

n -Dimensional Chaotic Map with application in secure communication

Weijia Cao ^{a,b,c}, Hang Cai ^d, Zhongyun Hua ^{d,*}

^a Aerospace Information Research Institute, Chinese Academy of Sciences, Beijing 100094, China

^b University of Macau, Macau 999078, China

^c Yangtze Three Gorges Technology and Economy Development Co Ltd., Beijing 101100, China

^d School of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, Shenzhen 518055, China

ARTICLE INFO

Keywords:

Chaotic system
Chaotic map
Secure communication
Lyapunov exponent
Image encryption

ABSTRACT

When applied to practical applications, existing chaotic systems exhibit many weaknesses, including discontinuous chaotic intervals and easily predicted chaotic signals. This study proposes an n -dimensional chaotic model (n D-CM) to resolve the weaknesses of existing chaotic systems. n D-CM can produce chaotic maps with any desired dimension utilizing existing 1D chaotic maps as seed chaotic maps. To demonstrate the effect of n D-CM, we generate three 2D and one 3D chaotic map as examples, utilizing three 1D chaotic maps as the seed maps. The evaluation and experiment results show that these newly generated chaotic maps can obtain continuous and wider chaotic intervals and better performance using the indicators of the Lyapunov exponent, sample entropy and correlation dimension, compared to existing maps. To further show the practicality of n D-CM, the generated maps are additionally applied to secure communication. The experimental results show that these chaotic maps exhibit much better performance in resisting transmission noise in this application than existing chaotic maps.

1. Introduction

Recently, nonlinear theories have attracted increasing attention [1, 2]. As a typical branch of non-linear theory, the chaos theory demonstrates nonlinear behaviors that are extremely sensitive to their initial states [3,4]. Based on Devaney's definition, a nonlinear system with chaotic behavior should exhibit initial state sensitivity, topological mixing, and dense periodic orbits [5]. Due to these significant properties, chaos theory has been widely applied into various scientific and engineering fields [6–9]. For example, chaotic systems are commonly used in secure communication and random number generators [10–12], because the outputs of chaotic systems can carry confidential data [13]; moreover, chaotic systems have similar properties to pseudo-random number generators [14].

Recently, many research reports have indicated that existing chaotic systems have many weaknesses when applied to real engineering applications [15,16]. First, many chaotic systems exhibit discontinuous chaotic ranges [17,18], for example, the well-known Hénon map [5]. The continuity of a chaotic range indicates that the chaotic system exhibits chaotic behavior in a continuous parameter range. All digital platforms have finite precision. When a chaotic system is implemented on these platforms, its digitalized parameter(s) can only achieve approximate values. If the chaotic ranges are discontinuous, a slight

disturbance to the parameters may result in the parameter(s) without chaotic ranges, leading to chaotic behaviors degrading to regular behaviors [19]. Thus, the discontinuous chaotic ranges of chaotic systems have serious adverse effects in many chaos-based practical applications [20,21].

In addition, many research reports have indicated that the chaotic signals can be predicted if the structures of the related chaotic maps are simple [22–24]. These studies estimated chaotic signals by identifying the mathematical models of the chaotic systems generating the signals [25,26], deducing the initial states' control parameters [27,28], or predicting the chaotic signals directly [29,30]. The unpredictability of chaotic systems is required for many practical applications that use chaos. When the chaotic signals of a chaotic system are successfully estimated, the chaotic system in these applications is ineffective [31]. For example, in chaos-based cryptography systems, if the attackers can successfully predict the chaotic signals, they can determine the emulative keys of the cryptography systems and thus, break the cryptography systems without secure keys [20,32,33].

To date, researchers have developed many techniques to increase the complexity of existing chaotic systems [34,35]. These studies can be divided into two based on the strategies they use. The first strategy directly enhances the dynamic complexity of the existing chaotic signals by disturbing the chaotic signals or control parameters [18,36,37].

* Corresponding author.

E-mail address: huazhongyun@hit.edu.cn (Z. Hua).

This strategy works well in specific applications. However, in [38], the effectiveness of this strategy for enhancing chaos complexity was proved to be limited and unsuitable for some applications that require robust chaos. Another method of strengthening chaotic complexity is to produce new chaotic systems with more complex behaviors [39,40]. These new chaotic systems are created by either using existing maps as seed maps or directly from nonlinear equations. This strategy can significantly enhance the complexity of existing chaotic maps. However, they primarily focus on low-dimensional systems. A high-dimensional system typically has more complex structures and behaviors than a low-dimensional system and thus computation with this system is difficult [41]. Few methods for generating high-dimensional chaotic systems consider the continuity of chaotic ranges, which means that these chaotic systems do not have continuous chaotic ranges [3,33]. These weaknesses occur in general chaotic systems because most existing ones do not have continuous chaotic ranges. Thus, developing high-dimensional chaotic systems with more complex chaotic behaviors is required.

This study proposes an n -dimensional chaotic model (n D-CM) to overcome these drawbacks of the existing chaotic systems. The n D-CM can produce chaotic maps of any dimension by utilizing 1D chaotic maps as seed chaotic maps. Property discussions show the effects of n D-CM. To experimentally demonstrate the effectiveness of n D-CM, three 2D and one 3D chaotic map are produced as examples, utilizing three 1D chaotic maps as seed chaotic maps. The performance analysis demonstrates that these new chaotic maps have wide and continuous chaotic ranges. To illustrate the practicality of the n D-CM, we applied these newly produced chaotic maps to secure communication. The experimental results show that the maps generated by n D-CM show much better performance in resisting transmission noise in this application than the existing maps.

The remainder of this paper is organized as follows. Section 2 presents the three existing 1D chaotic systems and discusses their properties. Section 3 introduces the proposed n D-CM and illustrates several new 2D and 3D chaotic maps produced by n D-CM. Section 4 measures the performance indicators of the chaotic maps produced by n D-CM, and Section 5 applies the generated chaotic maps to secure communication application. The final section concludes the paper.

2. 1D chaotic maps

We first present three 1D classic chaotic maps as a background and discuss their dynamic properties. Our proposed chaotic model uses them as seed chaotic maps, as discussed in Section 3.

2.1. Definitions of three 1D maps

The logistic map was built to model the growth of popularity, and its mathematical equation is defined as

$$x_{i+1} = L(x_i) = 4ax_i(1 - x_i), \quad (1)$$

where a acts as the control parameter with $a \in [0, 1]$.

A fraction map was developed to model the random behavior of a genetic algorithm in evolutionary computation [42]. The equation is described as

$$x_{i+1} = F(x_i) = \frac{1}{x_i^2 + 0.1} - bx_i. \quad (2)$$

Its dynamic properties are typically analyzed for its control parameter $b \in [0, 1]$.

Trigonometric functions exhibit complex nonlinear properties. By scaling with π , the sine transform can map input of range $(0, 1)$ to the same range $(0, 1)$, and thus can derive to the sine map. The sine map is defined as

$$x_{i+1} = S(x_i) = c \sin(\pi x_i). \quad (3)$$

The c acts as a control parameter, with $c \in [0, 1]$.

A bifurcation diagram plots the distributions for a dynamic system's output states depending on its control parameter(s). In contrast, the Lyapunov exponent (LE) tests the average exponential separation rate between two close trajectories beginning from two closed initial values [43]. A positive LE means that these two trajectories will separate in every unit of time and thereby is an indicator of chaos if the phase space of the dynamic system is also bounded. Fig. 1 plots the bifurcation diagrams and LEs of the three existing maps. These maps exhibit chaotic behaviors only in minimal parameter settings, and have discontinuous chaotic ranges. In addition, their outputs can be distributed over a restricted area in the phase plane.

2.2. Performance analysis

According to the mathematical definitions, plotted bifurcation diagrams, and calculated LEs, the logistic, fraction, and sine maps have many noticeable properties. Firstly, as shown in Fig. 1, the chaotic ranges of these chaotic maps are narrow and discontinuous. Minor changes in their parameters could lead them to fall into the non-chaotic ranges and lead to chaotic behaviors degrading to regular behaviors. Secondly, chaotic maps have incomplete output distributions. This implies that their outputs can visit a restricted region in the phase plane and cannot be distributed uniformly. Thirdly, their structures and chaotic behaviors are straightforward. This may lead to chaotic degradation. These properties can negatively affect the practical applications of chaos. Thus, it is meaningful to resolve the weaknesses of these chaotic systems, which can benefit practical applications that use chaos.

3. n -Dimensional chaotic model

This section first presents the n -dimensional chaotic model (n D-CM), and then generates several 2D and 3D new chaotic maps by n D-CM utilizing these 1D chaotic maps introduced in Section 2.

