence B_2, by map (10) with initial condition $(x_0+\Delta x, y_0)$.
Step 5: Execute XOR operation on B_1 and B_2 to get B, depicted by $B = B_1(s) \oplus B_1(s)$.
Step 6:Convert binary sequence B into decimal sequence T.

TABLE 3. Cycle length of pseudo-random sequence.

	Pseudo-random sequences	Cycle length
T_1	3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2 3 4 1 2	4
T_2	1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3 1 2 3	3
$T = T_1 \oplus T_2$	2 6 2 3 1 7 0 0 0 5 3 1 2 6 2 3 1 7 0 0 0 5 3 1	12

TABLE 4. NIST test result of pseudo-random sequences.

Statistical Test	P-Value	Proportion	Result
Frequency (Monobit) Test	0.816537	99/100	Success
Frequency Test within a Block	0.401199	98/100	Success
Runs Test	0.554420	99/100	Success
Longest run test	0.678686	100/100	Success
Binary Matrix Rank Test	0.494392	100/100	Success
Discrete Fourier Transform Test	0.699313	100/100	Success
Non-overlapping Template Matching Test	0.122325	98/100	Success
Overlapping Template Matching Test	0.924076	100/100	Success
Maurer's "Universal Statistical" Test	0.924076	100/100	Success
Linear Complexity Test	0.350485	98/100	Success
Serial Test 1	0.213309	100/100	Success
Serial Test 2	0.574903	99/100	Success
Approximate Entropy Test	0.204076	61/61	Success
Cumulative Sums Test (left)	0.437274	99/100	Success
Cumulative Sums Test (right)	0.437274	98/100	Success
Random Excursions Test (mean value)	0.585209	61/61	Success
Random Excursions Variant (mean value)	0.033288	59/61	Success

The optimized robust chaotic map is suitable for the design of CPNG for presenting better dynamic performance.

The design scheme of CPNG based on the optimized robust chaotic map is described as below

B. PERFORMANCE ANALYSIS

As an important candidate of PRNG, chaotic map can provide complex pseudo-random sequences. However, for the sake of finite computing precision and digital processing of chaotic sequence, the generated numbers of CPNG may suffer from dynamical degradation, which refers to short cycle length, strong correlation, non-ergodicity and low linear-complexity [37]. This degradation often results in the performance attenuation of digital chaos applications [38]–[40]. The two pseudo-random byte sequences adopted to perform XOR operation in the proposed CPNG method are generated by the optimized chaotic maps with different initial conditions. This will extend the cycle length of the output sequence and increase the randomness of CPNG. For example, the period of sequence T_1 is 4, the period of sequence T_2 is 3. However, the cycle length of $T = T_1 \oplus T_2$ is 12, which is significantly larger than those of T_1 and T_2, as is shown in Table 3.

The randomness of the generated binary sequences by CPNG can be comprehensively evaluated by the PRNG statistical test suite NIST SP800-22. The PRNG statistical test suite consists of 15 different sub-tests for finding the nonrandom region in all sides within a test sequence. The results of the NIST-800-22 test should be greater than 0.01 for success. We set the parameters of compound map (10) as $a = 1$, $b = 1.98$, $c = 1.0$, $g_1 = 2$, $g_2 = 2$, $k_1 = 6$, $k_2 = 6$, and the initial conditions are $x_0 = 0.1$, $y_0 = 0.1$, $\Delta x = 0.00001$. The process of random number generation is based on the designed scheme in section 4.1. The bit length of the binary sequence is set to be 10^6, and 100 segments of sequences are used. The experimental result is shown in Table 4. It's concluded from Table 4 that the binary sequences generated by the introduced CPNG scheme have good statistical properties and have passed all tests of the suite.

V. CONCLUSION

Aiming at the properties of limited chaotic parameter space and small Lyapunov exponent for the existing discrete maps, this paper introduced a two-dimensional smooth map and studied its dynamical behavior. It is found that the Lyapunov exponents of the 2D map remain invariable when some parameters vary in infinite real space, and the signal amplitudes change regularly following some functional relationship in the same time. The introduced compound operation-based method can effectively increase the Lyapunov exponent of the 2D map. Thus, it theoretically guarantees that the compound map holds infinite parameter range of robust chaos and high complexity. Therefore, this work provides a new pathway for exploring the robustness and complexity of discrete chaotic system. Finally, we introduce a CPNG based on the compound map, the careful analysis shows that the proposed CPNG has high quality of randomness and can passed the rigorous NIST test. The suggested

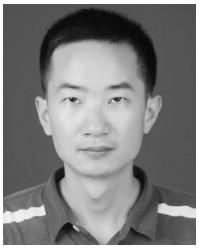
future work directions are the construction of high dimension robust chaotic map and its application.

