A novel method of constructing high-dimensional digital chaotic systems on finite-state automata[*]

Jun Zheng(郑俊)[1] and Han-Ping Hu(胡汉平)[1,2,†]

[1] *School of Artificial Intelligence and Automation, Huazhong University of Science and Technology, Wuhan* 430074, *China*
[2] *Key Laboratory of Image Information Processing and Intelligent Control, Ministry of Education, Wuhan* 430074, *China*

(Received 18 May 2020; revised manuscript received 7 July 2020; accepted manuscript online 15 July 2020)

When chaotic systems are implemented on finite precision machines, it will lead to the problem of dynamical degradation. Aiming at this problem, most previous related works have been proposed to improve the dynamical degradation of low-dimensional chaotic maps. This paper presents a novel method to construct high-dimensional digital chaotic systems in the domain of finite computing precision. The model is proposed by coupling a high-dimensional digital system with a continuous chaotic system. A rigorous proof is given that the controlled digital system is chaotic in the sense of Devaney's definition of chaos. Numerical experimental results for different high-dimensional digital systems indicate that the proposed method can overcome the degradation problem and construct high-dimensional digital chaos with complicated dynamical properties. Based on the construction method, a kind of pseudorandom number generator (PRNG) is also proposed as an application.

Keywords: high-dimensional digital chaotic system, dynamical degradation, anti-control, pseudorandom number generator

PACS: 05.40.−a, 05.45.Gg, 05.45.Jn, 05.45.Vx **DOI:** 10.1088/1674-1056/aba60f

1. Introduction

Chaos has aroused wide concerns because of its simple structure and complex dynamical properties, such as sensitivity to initial conditions, inner randomness in the definitive systems, aperiodicity, and unpredictability.[1,2] Such properties exactly meet the requirements of cryptography,[3,4] so chaotic systems have been widely used in many different secure encryption systems,[5–8] including digital ciphers, pseudorandom number generator (PRNG), and so on. However, when chaotic systems are implemented on digital devices with finite computing precisions, they cannot preserve the desired dynamics and degrade of varying degrees.[9] This phenomenon is called dynamical degradation, which may cause serious flaws in chaos-based applications.[10,11]

Focusing on this problem, multiple remedies have been proposed to enhance chaotic systems and reduce the dynamical degradation, such as perturbing method (perturbation of chaotic states or control parameters),[12–14] integrating multiple chaotic systems (including cascading and switching methods),[15–17] or error compensation method.[18] Recently, Tutueva *et al.* proposed a novel concept of chaotic maps with adaptive symmetry[19] and a two-parameter modified logistic map technique,[20] which both increase the length of chaotic orbits through introducing new parameters. These methods perform well, however, they are lack of a systematic theory to analyze the dynamical degradation. Since 2010, Bahi *et al.* constructed digital chaotic systems designated as chaotic iterations systems via introducing random streams.[21–23] They showed that the constructed systems satisfied Devaney's definition of chaos. Alawida *et al.* proposed deterministic chaotic finite-state automata for enhancing the existing chaotic maps[24] and generating new chaotic maps.[25] Hu *et al.* constructed digital chaotic systems via hybrid control without random entropy sources added, which were rigorously proven to be chaotic.[26] However, the researches of directly constructing chaos on finite state automata develop slowly. In addition, compared with low-dimensional chaotic systems, higher-dimensional chaotic systems have more complex dynamical behaviors, which are usually used to resist the dynamical degradation of chaotic systems.[27,28] As a result, the problem of their own degradation is always neglected, which may cause serious hidden troubles.

In this paper, the problem of constructing high-dimensional digital chaotic systems (HDDCS) in digital devices with finite precision is studied. We establish the general framework of constructing HDDCS by introducing a continuous chaotic system, which owns infinite phase space and ergodicity of orbit. The continuous chaotic system, which still has infinite sequence space even under the influence of quantization function, is used to control the high-dimensional digital system (HDDS). Therefore, the periodic orbits of the constructed HDDCS can be extended to infinity. Then we prove that the controlled HDDS satisfies Devaney's definition

[*] Project supported by the National Key R&D Program of China (Grant No. 2017YFB0802000) and the Cryptography Theoretical Research of National Cryptography Development Fund, China (Grant No. MMJJ20170109).

[†] Corresponding author. E-mail: husthhh@qq.com

of chaos in mathematics, which means the constructed HDDCS can overcome the problem of dynamical degradation. In the simulation experiments, 2-dimensional linear map, nonlinear Henon map, and 4-dimensional linear map under finite precisions are taken as examples for constructing digital chaotic systems. The experiment results demonstrate the effectiveness of our method. Finally, a PRNG based on the constructed digital chaotic system is proposed as a simple application of our method. The main contributions of this paper are listed as follows:

1. The constructed digital chaotic systems can be verified by Devaney's definition, which makes the actual performances of this method generally convincing.

2. This method can be used to construct digital chaotic systems with any dimension.

3. Even for the simplest high-dimensional linear systems, we can construct HDDCS. Therefore, much more HDDCS can be constructed effortlessly via our method.

The remaining parts of this paper are organized as follows. The description of our model is given in Section 2, followed by the theoretical proof that the controlled digital system is chaotic in Section 3. The experimental examples are presented in Section 4 to show the validity of the method. In Section 5, a new kind of PRNG based on the constructed HDDCS is proposed. Conclusion remarks follow in Section 6.

2. Description of the model

In this model, a continuous chaotic system is used to generate sampled output sequences to anti-control the HDDS based on the external feedback anti-control theory, and construct high-dimensional chaos on the finite-state automata.

The continuous chaotic system can be described as

$$\begin{aligned} &\dot{Y}(t) = F(Y(t)) = AY(t) + \varphi(Y(t)), \\ &Y(0) = Y_0, \end{aligned} \tag{1}$$

where $Y(t) = [y^1(t), y^2(t), \dots y^n(t)]^{\mathrm{T}} \in \Omega \subset R^n$ is an n-dimensional state vector, Ω is basin of attraction, $A \in R^{n\times n}$ is a constant matrix, φ is a function representing the nonlinear part.