3.1. n D-CM

n D-CM was developed to resolve the issues associated with existing chaotic systems. It can produce chaotic maps with any dimension by performing a sine transformation on the addition results of the seed chaotic maps. The mathematical structure of n D-CM is defined as

$$\begin{cases} x_{1,i+1} = \sin(\pi(F_1(x_{1,i}) + F_2(x_{2,i}) + \dots + F_n(x_{n,i}))) \\ x_{2,i+1} = \sin(\pi(F_1(x_{2,i}) + F_2(x_{3,i}) + \dots + F_n(x_{1,i}))) \\ \vdots \\ x_{n,i+1} = \sin(\pi(F_1(x_{n,i}) + F_2(x_{1,i}) + \dots + F_n(x_{n-1,i}))), \end{cases} \quad (4)$$

where $F_1(\cdot)$, $F_2(\cdot)$, \dots , and $F_n(\cdot)$ are n seed chaotic maps that are all 1D chaotic maps, and $\mathbf{x}(i) = \{x_{1,i}, x_{2,i}, \dots, x_{n,i}\}$ is an n -length vector that is the i th observation states of the chaotic model. Several n seed chaotic maps are required to produce an n -D chaotic map. For each dimension, the n D-CM combines the outputs of the n seed chaotic maps and then performs a sine transformation on the addition results of all the seed chaotic maps. The next dimension is generated by shifting the inputs of the n seed chaotic maps from the current dimension. The combinations of the outputs of the n equations are the outputs of n D-CM, which are also for recursive iterations.

The sine transformation is a bounded operation that exhibits complex nonlinearity. This can generate chaos for any parameter setting. Therefore, the proposed n D-CM has the following properties. (1) The proposed n D-CM is an effective but straightforward chaos generation model. Users can flexibly produce chaotic maps of any dimension by combining various seed chaotic maps. When swapping n seed chaotic maps in the generation, different n D chaotic systems can be produced. (2) The newly produced n D chaotic maps can overcome the drawbacks

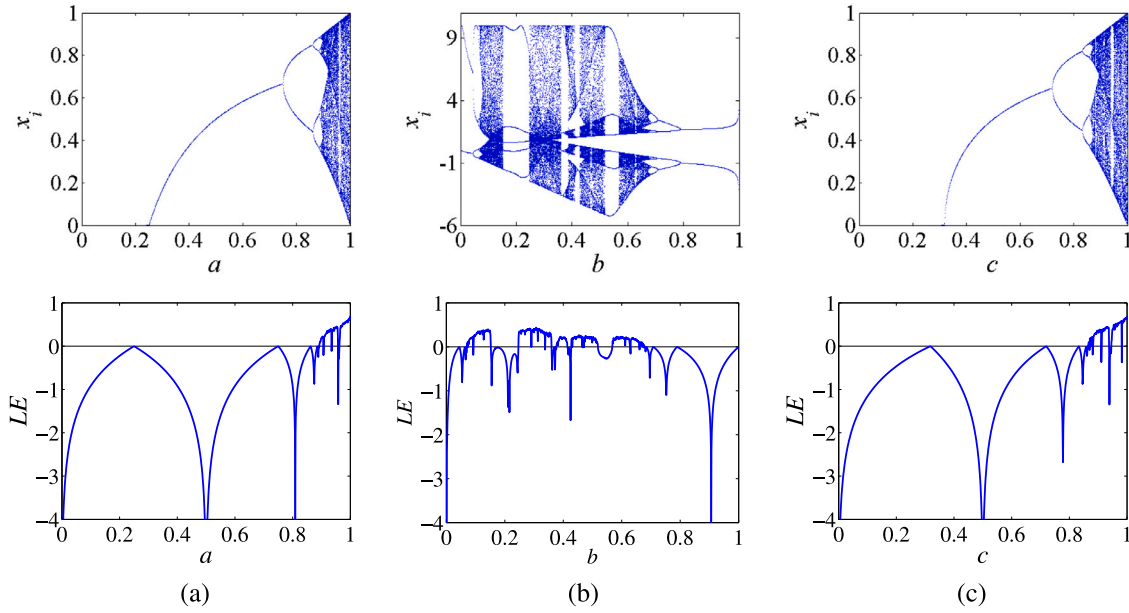


Fig. 1. Top and bottom rows depict the bifurcation diagrams and LEs of the (a) logistic, (b) fraction, and (c) sine maps along their control parameters.

of existing maps in discontinuous chaotic intervals and nonuniformly distributed signals. (3) The generated n D chaotic maps exhibit chaos in large parameter ranges in contrast to most existing chaotic systems, who exhibit chaos only in very narrow parameter ranges.

3.2. Examples of 2D chaotic map

To demonstrate the advantages of n D-CM in producing chaotic maps, we applied the n D-CM to generate three 2D and one 3D chaotic map utilizing the chaotic maps presented in Section 2 as seed chaotic maps.

3.2.1. 2D logistic-fraction map

When selecting the logistic and fraction maps as the two seed chaotic maps in Eq. (4), the seed chaotic maps $F_1(\cdot)$ and $F_2(\cdot)$ are set as the logistic and fraction maps, respectively. A new 2D logistic-fraction (2D-LF) map is generated, and its mathematical equation is written as

$$\begin{cases} x_{i+1} = \sin(\pi(4p_1x_i(1-x_i) + \frac{1}{y_i^2+0.1} - p_2y_i)) \\ y_{i+1} = \sin(\pi(4p_1y_i(1-y_i) + \frac{1}{x_i^2+0.1} - p_2x_i)), \end{cases} \quad (5)$$

where p_1 and p_2 act as two control parameters inherited from the logistic and fraction maps, respectively. Because the sine transformation is a bounded operation, the parameters p_1 and p_2 can have large values. This study investigates the properties of the 2D-LF map for $p_1, p_2 \in [1, 100]$.

3.2.2. 2D logistic-sine map

When changing one seed chaotic map to generate the 2D-LF map, setting the seed chaotic maps $F_1(\cdot)$ and $F_2(\cdot)$ as the logistic and sine maps, respectively, the 2D logistic-sine (2D-LS) map is generated and given as

$$\begin{cases} x_{i+1} = \sin(\pi(4p_1x_i(1-x_i) + p_2\sin(\pi y_i))) \\ y_{i+1} = \sin(\pi(4p_1y_i(1-y_i) + p_2\sin(\pi x_i))), \end{cases} \quad (6)$$

where p_1 and p_2 are two control parameters of the 2D-LS map. We set the ranges of these parameters to be the same as the two parameters in the 2D-LF map, namely $p_1, p_2 \in [1, 100]$.

3.2.3. 2D fraction-sine map

When setting the two seed chaotic maps $F_1(\cdot)$ and $F_2(\cdot)$ in Eq. (4) as the fraction and sine maps, respectively, the new chaotic map 2D fraction-sine (2D-FS) map is obtained and is written as

$$\begin{cases} x_{i+1} = \sin(\pi(\frac{1}{x_i^2+0.1} - p_1x_i + p_2\sin(\pi y_i))) \\ y_{i+1} = \sin(\pi(\frac{1}{y_i^2+0.1} - p_1y_i + p_2\sin(\pi x_i))). \end{cases} \quad (7)$$

Similar to the two parameters in the 2D-LF and 2D-LS maps, the two parameters p_1 and p_2 can also have large values and we limit their values within $[1, 100]$ in this study.

The phase space trajectory of a dynamic system plots the visited and approached points of a 2D dynamic system under a fixed parameter setting. Fig. 2 plots the bifurcation diagrams of the 2D-LF, 2D-LS and 2D-FS maps for the parameters $(p_1, p_2) \in [1, 100]$ and their trajectories when the parameters $(p_1, p_2) = (50, 50)$. It is evident that the two variables x_i and y_i are uniformly distributed in the range $[-1, 1]$, which indicates that these outputs can entry all areas of its 2D phase plane. These 2D chaotic maps have robust chaotic behaviors. On the view of this point, the new 2D chaotic maps produced by n D-CM exhibit extremely complicated behaviors and large chaotic parameter ranges. With uniformly distributed outputs and continuous chaotic ranges, these new chaotic maps have advantages in many practical applications, such as the chaos-based random number generators.

3.3. Example of 3D chaotic map

The proposed n D-CM can generate high-dimensional chaotic maps. To demonstrate this effect, we created a 3D chaotic map as an example, utilizing the three 1D chaotic maps introduced in Section 2 as seed chaotic maps.