REFERENCES

[1] C. Li, B. Feng, S. Li, J. Kurths, and G. Chen, "Dynamic analysis of digital chaotic maps via state-mapping networks," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 66, no. 6, pp. 2322–2335, Jun. 2019.
[2] F. Peng, X. Zhang, Z.-X. Lin, and M. Long, "A tunable selective encryption scheme for H.265/HEVC based on chroma IPM and coefficient scrambling," *IEEE Trans Circuits Syst Video Technol.*, to be published, doi: 10.1109/TCSVT.2019.2924910.
[3] C. Li, Y. Zhang, and E. Y. Xie, "When an attacker meets a cipher-image in 2018: A year in review," *J. Inf. Secur. Appl.*, vol. 48, Oct. 2019, Art. no. 102361.
[4] F. Peng, Q. Long, Z.-X. Lin, and M. Long, "A reversible watermarking for authenticating 2D CAD engineering graphics based on iterative embedding and virtual coordinates," *Multimed Tools Appl.*, vol. 78, no. 19, pp. 26885–26905, 2019.
[5] F. Peng, Z.-X. Lin, X. Zhang, and M. Long, "Reversible data hiding in encrypted 2D vector graphics based on reversible mapping model for real numbers," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 9, pp. 2400–2411, Sep. 2019.
[6] A. A. A. El-Latif, B. Abd-El-Atty, and M. Talha, "Robust encryption of quantum medical images," *IEEE Access*, vol. 6, pp. 1073–1081, 2017.
[7] S. Jafari, A. Ahmadi, A. J. M. Khalaf, H. R. Abdolmohammadi, V.-T. Pham, and F. E. Alsaadi, "A new hidden chaotic attractor with extreme multi-stability," *AEU-Int. J. Electron. Commun.*, vol. 89, pp. 131–135, May 2018.
[8] V.-T. Pham, C. Volos, S. T. Kingni, T. Kapitaniak, and S. Jafari, "Bistable hidden attractors in a novel chaotic system with hyperbolic sine equilibrium," *Circuits, Syst., Signal Process.*, vol. 37, no. 3, pp. 1028–1043, 2018.
[9] S. Jafari, V.-T. Pham, S. M. R. H. Golpayegani, M. Moghtadaei, and S. T. Kingni, "The relationship between chaotic maps and some chaotic systems with hidden attractors," *Int. J. Bifurcation Chaos*, vol. 26, no. 13, 2016, Art. no. 1650211.
[10] D. Aniszewska, "New discrete chaotic multiplicative maps based on the logistic map," *Int. J. Bifurcation Chaos*, vol. 28, no. 9, 2018, Art. no. 1850118.
[11] G. Livadiotis, "High density nodes in the chaotic region of 1D discrete maps," *Entropy*, vol. 20, no. 1, p. 24, 2018.
[12] R. Alonso-Sanz, J. C. Losada, and M. A. Porras, "Bifurcation and chaos in the logistic map with memory," *Int. J. Bifurcation Chaos*, vol. 27, no. 12, 2017, Art. no. 1750190.
[13] S. Panahi, J. C. Sprott, and S. Jafari, "Two simplest quadratic chaotic maps without equilibrium," *Int. J. Bifurcation Chaos*, vol. 28, no. 12, 2018, Art. no. 1850144.
[14] 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.
[15] G.-Y. Wang and F. Yuan, "Cascade chaos and its dynamic characteristics," *Acta Phys. Sinica* vol. 62, no. 2, 2013, Art. no. 020506.
[16] 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.
[17] F. Yuan, Y. Deng, Y. Li, and G. Chen, "A cascading method for constructing new discrete chaotic systems with better randomness," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 29, no. 5, 2019, Art. no. 053120.
[18] 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.
[19] A. S. Saljoughi and H. Mirvaziri, "A new method for image encryption by 3D chaotic map," *Pattern Anal. Appl.*, vol. 22, no. 1, pp. 243–257, 2019.
[20] J. Li and H. Liu, "Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map," *IET Inf. Secur.*, vol. 7, no. 4, pp. 265–270, Dec. 2013.
[21] W. Liu, K. Sun, and S. He, "SF-SIMM high-dimensional hyperchaotic map and its performance analysis," *Nonlinear Dyn.*, vol. 89, no. 4, pp. 2521–2532, 2017.
[22] M. Yu, K. Sun, W. Liu, and S. He, "A hyperchaotic map with grid sinusoidal cavity," *Chaos, Solitons Fractals*, vol. 106, pp. 107–117, Jan. 2018.
[23] Y. Peng, K. Sun, D. Peng, and W. Ai, "Dynamics of a higher dimensional fractional-order chaotic map," *Phys. A, Stat. Mech. Appl.*, vol. 525, pp. 96–107, Jul. 2019.
[24] C. Cao, K. Sun, and W. Liu, "A novel bit-level image encryption algorithm based on 2D-LICM hyperchaotic map," *Signal Process.*, vol. 143, pp. 122–133, Feb. 2018.
[25] L.-Y. Sheng, K.-H. Sun, and C.-B. Li, "Study of a discrete chaotic system based on tangent-delay for elliptic reflecting cavity and its properties," *Acta Phys. Sinica*, vol. 53, no. 9, pp. 2871–2876, 2004.
[26] Y. Naseer, D. Shah, and T. Shah, "A novel approach to improve multimedia security utilizing 3D mixed chaotic map," *Microprocessors Microsyst.* vol. 65, pp. 1–6, Mar. 2019.
[27] M. Y. Valandar, M. J. Barani, P. Ayubi, and M. Aghazadeh, "An integer wavelet transform image steganography method based on 3D sine chaotic map," *Multimedia Tools Appl.*, vol. 78, no. 8, pp. 9971–9989, 2019.
[28] 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.
[29] S. Banerjee, J. A. Yorke, and C. Grebogi, "Robust chaos," *Phys. Rev. Lett.*, vol. 80, no. 14, pp. 3049–3052, 1998.
[30] S. Banerjee and C. Grebogi, "Border collision bifurcations in two-dimensional piecewise smooth maps," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 59, no. 4, p. 4052, 1999.
[31] D. Han, L. Min, and L. Hao, "A chaos robustness criterion for 2D piecewise smooth map with applications in pseudorandom number generator and image encryption with avalanche effect," *Math. Problems Eng.*, vol. 2016, pp. 1–14, Jan. 2016.
[32] M. Andrecut and M. K. Ali, "Robust chaos in smooth unimodal maps," *Phys. Rev. E, Stat. Phys. Plasmas Fluids Relat. Interdiscip. Top.*, vol. 64, no. 2, 2001, Art. no. 025203.
[33] M. Patra and S. Banerjee, "Robust chaos in 3-D piecewise linear maps," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 28, no. 12, 2018, Art. no. 123101.
[34] C. Li and J. Zhang, "Synchronisation of a fractional-order chaotic system using finite-time input-to-state stability," *Int. J. Syst. Sci.*, vol. 47, no. 10, pp. 2440–2448, Jul. 2016.
[35] C. Li, K. Su, and J. Zhang, "Amplitude control and projective synchronization of a dynamical system with exponential nonlinearity," *Appl. Math. Model.*, vol. 39, no. 18, pp. 5392–5398, 2015.
[36] C. Li, L. Wu, H. Li, and Y. Tong, "A novel chaotic system and its topological horseshoe," *Nonlinear Anal., Model. Control*, vol. 18, no. 1, pp. 66–77, 2013.
[37] Z. Zhuang, J. Wang, J. Liu, D. Yang, and S. Chen, "A new digital image encryption algorithm based on improved logistic mapping and Josephus circle," *J. Comput. Commun.*, vol. 6, no. 6, pp. 31–44, 2018.
[38] L. Zhou, C. Wang, X. Zhang, and W. Yao, "Various attractors, coexisting attractors and antimonotonicity in a simple fourth-order memristive twin-T oscillator," *Int. J. Bifurcation Chaos*, vol. 28, no. 4, 2018, Art. no. 1850050.
[39] Y. Liu, Y. Luo, S. Song, L. Cao, J. Liu, and J. Harkin, "Counteracting dynamical degradation of digital chaotic Chebyshev map via perturbation," *Int. J. Bifurcation Chaos*, vol. 27, no. 3, 2017, Art. no. 1750033.
[40] Y. Luo, R. Zhou, J. Liu, C. Yi, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.