An l-dimensional digital system can be described as

$$x_{i+1} = f_P(x_i) \to \begin{cases} x^1_{i+1} = f^1_P(x^1_i, x^2_i, \dots, x^l_i), \\ x^2_{i+1} = f^2_P(x^1_i, x^2_i, \dots, x^l_i), \\ \vdots \\ x^l_{i+1} = f^l_P(x^1_i, x^2_i, \dots, x^l_i), \end{cases} \tag{2}$$

where $x_i \in \Phi_P$ is the state vector and Φ_P is the finite version of real set Φ under the influence of quantization function, P is the computing precision, and f_P is the iterative function, which is the composition of f and the quantization function.

The control problem is studied that the HDDS Eq. (2) is controlled by the continuous chaotic system. In order to make the controlled digital system behave chaotically with desirable dynamical properties, we design a control term $u(Y(t_i))$. The controlled digital system can be written as

$$x_{i+1} = f_P(x_i) + G_P(u(Y(t_i))), \tag{3}$$

where $G_P : \Omega \to \Omega_P$ is a quantization function, $u(Y(t_i)) = B \cdot Y(t_i)$, and $B \in R^{l\times n}$ is the control gain matrix. Here we only consider the linear state controller to anti-control the digital system.

Since the control term can make orbits of the controlled system diffuse outside owing to the chaotic properties of the external continuous chaotic system. In addition, a modular function should be used to confine the orbit of the controlled digital system. Then the controlled digital system can be described as

$$x_{i+1} = h_P(x_i, Y(t_i)) = (f_P(x_i) + G_p(B \cdot Y(t_i))) \bmod \alpha, \tag{4}$$

where α is a constant.

3. Devaney's chaos of the controlled high-dimensional digital systems

In this section, we prove that the controlled HDDS satisfies Devaney's definition of chaos.[29]

The state space of the digital system is Φ_P. With the state feedback control of the continuous chaotic system, Cartesian product is applied to describe the state space of the control sequences and the state space of the digital system. Consider the new state space of the controlled digital system $\Psi : \Phi_P \times \Omega$, and the map H_{h_P} defined on Ψ,

$$(x_{i+1}, Y(t_{i+1})) = H_{h_P}(x_i, Y(t_i)) = (h_P(x_i, Y(t_i)), Y(t_i)).$$

For continuous chaos, two assumptions are given hereinafter.

Assumption 1 The continuous chaotic system is ergodic in the chaotic basins of attraction. Namely, for $\forall \hat{Y} \in \Omega$, $\exists t$ such that $Y(t, Y_0) = \hat{Y}$, where $Y(t, Y_0)$ is the trajectory of the continuous chaotic system, and $Y_0 \in \Omega$ is the initial state.

Assumption 2 The output state $Y(t_i)$ of the continuous chaotic system is random-like.

The aforementioned assumptions are reasonable because of chaotic properties. According to Assumptions 1 and 2, the control sequences $u(Y(t_i))$ also are random-like, then all the states in the phase space of the digital system can be achieved via the state feedback control. Thus, we can assume that the controlled digital system on finite field is ergodic.

Assumption 3 The controlled digital system h_P is ergodic in a bounded region.

Before proving that h_P satisfies Devaney's definition of chaos, we prove some theorems in advance.

Theorem 1 The map h_P is non-periodic.

Proof Assuming that there exists N such that when $n \geqslant N$, the map h_P is periodic and the period is T, i.e., $x_n = x_{n+T}$,

$n \geqslant N$. The map F is non-periodic in the chaotic basins of attraction, then $Y(t_n) \neq Y(t_{n+T})$, $n \geqslant N$ can be obtained. So the control sequence $u(Y(t_i))$ cannot be the same all the time. $h_P(x_n, u(Y(t_n))) \neq h_P(x_{n+T}, u(Y(t_{n+T})))$ can be obtained, which is a contradiction. This concludes the proof of the theorem.

Note that the map h_P is non-periodic, inspired by symbolic dynamic systems in which the state of such system can be expressed as an infinite sequence of finite symbols, we consider the state space of the symbolic dynamic system generated with the controlled digital system. The state space can be generated in the following form:

$$Z_i = [x_i, x_{i+1}, \ldots, x_{i+(m-1)}]^{\mathrm{T}} \in \mathit{\Pi}, \ \ i = 0, 1, \ldots, \ \ m \to +\infty,$$

where $\mathit{\Pi}$ is the new state space.

Thus, we establish a bijection between the state space $\mathit{\Pi}$ and the state space of the controlled digital system.

Define H: $Z_i \to Z_{i+1}, Z_i \in \mathit{\Pi}$, and the distance d in $\mathit{\Pi}$: $d(Z_i, Z_j) = \sum_{k=0}^{m-1} \frac{\|x_{i+k} - x_{j+k}\|}{2^k}$, where $\|\cdot\|$ denotes the Euclidean norm. Then, there exists a continuous map $\phi : \mathit{\Psi} = \mathit{\Phi}_P \times \mathit{\Omega} \to \mathit{\Pi}$, which satisfies $\phi \circ H_{h_P} = H \circ \phi$. According to the definition above,

$$\begin{tikzcd}
\mathit{\Psi} \arrow[r, "H_{h_P}"] \arrow[d, "\phi"] & \mathit{\Psi} \arrow[d, "\phi"] \\
\mathit{\Pi} \arrow[r, "H"] & \mathit{\Pi}
\end{tikzcd}$$

so, we construct a map H which is equivalent with H_{h_P}.

Theorem 2 The map H is continuous.