When setting the logistic, fraction, and sine maps as the three seed chaotic maps $F_1(\cdot)$, $F_2(\cdot)$ and $F_3(\cdot)$, a 3D logistic-fraction-sine (3D-LFS) map is generated, and its mathematical equation can be written as

$$\begin{cases} x_{i+1} = \sin(\pi(4p_1x_i(1-x_i) + \frac{1}{y_i^2+0.1} - p_2y_i + p_3\sin(\pi z_i))) \\ y_{i+1} = \sin(\pi(4p_1y_i(1-y_i) + \frac{1}{z_i^2+0.1} - p_2z_i + p_3\sin(\pi x_i))) \\ z_{i+1} = \sin(\pi(4p_1z_i(1-z_i) + \frac{1}{x_i^2+0.1} - p_2x_i + p_3\sin(\pi y_i))), \end{cases} \quad (8)$$

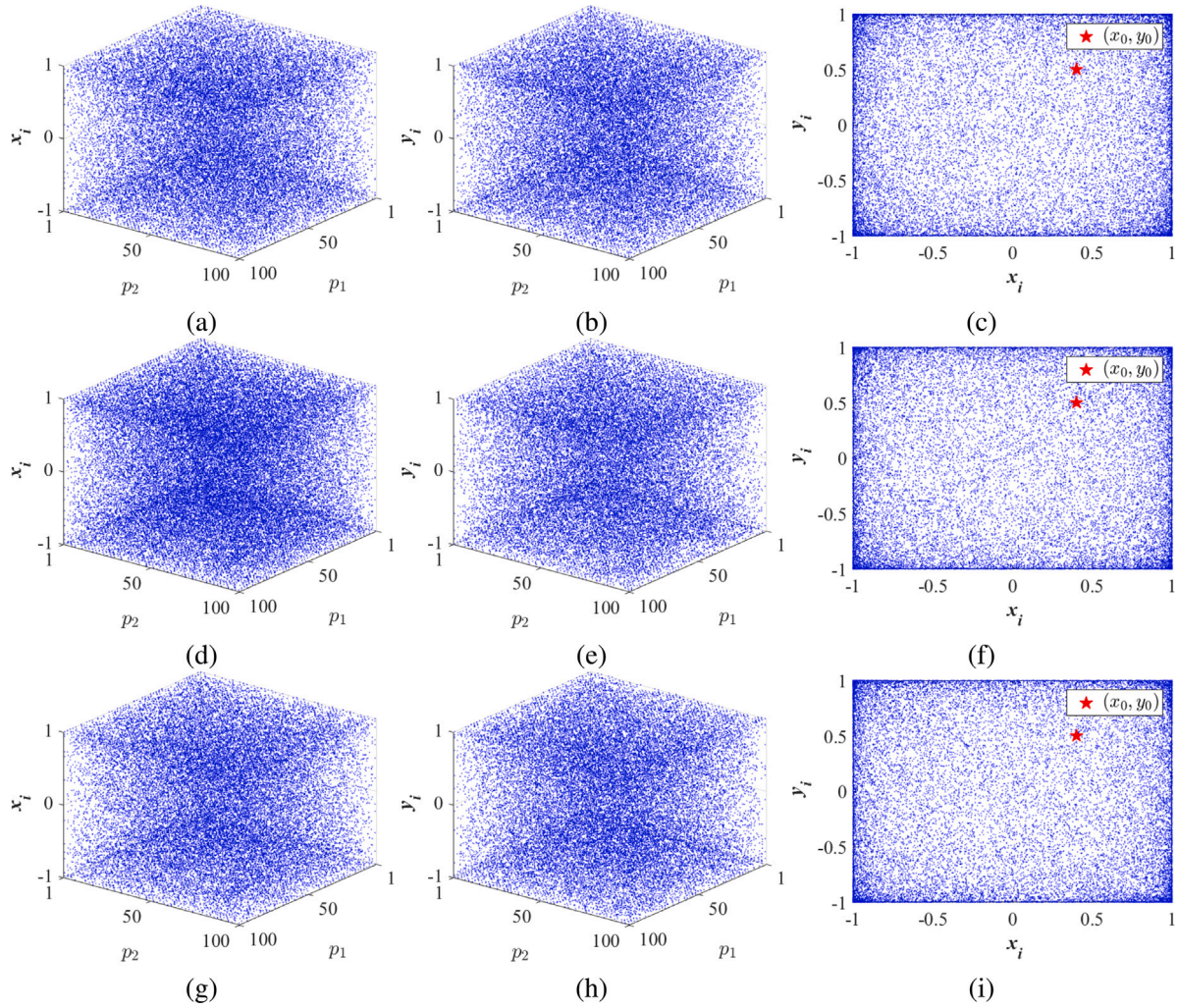


Fig. 2. 3D bifurcation diagrams and 2D trajectories for (a)–(c) 2D-LF map, (d)–(f) 2D-LS map, and (g)–(i) 2D-FS map.

where p_1 , p_2 and p_3 are the three parameters of the 3D-LFS map inherited from the logistic, faction, and sine maps, respectively. As the sine transform is a bounded operation, these three parameters can have large values. This study also investigates the ranges of these three parameters for $p_1, p_2, p_3 \in [1, 100]$.

Fig. 3 plots the bifurcation diagrams of the variable x_i and its 3D trajectory under a fixed parameter setting. To better show the dynamic behaviors of the 3D-LFS map, we plotted the bifurcation diagrams under the parameter space of the two parameters by setting the other parameter as a fixed value. Only the bifurcation diagrams of x_i are plotted because the bifurcation diagrams of variables y_i and z_i have similar visual effects as the bifurcation diagrams of x_i . The 3D-LFS map can generate outputs with uniform distributions in a large and continuous parameter space, which indicates the complex and stable chaotic behaviors of the 3D-LFS map.

4. Performance evaluations

The proposed n D-CM method produces chaotic maps with several advantages. This section qualitatively measures the performance indicators of new 2D and 3D chaotic maps to demonstrate this effect.

4.1. Lyapunov exponent

“chaos” is a kind of observed behavior with no common standard to define its existence. Among the various definitions of chaos, LE is

regarded as a widely accepted criterion for measuring chaos [43]. The LE defines chaos by characterizing the separation rate of extremely close trajectories. Mathematically, the LE of a dynamic system $H(x)$ is given by

$$LE = \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \ln \left| \frac{H^{(n)}(x_0 + \delta) - H^{(n)}(x_0)}{\delta} \right| \right\}, \quad (9)$$

where δ denotes a small positive value. From the definition of LE, one can see that the average divergence of the close trajectory rate is e^{LE} . Thus, a positive LE means the exponential separation of the close trajectories, and is thereby taken as an indication of chaos when the phase plane of the dynamic system is bounded. For a dynamic system, its LE number equals the dimensionality of its phase plane, and a multi-dimensional system has several LEs. Two or more positive LEs indicate that the trajectories diverged from several dimensions. This further suggests that the dynamic system exhibits hyperchaotic behavior. In addition, since the LE characterizes the separation rate of extremely close trajectories of a chaotic system, a larger positive LE indicates more sensitive to initial conditions [43].

Fig. 4 shows the calculated LEs of the 2D chaotic maps produced by the n D-CM with existing 2D chaotic maps containing the Hénon, Duffing and Zeraoulia–Sprott maps. It is clear that these existing 2D chaotic maps only have positive LEs in very narrow intervals and discontinuous ranges. However, the 2D-LF, 2D-LS and 2D-FS maps produced by the n D-CM can achieve positive LEs under all parameters and have continuous chaotic parameter ranges. In addition, the existing

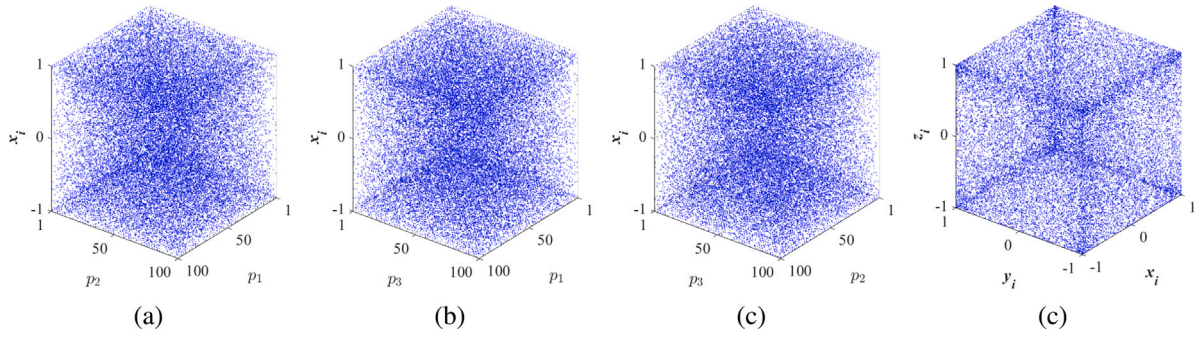


Fig. 3. Bifurcation diagrams and trajectory of the 3D-LFS map. Bifurcation diagrams of the variables x_i for the parameters (a) $p_3 = 50$, (b) $p_2 = 50$ and $p_1 = 50$. (d) Trajectory for the parameters $(p_1, p_2, p_3) = (50, 50, 50)$.