CHUNLAI LI received the Master of Engineering degree from the College of Electronic Engineering, Guangxi Normal University, Guilin, China, in 2006, and the Ph.D. degree from the College of Automation, Guangdong University of Technology, Guangzhou, China, in 2012. He is currently a Professor with the College of Physics and Electronics, Hunan Institute of Science and Technology. His current research interests include chaos dynamics, chaotic encryption, chaos control, and stable operation of power systems.

KUN QIAN received the Ph.D. degree in instrumentation science and technology from the School of Instrument and Electronics, North University of China, Taiyuan, China, in 2017. He is currently an Associate Professor with the College of Physics and Electronic Sciences, Hunan Institute of Science and Technology, Hunan, China. His research interests include chaotic systems, chaotic image encryption, and cryptanalysis.



SHAOBO HE received the B.Sc., M.S., and Ph.D. degrees from the School of Physics and Electronics, Central South University, Changsha, China, in 2010, 2013, and 2016, respectively. He is currently a Postdoctor of physics with Central South University. This position is supported by the Postdoctoral Innovative Talent Support Program. His research interests include dynamical analysis and applications of nonlinear systems, especially those with fractional derivative.

HONGMIN LI received the M.Sc. degree in communications and information systems from the College of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing, China, in 2003, and the Ph.D. degree in electrical engineering from Hunan University, Changsha, China, in 2008. He is currently a Professor and the Head of the College of Physics and Electronics, Hunan Institute of Science and Technology, Hunan, China. His research interests include signal processing, wavelet analysis, and analog-integrated design.

WEI FENG received the M.Sc. degree in computer applied technology from the College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, China, in 2007. He is currently pursuing the Ph.D. degree in electrical engineering with the Hefei University of Technology, Anhui, China. He is also an Associate Professor with the College of Physics and Electronics, Hunan Institute of Science and Technology, Hunan, China. His research interests include chaotic systems, chaotic image encryption, and cryptanalysis.