Proof This problems is equivalent to proving that $\forall \varepsilon > 0$, $\exists \delta > 0$, if $d\left(Z, \hat{Z}\right) < \delta$, then $d\left(H(Z), H(\hat{Z})\right) < \varepsilon$, where $Z = [x_k, x_{k+1}, \ldots x_{k+(m-1)}]^{\mathrm{T}}$, $\hat{Z} = [x_t, x_{t+1}, \ldots x_{t+(m-1)}]^{\mathrm{T}}$. If $d\left(H(Z), H(\hat{Z})\right) = \sum_{i=1}^{m} \frac{\|x_{k+i} - x_{t+i}\|}{2^i} < \varepsilon$, then

$$\begin{aligned}
& d\left(H(Z), H(\hat{Z})\right) \\
={}& \sum_{i=0}^{m-1} \frac{\|x_{k+i} - x_{t+i}\|}{2^i} + \frac{\|x_{k+m} - x_{t+m}\|}{2^m} - \|x_k - x_t\| \\
={}& d\left(Z, \hat{Z}\right) + \frac{\|x_{k+m} - x_{t+m}\|}{2^m} - \|x_k - x_t\| < \varepsilon,
\end{aligned}$$

which leads to

$$d\left(Z, \hat{Z}\right) < \varepsilon - \frac{\|x_{k+m} - x_{t+m}\|}{2^m} + \|x_k - x_t\|.$$

The digital system is bounded, so we can assume that for $\forall x_{k+i}$, x_{t+i} $\|x_{k+i} - x_{t+i}\| < \theta$, $i = 0, 1, \ldots$ holds. Then choosing $\delta = \varepsilon - \theta/2^m$, we obtain

$$d\left(Z, \hat{Z}\right) < \delta = \varepsilon - \frac{\theta}{2^m} < \varepsilon - \frac{\|x_{k+m} - x_{t+m}\|}{2^m} + \|x_k - x_t\|,$$

so $d\left(H(Z), H(\hat{Z})\right) < \varepsilon$. This concludes the proof of the theorem.

Theorem 3 The periodic points of H are dense in the metric space $(\mathit{\Pi}, d)$.

Proof For $Z = (x_{k+1}, x_{k+2}, \ldots, x_{k+m}) \in \mathit{\Pi}$ and any given $\varepsilon > 0$, we prove that a periodic point $\bar{Z} = (\bar{x}_{t+1}, \bar{x}_{t+2}, \ldots, \bar{x}_{t+m})$ of H in $(\mathit{\Pi}, d)$ can always be found in the neighborhood of distance ε of point Z, i.e., $d(Z, \bar{Z}) < \varepsilon$.

According to the definition of the distance function d, if we want to obtain $d(Z, \bar{Z}) < \varepsilon$, we could find a constant $\omega \in N^*$ and let $\bar{x}_{t+i} = x_{k+i}$, $1 \leqslant i \leqslant \omega$ satisfy the condition, where N^* denotes the set of positive integers.

In order to satisfy

$$\begin{aligned}
d(Z, \bar{Z}) &= \sum_{i=\omega+1}^{m} \frac{\|x_{k+i} - x_{t+i}\|}{2^i} \leqslant \sum_{i=\omega+1}^{m} \frac{\theta}{2^i} \\
&= \frac{\theta}{2^{\omega+1}} \frac{1 - (1/2)^{m-\omega}}{1 - 1/2} \\
&= \frac{\theta}{2^{\omega}} \left(1 - \left(\frac{1}{2}\right)^{m-\omega}\right) < \varepsilon,
\end{aligned}$$

we obtain

$$\frac{2^m \theta}{2^m \varepsilon + \theta} < 2^{\omega}, \quad \log_2 \frac{2^m \theta}{2^m \varepsilon + \theta} < \omega,$$

where $m > 0, \varepsilon > 0, \theta > 0$, and

$$\begin{gathered}
\theta < 2^m \varepsilon + \theta, \quad \theta 2^m < (2^m \varepsilon + \theta) 2^m, \\
\frac{2^m \theta}{2^m \varepsilon + \theta} < 2^m, \quad \log_2 \frac{2^m \theta}{2^m \varepsilon + \theta} < m,
\end{gathered}$$

So the value of ω can be chosen as $\log_2 \frac{2^m \theta}{2^m \varepsilon + \theta} < \omega < m$ which makes $d(Z, \bar{Z}) < \varepsilon$. After the ω iteration, $H^{\omega}(\bar{Z}) = (\bar{x}_{t+\omega+1}, \bar{x}_{t+\omega+2}, \ldots, \bar{x}_{t+\omega+m})$ can be obtained. According to Assumption 3, there exists at least one orbit from $\bar{x}_{t+\omega+1}$ to x_{k+1} by the control sequences S^u, i.e., there exists $u \in N^*$ that makes $h_p^u(\bar{x}_{t+\omega+1}, S^u) = x_{k+1}$, so $h_p^{\omega+u}(\bar{x}_{t+1}, S^{\omega+u}) = x_{k+1}$. Then, by making the control sequence $S = (S^{\omega+u}, S^{\omega+u}, \ldots) = (u(Y(t_{i+1})), u(Y(t_{i+2})), \ldots u(Y(t_{i+\omega+u})), u(Y(t_{i+1})), \ldots)$, this implies that a periodic point is found by checking

$$\begin{aligned}
\bar{Z} &= (\bar{x}_{t+1}, \bar{x}_{t+2}, \ldots, \bar{x}_{t+\omega}, \bar{x}_{t+\omega+1}, \ldots, \bar{x}_{t+\omega+u+1}, \ldots) \\
&= (x_{k+1}, x_{k+2}, \ldots, x_{k+\omega}, \bar{x}_{t+\omega+1}, \ldots x_{k+1}, \ldots), \\
& H^{\omega+u}(\bar{Z}) = (x_{k+1}, x_{k+2}, \ldots).
\end{aligned}$$

Therefore, the point satisfies $d(Z, \bar{Z}) < \varepsilon$ by the discussion above. As a conclusion, the periodic points of H are dense.

Theorem 4 H is topological transitive.