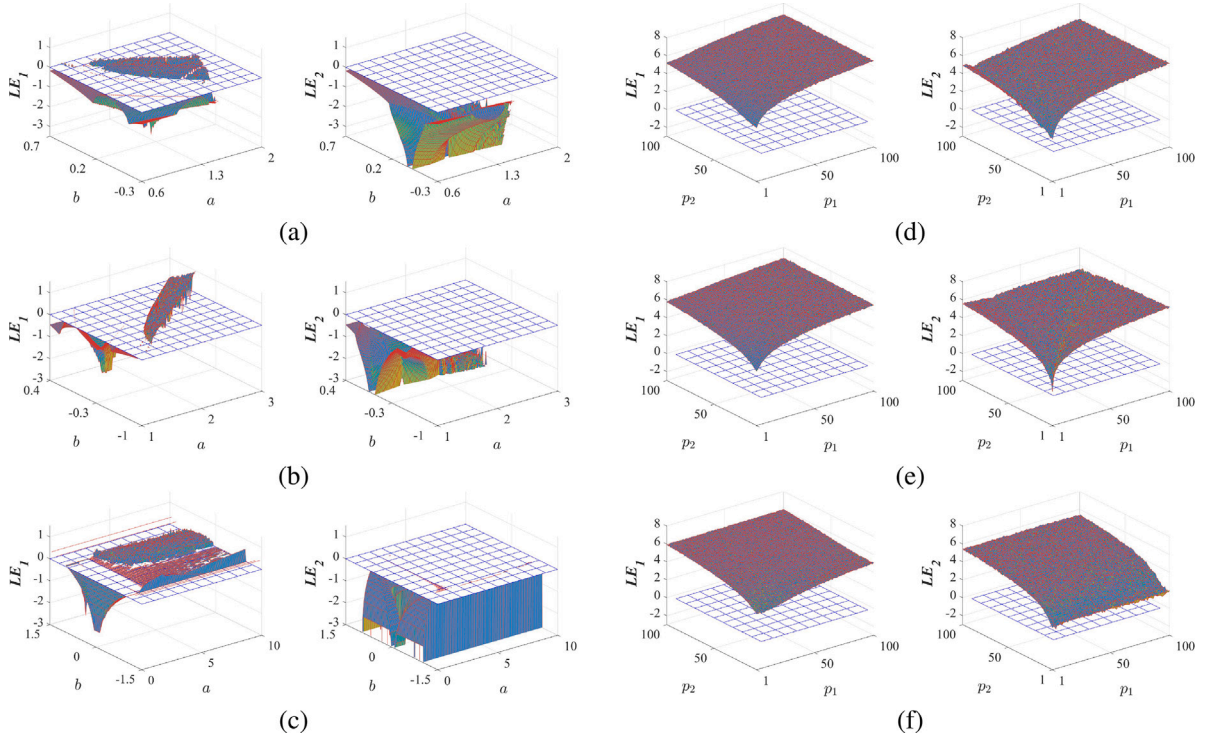


Fig. 4. Two LEs for different 2D chaotic maps under their control parameters. (a) Hénon map; (b) Duffing map; (c) Zeraouia-Sprott map; (d) 2D-LF map; (e) 2D-LS map; (f) 2D-FS map.

2D chaotic maps have only one positive LE, whereas these new maps have two positive LEs and their LEs are much larger than those of the existing ones. Thus, 2D chaotic maps can exhibit hyperchaotic behaviors and much more complex behaviors.

Fig. 5 shows the three LEs of the 3D-LFS generated by nD -CM. To display the LEs in the entire parameter space (p_1, p_2, p_3) , we plotted their LEs in 3D coordinates and used color to represent the LE values. It can be observed that 3D-LFS has positive LEs for all parameter settings. In addition, it has three positive LEs except for a few parameter settings. This indicates the advantages of 3D-LFS.

4.2. Sample entropy

Sample entropy (SE) is a measurement for testing the complexity level within a time-series [44] and is widely utilized to test the complexity of chaotic sequences. For a sequence $\{x_1, x_2, \dots, x_N\}$ and dimension m , SE can be defined as

$$SE(m, r, N) = -\log \frac{A}{B}, \quad (10)$$

where A and B are vector numbers that satisfy $d[X_{m+1}(i), X_{m+1}(j)] < r$ and $d[X_m(i), X_m(j)] < r$. The $X_m(i)$ is a vector comprising $X_m(i) = \{x_i, x_{i+1}, \dots, x_{i+m-1}\}$. The $d[X_m(i), X_m(j)]$ represents the Chebyshev distance [45] between the two vectors $X_m(i)$ and $X_m(j)$, where r is a predefined distance. A positive SE indicates that the corresponding chaotic map can output chaotic sequences with chaotic behavior. A larger SE demonstrates a smaller regularity of the chaotic sequence and indicates the higher complexity of the corresponding chaotic map [44].

Fig. 6 shows the calculated SEs of the newly generated and existing 2D chaotic maps. Note that we only plot the SEs of the chaotic signal $X = \{x_i | i = 1, 2, \dots\}$ of these chaotic maps, because the chaotic signals from different dimensions have similar SEs. These existing 2D chaotic maps can have positive SEs in narrow and discontinuous parameter ranges. Conversely, the 2D-LF, 2D-LS, and 2D-FS maps generated by the nD -CM can achieve positive SEs within all parameters, and their SEs are much larger than those of the existing chaotic maps. These results demonstrate the consistency of the results of the LE experiments.

Fig. 7 shows the SEs of the chaotic signal $X = \{x_i | i = 1, 2, \dots\}$ in the 3D-LFS map. We plot only their SEs with two control parameters and set the third parameter as a fixed value to clearly demonstrate

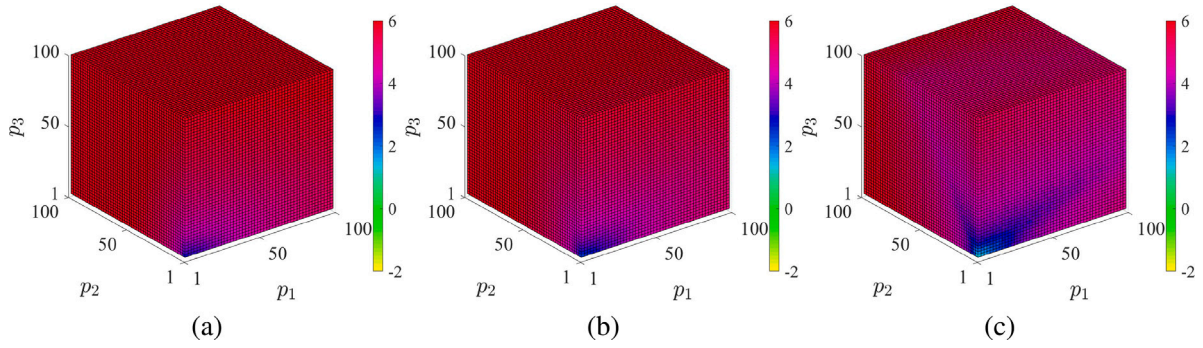


Fig. 5. Three LEs of the 3D-LFS map 2D along the change of its three control parameters. (a) First LE; (b) Second LE; (c) Third LE. (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

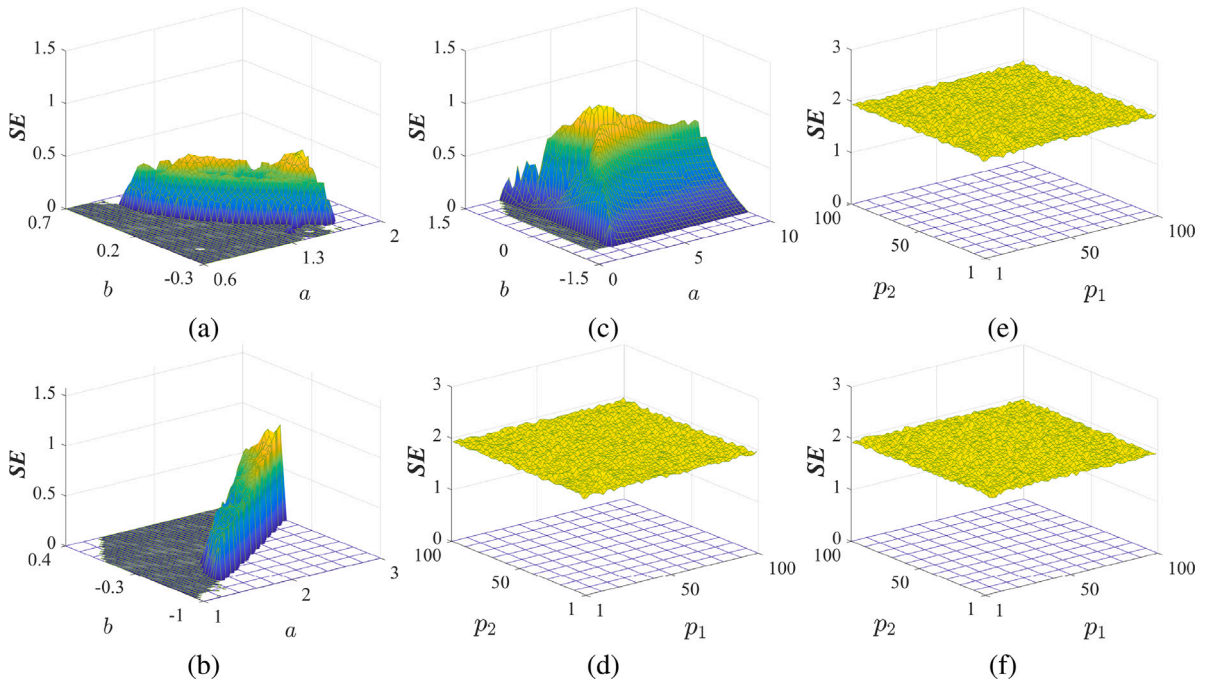


Fig. 6. SEs for different 2D chaotic maps along the change of their parameter values. (a) Hénon map; (b) Duffing map; (c) Zeraoulia-Sprott map; (d) 2D-LF map; (e) 2D-LS map; (f) 2D-FS map.

the experimental effect. One can observe that the 3D-LFS can achieve positive SEs under all parameter values, and its SEs are the same for different parameter values. This indicates that the 3D-LFS map can achieve robust chaotic behavior.

4.3. Correlation dimension

The correlation dimension (CD) is a fractal dimension and developed to measure the space dimensionality of a time series [46]. When a system's chaotic sequence has a CD larger than 0, the dynamic system exhibits chaotic behavior and a larger CD usually indicates a higher dimensionality [46]. For a time series $\{s_1, s_2, \dots, s_n, \dots\}$ and dimension m , CD is defined as

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

The $C_m(r)$ is the correlation integral, which can be calculated as

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

The $\theta(\omega)$ acts as a step function, where $\theta(\omega) = 0$ for $\omega \leq 0$ and $\theta(\omega) = 1$ for $\omega > 0$. The ζ is the time delay, and is typically set to 1. Sequence $\{\bar{s}_1, \bar{s}_2, \dots, \bar{s}_n, \dots\}$ is a new sequence:

$$\begin{aligned} \bar{s}_t &= (s_t, s_{t+\zeta}, s_{t+2\zeta}, \dots, s_{t+(m-1)\zeta}), \\ t &= 1, 2, \dots, N - (m-1)\zeta. \end{aligned}$$

Fig. 8 shows the CDs of the 2D-LF, 2D-LS, and 2D-FS maps along with those of the existing maps. The parameter settings for all chaotic maps were the same as those used in the SE experiments. The experimental results showed that the 2D-LF, 2D-LS, and 2D-FS maps have positive CDs within all parameter ranges. However, the Hénon, Duffing, and Zeraoulia-Sprott maps only have positive CDs within a few parameter values. In addition, the CDs of these new 2D chaotic maps are much larger than those of the existing ones.

Fig. 9 shows the CDs of the chaotic signal $X = \{x_i | i = 1, 2, \dots\}$ in the 3D-LFS map. We plot only their CDs with two control parameters and set the third parameter as a fixed value to clearly demonstrate the experimental effect. The 3D-LFS map achieves positive CDs for all parameter values. This also indicates that the 3D-LFS can achieve stable and robust chaotic behavior.

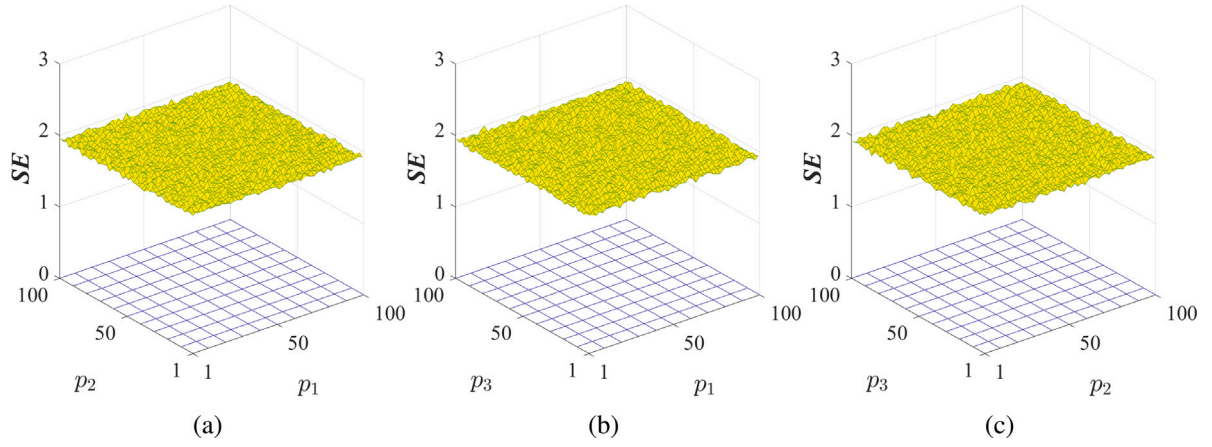


Fig. 7. SEs of the 3D-LFS map in the parameter space of two control parameters by setting the other parameter as a fixed value of 50. (a) $p_1, p_2 \in [1, 100]$ and $p_3 = 50$; (b) $p_1, p_3 \in [1, 100]$ and $p_2 = 50$; (c) $p_2, p_3 \in [1, 100]$ and $p_1 = 50$.

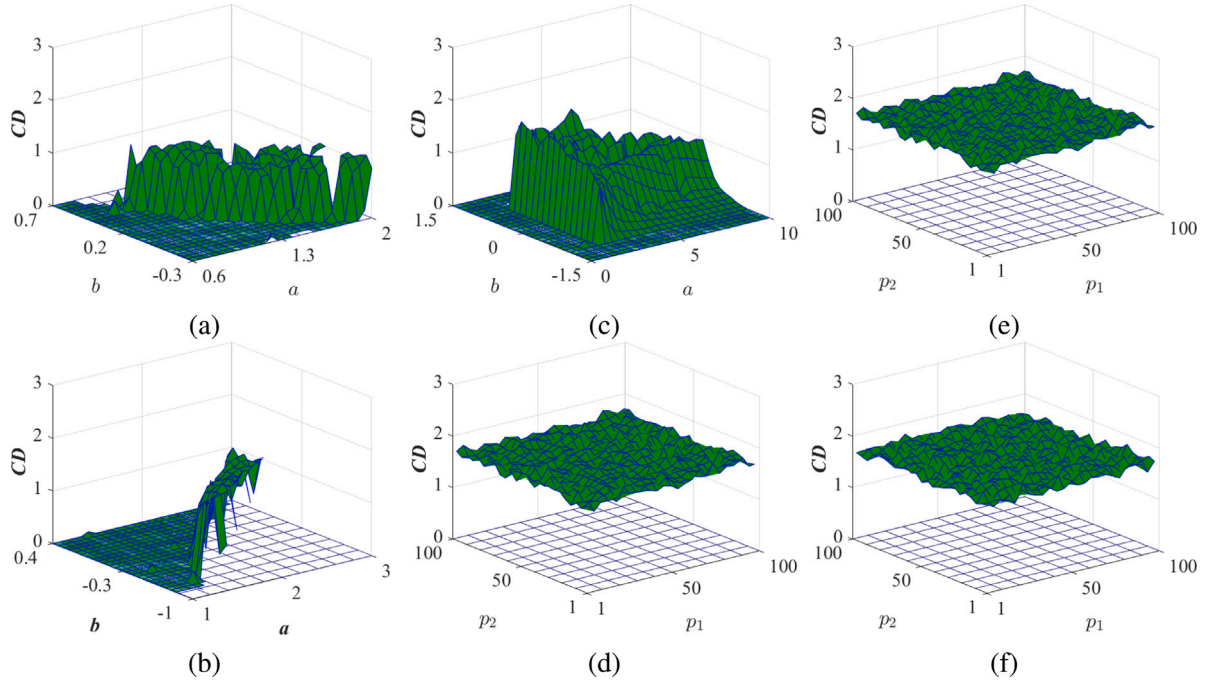


Fig. 8. CDs for different 2D chaotic maps along the change of their parameter values. (a) Hénon map; (b) Duffing map; (c) Zeraoulia-Sprott map; (d) 2D-LF map; (e) 2D-LS map; (f) 2D-FS map.