Proof Topological transitivity of function H means that for all open ball $B_A = B(Z_A, r_A) \subset \mathit{\Pi}$ and $B_B = B(Z_B, r_B) \subset \mathit{\Pi}$, where $Z_A = (x_{a+1}, x_{a+2}, \ldots, x_{a+m})$, $Z_B = (x_{b+1}, x_{b+2}, \ldots, x_{b+m})$, r_A, r_B are the sphere radii, there always exists $n_0 \in N^*$ and $\hat{Z} = (\hat{x}_{t+1}, \hat{x}_{t+2}, \ldots, \hat{x}_{t+m}) \in B_A$ satisfying $H^{n_0}(\hat{Z}) \in B_B$.

In order to satisfy $d(Z_A, \hat{Z}) < r_A$, we can choose ω which is the same as Theorem 3, and let $\hat{x}_{t+i} = x_{a+i}, 1 \leqslant i \leqslant \omega$. Next, we also need that the point $\hat{Z}$ satisfies $d(H^{n_0}(\hat{Z}), Z_B) < r_B$. After the n_0 iteration, $H^{n_0}(\hat{Z}) = (\hat{x}_{t+n_0+1}, \hat{x}_{t+n_0+2}, \ldots, \hat{x}_{t+m+n_0})$, we need to find $n_0 \in N^*$ and make $\hat{x}_{t+1+i} = x_{b+i-n_0+1}$, $n_0 \leqslant i \leqslant \hat{\omega}$.

By Assumption 3, h_P is ergodic, so there exists $q \in N^*$ at least, which makes $h_P^q(\hat{x}_{t+\omega+1}, S^q) = x_{b+1}$. Then $n_0 = \omega + q$ is found, and there exists

$$\begin{aligned}\hat{Z} &= (\hat{x}_{t+1}, \hat{x}_{t+2}, \ldots, \hat{x}_{t+\omega}, \hat{x}_{t+\omega+1}, \ldots, \\ &\quad \hat{x}_{t+\omega+q+1}, \ldots, \hat{x}_{t+\omega+q+\hat{\omega}+1}, \ldots), \\ &= (x_{a+1}, x_{a+2}, \ldots, x_{a+\omega}, \hat{x}_{t+\omega+1}, \ldots, x_{b+1}, \ldots, x_{b+\hat{\omega}} \ldots)\end{aligned}$$

which satisfies $\hat{Z} \in B_A$ and after the n_0 iteration,

$$H^{n_0}(\hat{Z}) = (x_{b+1}, x_{b+2}, \ldots, x_{b+\hat{\omega}}, \ldots) \in B_B.$$

In summary, H is transitive in the metric space (Π, d).

Additionally, Banks *et al.* proved that if a dynamical system on a metric space is topological transitive and has dense periodic points,[29] then it has sensitive dependence on the initial conditions.

In conclusion, H is topologically transitive, has dense periodic points and sensitive dependence on the initial conditions. Then we have the following result.

Theorem 5 *H* is chaotic in the sense of Devaney's definition of chaos.

So according to Theorem 5 and the previous discussion, we have proved that h_P is chaotic in the sense of Devaney's definition of chaos.

4. Experimental simulation

In this section, different HDDSs are given to show validity of the proposed method.

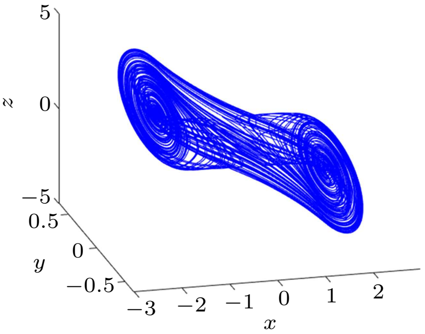


Fig. 1. Chaotic behavior of Chua chaotic system.

Consider Chua chaotic system as the continuous chaotic system, which can be described as

$$\begin{cases} \dot{x}(t) = a(y(t) - x(t) - f(x(t)), \\ \dot{y}(t) = x(t) - y(t) + z(t), \\ \dot{z}(t) = -by(t), \end{cases} \tag{5}$$
$$f(x(t)) = cx(t) + 0.5(d-c) \times (|x(t)+1| - |x(t)-1|),$$

where $Y = (x, y, z)^{\mathrm{T}}$ is the continuous system state vector, and a, b, c, d are the parameters of Chua chaotic system. We choose $a = 10, b = 14.87, c = -0.65, d = -1.27$ in this paper. Remarkably, the continuous chaotic system can be implemented on analog devices. In this paper, the chaotic behavior of Chua chaotic system simulated by Runge–Kutta algorithm is depicted in Fig. 1, which shows a classical double scroll attractor. The simulation results almost have no influence on the proposed method.

4.1. Example 1: 2-dimensional linear map

Consider the following simplest 2-dimensional linear map (2DLM) realized with *P*-bits finite precision

$$(x_{n+1}, y_{n+1}) = F_p(x_n, y_n) \to \begin{cases} x_{n+1} = G_p(k_1 y_n), \\ y_{n+1} = G_p(k_2 x_n), \end{cases} \tag{6}$$

where k_1, k_2 are the constants.

Here Chua chaotic system is applied to anti-control the digital 2-dimensional linear map. Using the control gain matrix $B = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, then the controlled digital 2DLM can be written as

$$\begin{cases} x_{n+1} = G_p(k_1 y_n) + G_p(\lambda x(t)) \bmod \alpha, \\ y_{n+1} = G_p(k_2 x_n), \end{cases} \tag{7}$$

where α, λ are the constants, and $x(t)$ is the x-dimensional state variable of Chua chaotic system.

Next, we analysis some characteristics to show the effectiveness of the method. The largest precision P is set at 2^{-16}. Set $k_1 = 2, k_2 = 0.3, \lambda = 10, \alpha = 1$ and the initial values $(x_0, y_0) = (0.1, 0.1), Y(0) = (0.5, 0, 0)$.

According to Eq. (6), it is easy to figure out that the 2DLM eventually converges to a fixed point. Then we analyze the controlled 2DLM Eq. (7). The simulation results of its dynamical properties are shown in Figs. 2 and 3.