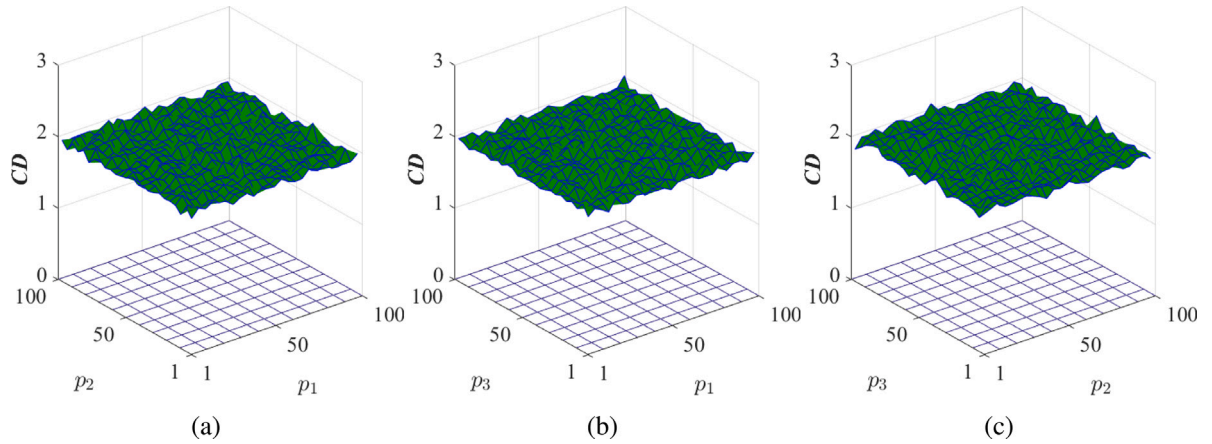


Fig. 9. CDs of the 3D-LFS map in the parameter space of two control parameters by setting the other parameter as a fixed value of 50. (a) $p_1, p_2 \in [1, 100]$ and $p_3 = 50$; (b) $p_1, p_3 \in [1, 100]$ and $p_2 = 50$; (c) $p_2, p_3 \in [1, 100]$ and $p_1 = 50$.

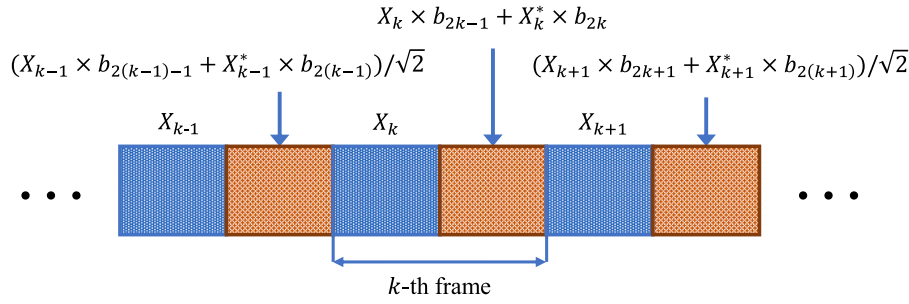


Fig. 10. Transmitted signal structure.

5. Application to secure communication

Because chaotic systems exhibit unpredictability, ergodicity, and many other properties, they have been widely applied to secure communication [47,48], where the chaotic behavior highly determines the performance of secure communication in resisting transmission noise. Because of the complex chaotic behaviors, the maps produced by the n D-CM are suitable candidates for secure communication. This section applies these new chaotic maps to a previously developed DCSK [49] and compares their ability to resist transmission noise with existing ones.

5.1. Structure of the proposed DCSK

This section introduces the scheme of secure communication, which contains two main parts: transmitter and receiver.

5.1.1. Structure of transmitter

The transmitter generates a transmitted signal by coding the data to be transmitted and the chaotic signal. The structure of the transmitted signal is depicted in Fig. 10, and one of each frame contains two parts: reference and information-embedding signals. The reference signal is an M -length chaotic sequence. The information-embedding signal comprises two parts. The first is the multiplication of the reference signal X with the first data bit, and the other is multiplication of the modified signal X^* with the second data bit. X^* is generated by initializing the values in the odd positions of X using opposite numbers and then exchanging the adjacent values. The generation of the modified signal X^* in each frame is expressed as

$$\begin{cases} X_{2i-1}^* = X_{2i} \\ X_{2i}^* = -X_{2i-1}, \end{cases} \quad i \in \{1, 2, \dots, \frac{M}{2}\} \quad (11)$$

The transmitted signal can embed two data bits within one frame, and the communication scheme can achieve a double transmission rate compared with the original DCSK. Fig. 11 illustrates this transmitter. Each frame can embed two data bits. The first data bit is modulated with the reference signal X , whereas the second data bit is modulated by the modified signal X^* . Because the transmitted data frame is of length $2M$, a time delay of M occurs when producing a transmitted frame. When the two data bits to be transmitted are b_1 and b_2 and the reference signal $X = \{x_i | i = 1, 2, \dots, M\}$, a frame S in the transmitted signal is generated as

$$S = \begin{cases} x_i, & \text{if } 1 < i \leq M; \\ (b_1 x_{i-M} + b_2 x_{i-M+1})/\sqrt{2}, & \text{if } M < i \leq 2M \cap \\ & i = 2n + 1 \ (n \in \mathbb{N}); \\ (b_1 x_{i-M} - b_2 x_{i-M+1})/\sqrt{2}, & \text{if } M < i \leq 2M \cap \\ & i = 2n \ (n \in \mathbb{N}) \end{cases} \quad (12)$$

5.1.2. Structure of receiver

The receiver decodes the data bits when a transmitted signal is received. Each frame has two data bits, so the receiver has two branches to recover them separately. The first data bit is recovered by multiplying the information-embedding signal by the reference signal X . The second data bit is recovered by multiplying the information-embedding signal by the modified reference signal X^* . Fig. 12 shows the receiver structure. It can be seen that r represents the received signal, and signal r' is generated from r .

$$\begin{cases} r'_{2i-1} = r_{2i} \\ r'_{2i} = -r_{2i-1}, \end{cases} \quad i \in \{1, 2, \dots, \frac{M}{2}\} \quad (13)$$

The two correlators for decoding the two embedding data bits in the k th frame can be described as

$$Z_{2k-1} = \sum_{i=2kM+1}^{2kM+M/2} r_i r'_{i-M} \quad (14)$$

and

$$Z_{2k} = \sum_{i=2kM+1}^{2kM+M/2} r_i r'_{i-M} \quad (15)$$

When transmitting signals in noisy channels, the signals may be blurred by different types of noise. Suppose that $r = S + \xi$, where ξ indicates the added noise. The correlator of the first data bit within the k th frame is calculated as

$$\begin{aligned} Z_{2k-1} &= \sum_{i=2kM-M+1}^{2kM} (s_i + \xi_i)(s_{i-M} + \xi_{i-M}) \\ &= \sum_{i=(k-1)M+1}^{(k-1)M+M/2} (x_{2i} + \xi_{2i}) \left(\frac{b_{2k-1} x_{2i-1}}{\sqrt{2}} - \frac{b_{2k} x_{2i-1}}{\sqrt{2}} + \xi_{2i+M} \right) \\ &\quad + (x_{2i-1} + \xi_{2i-1}) \left(\frac{b_{2k-1} x_{2i}}{\sqrt{2}} + \frac{b_{2k} x_{2i}}{\sqrt{2}} + \xi_{2i+M-1} \right) \\ &= \frac{b_{2k-1}}{\sqrt{2}} \sum_{i=2(k-1)M+1}^{2(k-1)M+M} (x_i^2) + \gamma, \end{aligned} \quad (16)$$

where γ includes the noise. The correlator of the second data bit within the k th frame is

$$\begin{aligned} Z_{2k} &= \sum_{i=2kM-M+1}^{2kM} (s_i + \xi_i)(s'_{i-M} + \xi'_{i-M}) \\ &= \sum_{i=(k-1)M+1}^{(k-1)M+M/2} (x_{2i} + \xi_{2i}) \left(\frac{b_{2k-1} x_{2i-1}}{\sqrt{2}} + \frac{b_{2k} x_{2i}}{\sqrt{2}} + \xi_{2i+M-1} \right) \\ &\quad - (x_{2i-1} + \xi_{2i-1}) \left(\frac{b_{2k-1} x_{2i}}{\sqrt{2}} - \frac{b_{2k} x_{2i-1}}{\sqrt{2}} + \xi_{2i+M} \right) \\ &= \frac{b_{2k}}{\sqrt{2}} \sum_{i=2(k-1)M+1}^{2(k-1)M+M} (x_i^2) + \eta, \end{aligned} \quad (17)$$

where η includes the noise. The first parts in Eqs. (16) and (17) are signal components, and the remaining are noise components. This is because the energies of the signal components are significantly larger than those of the noise components. The signal components determine

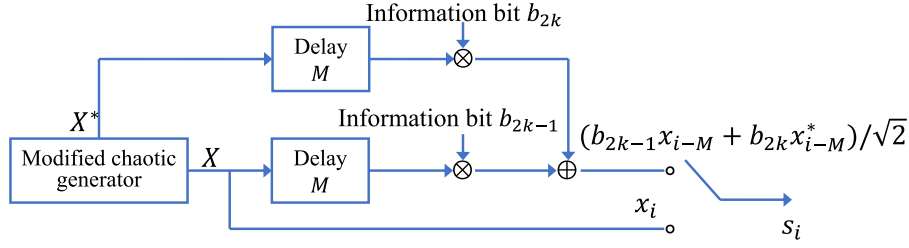


Fig. 11. Structure of the transmitter.

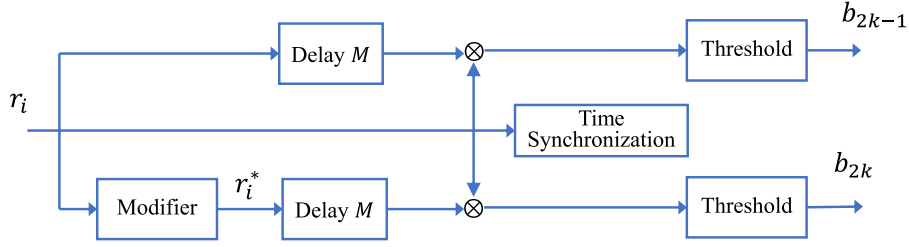
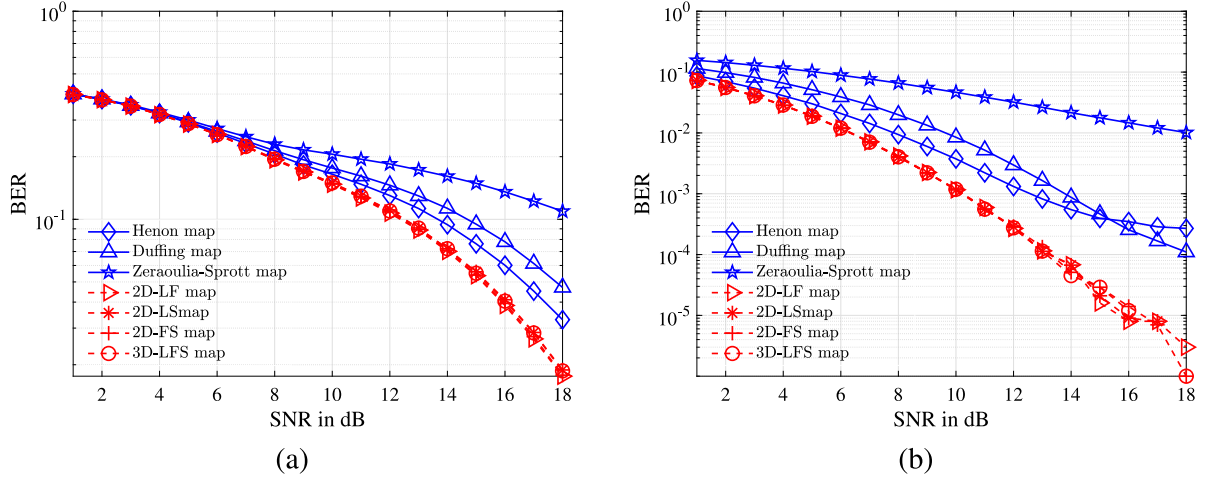
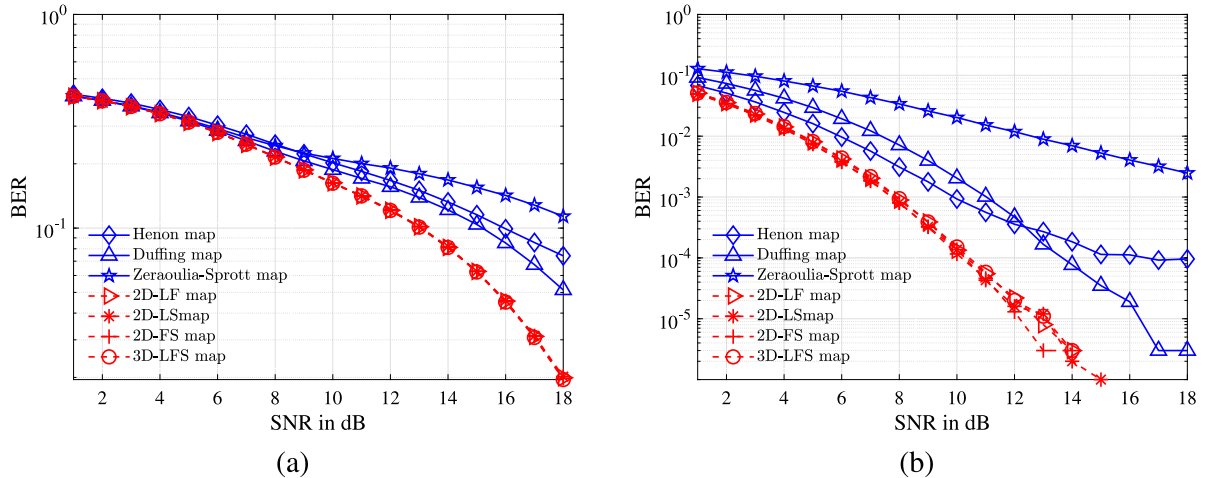


Fig. 12. Structure of receiver.

Fig. 13. BERs of the proposed DCSK using various chaotic maps when simulating in the (a) ARN transmission channel and (b) AWGN transmission channel (the bottom figure) for the signal noise rate $SNR \in [0, 18]$ and spread factor $M = 40$.Fig. 14. BERs of the proposed DCSK using various chaotic maps when simulating in the (a) ARN transmission channel and (b) AWGN transmission channel for the signal noise rate $SNR \in [0, 18]$ and spread factor $M = 60$.

the signs of Eqs. (16) and (17). Thus, despite the noise components, we can decode the two data bits according to the signs of the correlators.

$$b_{2k-1} = \begin{cases} 1, & \text{for } Z_{2k-1} > 0; \\ 0, & \text{for } Z_{2k-1} < 0. \end{cases} \quad (18)$$

$$b_{2k} = \begin{cases} 1, & \text{for } Z_{2k} > 0; \\ 0, & \text{for } Z_{2k} < 0. \end{cases} \quad (19)$$

5.2. Simulation results

The two most contained transition noises in the transmission channels are the additional random noise (ARN) and additive white Gaussian noise (AWGN). This section simulates the proposed DCSK under transmission channels with ARN and AWGN. The three 2D and one 3D chaotic maps produced by the n D-CM and the existing Hénon, Zeraoulia–Sprott, and Duffing maps were used separately as the source chaotic map. We tested the bit error rates (BERs) between the recovered and the original data bits under different chaotic maps.

The experiments were performed in the following steps: (1) Randomly produce a set of initial states, in which all the control parameters fall into the chaotic ranges. (2) Simulate the proposed DCSK by utilizing the chaotic sequences of the chaotic map and setting the spread factor M to 40 and 60, respectively. (3) Randomly generate the transmitted data as a 100000-bit binary sequence and calculate the BERs under different signal noise ratios (SNR). (4) The experiment was repeated ten times to calculate the average BERs.

Fig. 13 displays the BERs for the proposed DCSK when utilizing various chaotic maps as the source chaotic map under different SNRs and setting the spread factor $M = 40$. Fig. 14 shows the average BERs by setting the spread factor $M = 60$. When using the 2D and 3D chaotic maps generated by our n D-CM as the source chaotic map, the proposed DCSK can achieve much smaller average BERs than when using the existing maps as the source chaotic map; this is because the 2D-LF, 2D-LS, 2D-FS and 3D-LFS maps produced by the n D-CM have complex chaotic behaviors. Thus, their generated chaotic sequences are distribute more uniformly than in these existing maps. Therefore, the proposed n D-CM can produce new chaotic maps more suitable for secure communication.

6. Conclusion

This paper proposes an n -dimensional chaotic model (n D-CM) to overcome the drawbacks of the existing chaotic maps comprising discontinuous chaotic ranges and small performance indicators. Using 1D chaotic maps as seed chaotic maps, n D-CM can produce many new chaotic maps with any dimension. Three 2D and one 3D chaotic map were generated using three 1D chaotic maps as seed chaotic maps to show the effect of n D-CM. The performance analysis shows that the newly produced chaotic maps have more extensive and continuous chaotic ranges than existing ones. These chaotic maps were applied to secure communication to demonstrate the practicality of n D-CM. The simulation results indicate that these maps show a stronger ability to resist transition noise than the existing maps.

CRediT authorship contribution statement

Weijia Cao: Writing – original draft, Methodology, Conceptualization. **Hang Cai:** Data curation, Methodology, Conceptualization. **Zhongyun Hua:** Writing – review & editing, Supervision, Project administration, Funding acquisition, Conceptualization.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Acknowledgments

This work was supported in part by the National Key R&D Program of China under Grant 2020YFE0200700, the National Natural Science Foundation of China under Grant 62071142, the Guangdong Basic and Applied Basic Research Foundation, China under Grant 2021A1515011406, and the Shenzhen College Stability Support Plan, China under Grant GXWD20201230155427003-20200824210638001.