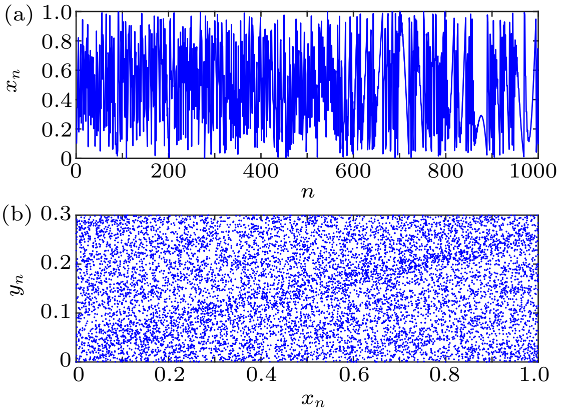


Fig. 2. (a) The trajectory of x-dimensional state of the controlled 2DLM. (b) The phase diagram of the controlled 2DLM.

Figure 2(a) shows the trajectory of the x-dimensional state of the controlled 2DLM. While the y-dimensional state has the same trend as the x-dimensional one due to Eq. (7). The controlled 2DLM has no cycles and behaves chaotically after anti-control. Figure 2(b) plots the phase diagram of the controlled 2DLM, which can achieve ergodicity. Meanwhile, the phase diagram is disrupted completely, which makes the generated sequence appear random. In this way, the obvious function correlation of neighbor points is removed, thus it will enhance the security of the digital chaos-based cryptosystem. Auto-correlation function is an important randomness measure. For an ideal chaotic sequence, the auto-correlation should be a delta-like function. It can be observed from Fig. 3(a) that the auto-correlation function of the controlled 2DLM can be delta-like. As shown in Fig. 3(b), the frequency distribution is smoothed to be homogeneous, which is helpful for some applications such as the secure communication or PRNG.

In addition, we study the dynamical behaviors of the controlled 2DLM with respect to the control parameter λ. We gradually change the control parameter λ, the evolution of the dynamical properties is showed in Figs. 4–8.

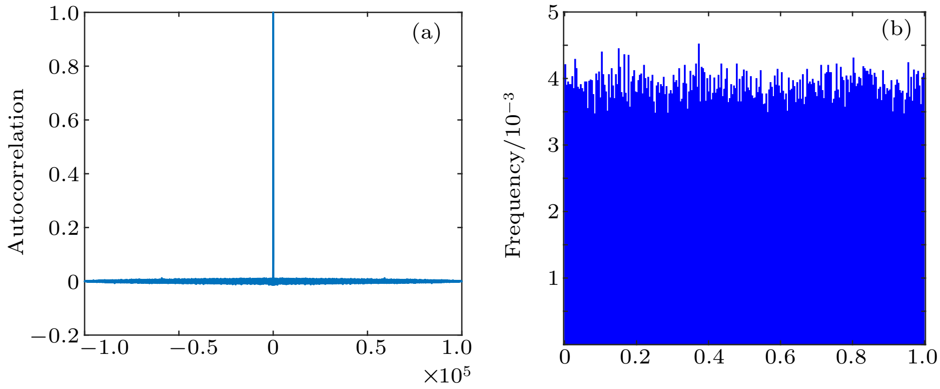
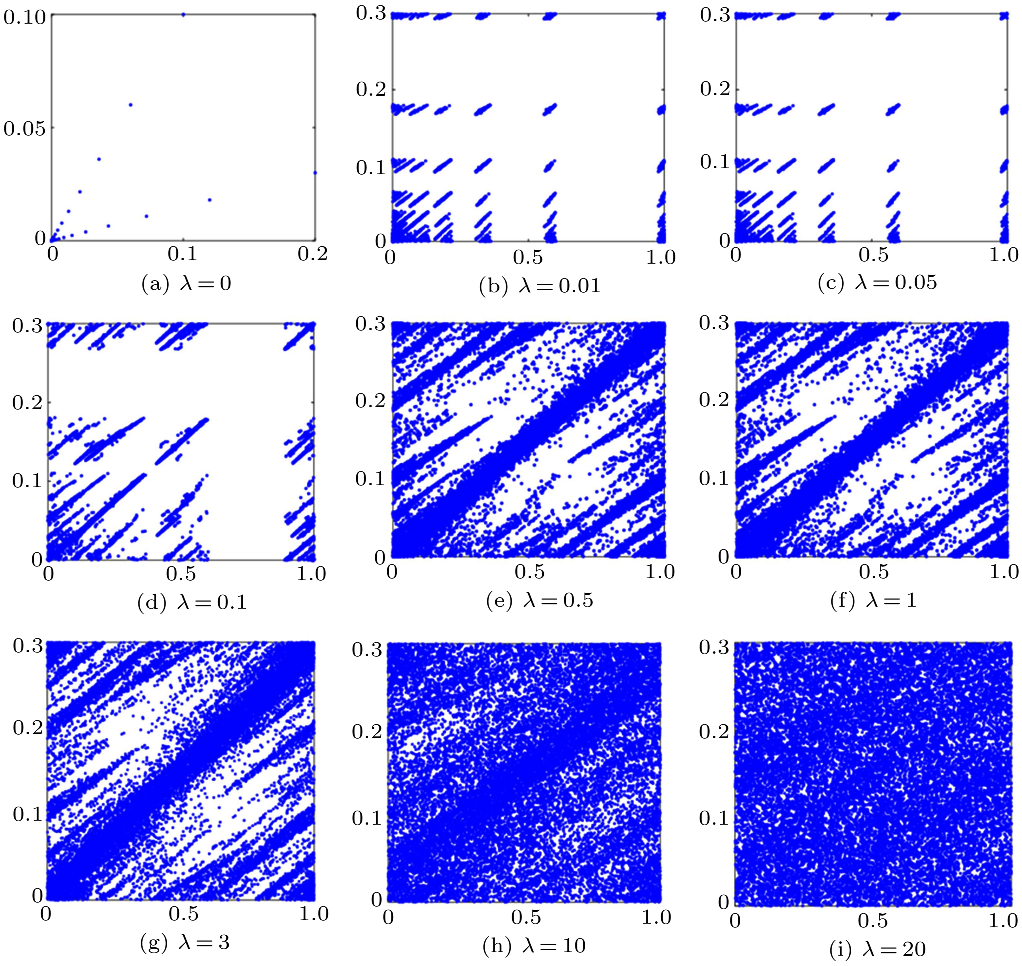


Fig. 3. (a) Auto-correlation functions of *x*-dimensional output of the controlled 2DLM. (b) The frequency distribution of *x*-dimensional output of the controlled 2DLM.

Figure 4 shows that with increasing λ, the phase space of the controlled 2DLM becomes more unordered. Finally, we cannot find any structure in the phase space and it just likes a state space filling with noise pattern.



(a) $\lambda=0$ (b) $\lambda=0.01$ (c) $\lambda=0.05$

(d) $\lambda=0.1$ (e) $\lambda=0.5$ (f) $\lambda=1$

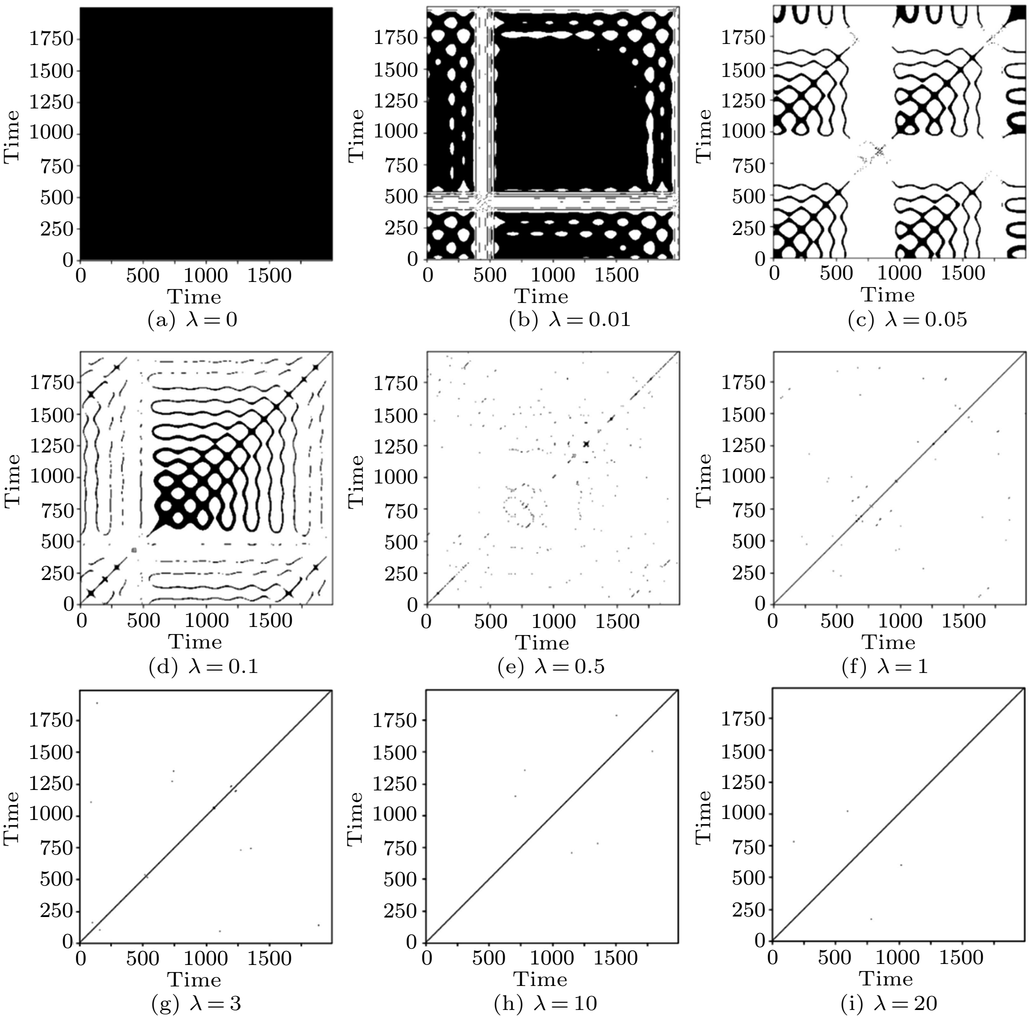
(g) $\lambda=3$ (h) $\lambda=10$ (i) $\lambda=20$

Fig. 4. Phase diagrams of the controlled 2DLM with different control parameters λ.

Figure 5 shows the recurrence plots (RP) of the controlled 2DLM with different control parameters. The RP method for time series is based on the analysis of a matrix R whose elements from the attractor $P=\{x_i\}_{i=1}^{N}\subset R^n$ are defined as

$$R_{ij}=\begin{cases}1, & \text{if } \|x_i-x_j\|<\varepsilon,\\ 0, & \text{otherwise.}\end{cases}$$

We use $\varepsilon=0.05$ in this paper, which was made based on empirical method. Recurrence quantification analysis (RQA) has been introduced to quantify the dynamical behavior from the structure of RP and can be applied to compare the trajectory's movements between different attractors. Two quantitative measures, determinism rate (DET) and laminarity (LAM),[30] which are very effective, are also given in Fig. 6. The DET and LAM decrease as λ increases. This result means that the controlled 2MLD is more indeterministic when λ is large, which is consistent with the result of the phase space analysis.



(a) $\lambda=0$ (b) $\lambda=0.01$ (c) $\lambda=0.05$

(d) $\lambda=0.1$ (e) $\lambda=0.5$ (f) $\lambda=1$

(g) $\lambda=3$ (h) $\lambda=10$ (i) $\lambda=20$

Fig. 5. Recurrence plots of the controlled 2DLM (x-dimensional state) with different control parameters λ.