References

- [1] Vaidyanathan S, Volos C. Advances and applications in chaotic systems. Berlin, Heidelberg, Germany: Springer; 2016.
- [2] Peng Y, He S, Sun K. A higher dimensional chaotic map with discrete memristor. AEU-Int J Electron Commun 2021;129:153539.
- [3] Chen S, Yu S, Lü J, Chen G, He J. Design and FPGA-based, realization of a chaotic secure video communication system. IEEE Trans Circuits Syst Video Technol 2018;28(9):2359–71.
- [4] Wu S, Li Y, Li W, Li L. Chaos criteria design based on modified sign functions with one or three-threshold. Chin J Electron 2019;28(2):364–9.
- [5] Devaney RL. An introduction to chaotic dynamical systems. second ed.. Boulder, Colorado: Westview Press; 2018.
- [6] Hua Z, Zhu Z, Chen Y, Li Y. Color image encryption using orthogonal latin squares and a new 2D chaotic system. Nonlinear Dynam 2021;104(4):4505–22.
- [7] Zhang Y. A chaotic system based image encryption scheme with identical encryption and decryption algorithm. Chin J Electron 2017;26(5):1022–31.
- [8] Li X, Zhou L, Tan F. An image encryption scheme based on finite-time cluster synchronization of two-layer complex dynamic networks. Soft Comput 2022;26(2):511–25.
- [9] Hua Z, Li J, Chen Y, Yi S. Design and application of an S-box using complete latin square. Nonlinear Dynam 2021;104(1):807–25.
- [10] Chen S, Yu S, Lü J, Chen G, He J. Design and FPGA-based realization of a chaotic secure video communication system. IEEE Trans Circuits Syst Video Technol 2018;28(9):2359–71.
- [11] Zhou L, Tan F, Li X, Zhou L. A fixed-time synchronization-based secure communication scheme for two-layer hybrid coupled networks. Neurocomputing 2021;433:131–41.
- [12] Ma Y, Li C, Ou B. Cryptanalysis of an image block encryption algorithm based on chaotic maps. J Inf Secur Appl 2020;54:102566.
- [13] Herceg M, Kaddoum G, Vranješ D, Soujeri E. Permutation index DCSK modulation technique for secure multiuser high-data-rate communication systems. IEEE Trans Veh Technol 2018;67(4):2997–3011.
- [14] Bakiri M, Couchot J, Guyeux C. Ciprng: A VLSI family of chaotic iterations post-processings for \mathbb{F}_2 , -linear pseudorandom number generation based on zynq MPSoC. IEEE Trans Circuits Syst I Regul Pap 2018;65(5):1628–41.
- [15] Liu M, Zhang S, Fan Z, Qiu M. H_∞ state estimation for discrete-time chaotic systems based on a unified model. IEEE Trans Syst Man Cybern B: Cybernetics 2012;42(4):1053–63.
- [16] Bo Yang XL. Some characteristics of logistic map over the finite field. Sci. China Inf. Sci. 2019;62(3):039104.
- [17] Hua Z, Chen Y, Bao H, Zhou Y. Two-dimensional parametric polynomial chaotic system. IEEE Trans Syst Man Cybern 2022;52(7):4402–14.
- [18] Li C, Feng B, Li S, Kurths J, Chen G. Dynamic analysis of digital chaotic maps via state-mapping networks. IEEE Trans Circuits Syst I Regul Pap 2019;66(6):2322–35.
- [19] Aybar OO, Aybar IK, Hacinliyan A. Stability and bifurcation in the hénon map and its generalizations. Chaotic Model Simul (CMSIM) 2013;4:529–38.
- [20] Chen L, Li C, Li C. Security measurement of a medical image communication scheme based on chaos and DNA coding. J Vis Commun Image Represent 2022;83:103424.
- [21] Zhang R, Yang S. Robust chaos synchronization of fractional-order chaotic systems with unknown parameters and uncertain perturbations. Nonlinear Dynam 2012;69(3):983–92.
- [22] Zhang Y, Bai S, Lu G, Wu X. Kernel estimation of truncated Volterra filter model based on ddp technique and its application to chaotic time series prediction. Chin J Electron 2019;28(1):127–35.
- [23] Xiao Z, Shan S, Cheng L. Identification of cascade dynamic nonlinear systems: A bargaining-game-theory-based approach. IEEE Trans Signal Process 2018;66(17):4657–69.
- [24] Zhang X, Xu J. An extended synchronization method to identify slowly time-varying parameters in nonlinear systems. IEEE Trans Signal Process 2018;66(2):438–48.

- [25] Xu M, Chen G, Tian Y-T. Identifying chaotic systems using Wiener and Hammerstein cascade models. *Math Comput Modelling* 2001;33(4–5):483–93.
- [26] Yeh J-P. Identifying chaotic systems using a fuzzy model coupled with a linear plant. *Chaos Solitons Fractals* 2007;32(3):1178–87.
- [27] Lazzús JA, Rivera M, López-Caraballo CH. Parameter estimation of Lorenz chaotic system using a hybrid swarm intelligence algorithm. *Phys Lett A* 2016;380(11):1164–71.
- [28] Lin L, Shen M, So HC, Chang C. Convergence analysis for initial condition estimation in coupled map lattice systems. *IEEE Trans Signal Process* 2012;60(8):4426–32.
- [29] Liu M, Zhang S, Fan Z, Zheng S, Sheng W. Exponential H_{∞} synchronization and state estimation for chaotic systems via a unified model. *IEEE Trans Neural Netw Learn Syst* 2013;24(7):1114–26.
- [30] Li J, Zhang Q, Zhang Y, Wu X, Wang X, Su Y. Hidden phase space reconstruction: A novel chaotic time series prediction method for speech signals. *Chin J Electron* 2018;27(6):1221–8.
- [31] Ergün S. On the security of chaos based “true” random number generators. *IEICE Trans Fundam Electron Commun Comput Sci* 2016;99(1):363–9.
- [32] Li C, Tan K, Feng B, Lü J. The graph structure of the generalized discrete Arnold’s Cat map. *IEEE Trans Comput* 2022;71(2):364–77.
- [33] Liu S, Li C, Hu Q. Cryptanalyzing two image encryption algorithms based on a first-order time-delay system. *IEEE MultiMedia* 2022;29:74–84.
- [34] Hua Z, Zhang Y, Bao H, Huang H, Zhou Y. N-dimensional polynomial chaotic system with applications. *IEEE Trans Circuits Syst I Regul Pap* 2021;69(2):784–97.
- [35] Zhang Y, Hua Z, Bao H, Huang H, Zhou Y. An n-dimensional chaotic system generation method using parametric pascal matrix. *IEEE Trans Ind Inf* 2022;1.
- [36] Zheng J, Hu H, Xia X. Applications of symbolic dynamics in counteracting the dynamical degradation of digital chaos. *Nonlinear Dynam* 2018;94(2):1535–46.
- [37] Liu L, Liu B, Hu H, Miao S. Reducing the dynamical degradation by bi-coupling digital chaotic maps. *Int J Bifurcation Chaos* 2018;28(05):1850059.
- [38] Li S, Chen G, Mou X. On the dynamical degradation of digital piecewise linear chaotic maps. *Int J Bifurcation Chaos* 2005;15(10):3119–51.
- [39] Zhou Y, Bao L, Chen CP. A new 1D, chaotic system for image encryption. *Signal Process* 2014;97:172–82.
- [40] Hua Z, Jin F, Xu B, Huang H. 2D logistic-Sine-coupling map for image encryption. *Signal Process* 2018;149:148–61.
- [41] Shen C, Yu S, Lü J, Chen G. Designing hyperchaotic systems with any desired number of positive Lyapunov exponents via a simple model. *IEEE Trans Circuits Syst I Regul Pap* 2014;61(8):2380–9.
- [42] Lu J-a, Wu X, Lü J, Kang L. A new discrete chaotic system with rational fraction and its dynamical behaviors. *Chaos Solitons Fractals* 2004;22(2):311–9.
- [43] Wolf A, Swift JB, Swinney HL, Vastano JA. Determining Lyapunov exponents from a time series. *Physica D* 1985;16(3):285–317.
- [44] Richman JS, Moorman JR. Physiological time-series analysis using approximate entropy and sample entropy. *Am J Physiol-Heart Circulatory Physiol* 2000;278(6):H2039–49.
- [45] Cantrell CD. Modern mathematical methods for physicists and engineers. Cambridge University Press; 2000.
- [46] Lacasa L, Gómez-Gardeñes J. Correlation dimension of complex networks. *Phys Rev Lett* 2013;110:168703.
- [47] Lin Z, Yu S, Lü J, Cai S, Chen G. Design and ARM-embedded implementation of a chaotic map-based real-time secure video communication system. *IEEE Trans Circuits Syst Video Technol* 2015;25(7):1203–16.
- [48] Chou HG, Chuang CF, Wang WJ, Lin JC. A fuzzy-model-based chaotic synchronization and its implementation on a secure communication system. *IEEE Trans Inf Forensics Security* 2013;8(12):2177–85.
- [49] Cai H, Hua Z, Huang H. A novel differential-chaos-shift-keying secure communication scheme. In: 2018 IEEE international conference on systems, man, and cybernetics (SMC). IEEE; 2018, p. 1794–8.