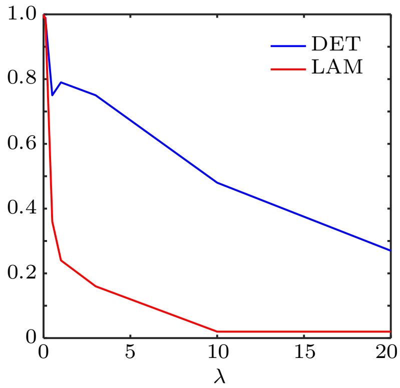


Fig. 6. Graphs of DET and LAM against different λ of the controlled 2DLM.

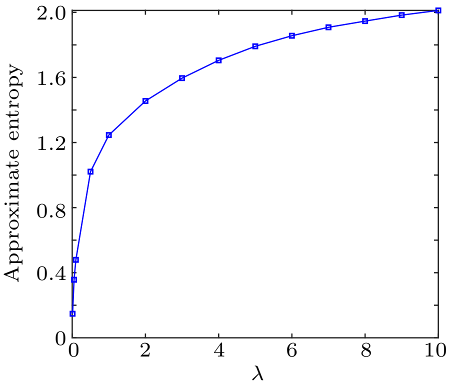


Fig. 7. Approximate entropy values of the controlled 2DLM (x-dimensional state) with different control parameters λ.

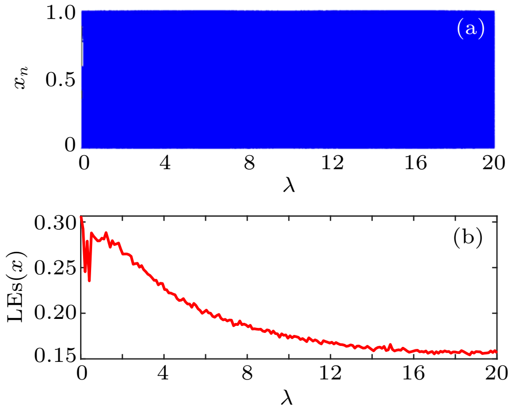


Fig. 8. (a) Bifurcation diagram and (b) Lyapunov exponent of the controlled 2DLM (x-dimensional state).

A complex chaotic system has few observable patterns in their trajectories. Approximate entropy, which is a method of quantifying the amount of regularity and unpredictability of the fluctuations over time series data,[31] is used to measure the complexity of the controlled 2DLM. As shown in Fig. 7, the approximate entropy of the controlled 2DLM increases with the increase of λ. We can conclude that the chaotic sequences of the controlled 2DLM become more complicated as λ increases. Moreover, bifurcation diagram and Lyapunov exponent analysis are used to depict the chaotic behaviors of the controlled 2DLM. Figure 8(a) shows that the proposed system has a large chaotic parameter range for the control parameter λ. The results in Fig. 8(b) indicate that the controlled 2DLM has positive Lyapunov exponent, but it is going down. Actually, when λ is small, the parameters of the 2DLM may enhance divergence of the controlled system. As λ increases, the control sequences generated from the continuous system gradually dominate, which causes the downward trend of the Lyapunov exponents. So we should select appropriate parameters in practical applications. Given the repetition and space constraints, we will choose the appropriate control parameters in the following examples and conduct the dynamic analysis.

4.2. Example 2: digital Henon map

In addition to high-dimensional linear map, consider the nonlinear Henon map under finite computing precision as follows:

$$F_P(x_i, y_i) \rightarrow \begin{cases} x_{i+1} = G_P(1 - ax_i^2 + y_i), \\ y_{i+1} = G_P(bx_i). \end{cases} \tag{8}$$

The original Henon map has the chaotic behavior where parameters $a = 1.4$ and $b = 0.3$, but when the Henon chaotic map is realized with finite precision, it will degrade and the orbits fall into a cycle.

Similarly, Chua chaotic system is applied to anti-control the digital Henon map, then, the controlled digital Henon map can be represented as

$$\begin{cases} x_{i+1} = (G_P(1 - ax_i^2 + y_i) + G_p(\gamma x(t))) \bmod \alpha, \\ y_{i+1} = G_P(bx_i), \end{cases} \tag{9}$$

where α, γ are the constants, and $x(t)$ is the x-dimensional state variable of the Chua chaotic system.

Let $\alpha = 2, \gamma = 10, P = 2^{-8}$ and the initial value $(x_0, y_0) = (0, 0)$, $Y(0) = (0.5, 0, 0)$. We compare the dynamical properties of the original Henon map, the digital Henon map, and the controlled digital Henon map. We perform the numerical experiments on trajectory, phase diagram, auto-correlation function, frequency distribution, and complexity, which is similar to Example 1.

As shown in Fig. 9, the original Henon map has a simple attractor, whereas for digital Henon map Eq. (8), the orbit can only go through several elements. Better than the two maps, the controlled digital Henon map Eq. (9) has more complicated attractor than its classical counterpart, which will enhance the resistance for statistical attack. Figure 10 shows the auto-correlation functions of the three maps. The original Henon map owns an irregular delta-like correlation function. Because of the low precision, the correlation of adjacent orbits becomes very strong in Fig. 10(b), which makes the digital Henon map vulnerable to correlation attack. As shown in Fig. 10(c), strong correlation is removed after control and the correlation function of the controlled digital Henon map is driven to be delta-like perfectly.

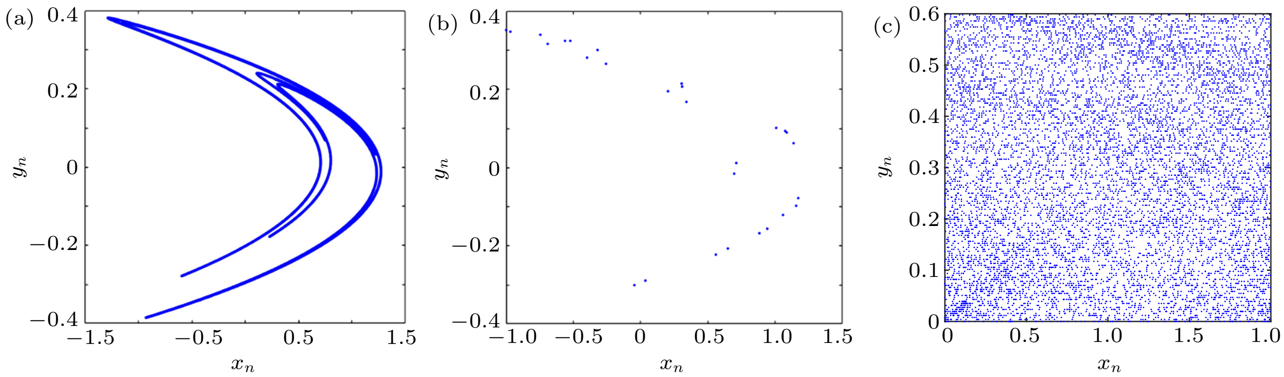


Fig. 9. The phase diagrams. Panels (a), (b), and (c) correspond to original Henon map, uncontrolled and controlled digital Henon maps.

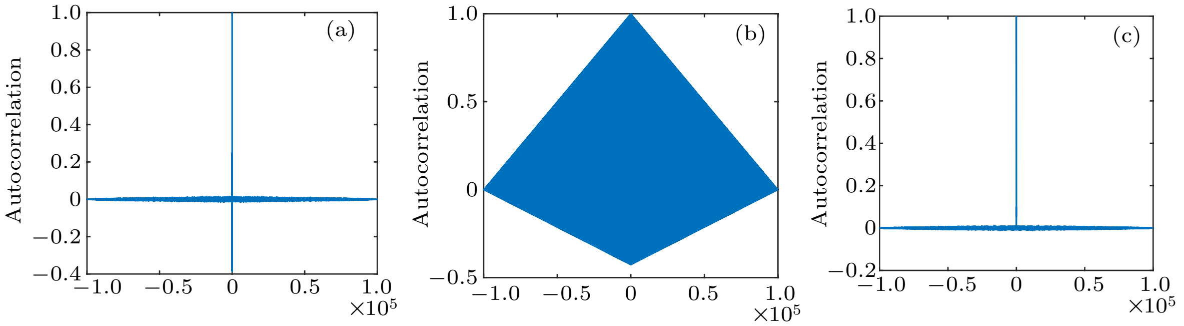


Fig. 10. Auto-correlation functions. Panels (a), (b), and (c) correspond to original Henon map, uncontrolled and controlled digital Henon maps.

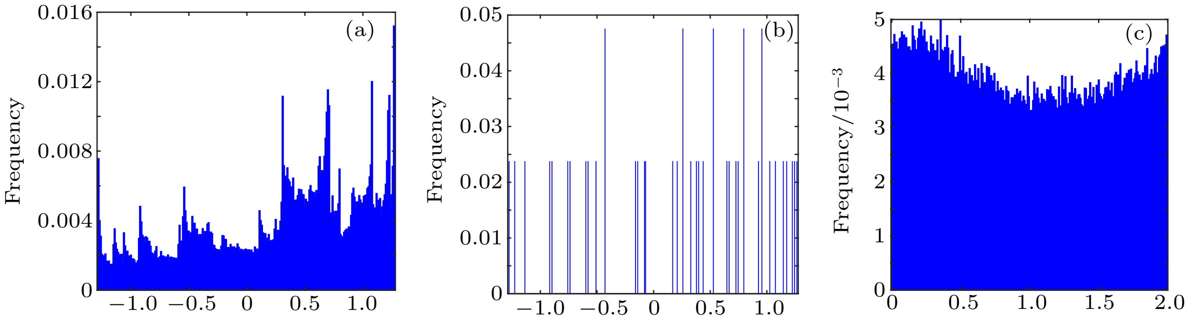


Fig. 11. The frequency distributions. Panels (a), (b), and (c) correspond to original Henon map, uncontrolled and controlled digital Henon maps.

Besides, the controlled Henon map has a more homogeneous frequency distribution than the original Henon map as shown in Fig. 11. The approximate entropy is also used to measure the complexity of three comparative maps and the values are shown in Fig. 12. It can be seen that the approximate entropy of the digital Henon map increases with the increasing of the precision P and eventually approaches to that of the original Henon map (0.477825). However, the approximate entropy of the controlled digital Henon map is always much larger than the original logistic map. From the above experiments, we can conclude that the control method can not only greatly solve the dynamical degradation of the digital Henon map, but also enhance the complexity of the system.

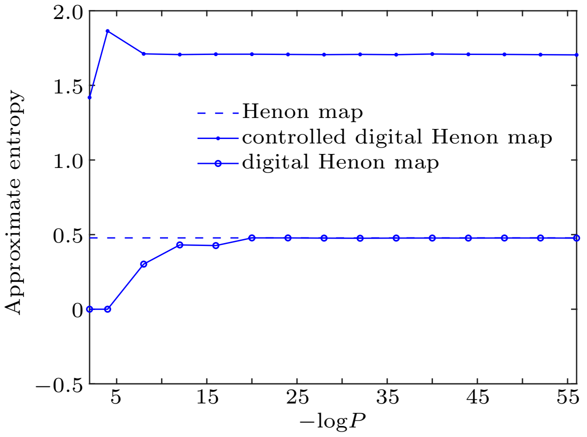


Fig. 12. The approximate entropies of Henon map, digital Henon map, and controlled Henon map with different finite precisions P.

4.3. Example 3: higher-dimensional linear map

Actually, there is little research on higher-dimensional digital chaotic systems. In this subsection, the constructed higher-dimensional linear map (HDLM) can be modeled as

$$\left(x_{n+1}^1, x_{n+1}^2, \ldots, x_{n+1}^k\right) = H_p\left(x_n^1, x_n^2, \ldots, x_n^k\right)$$
$$\rightarrow \begin{cases} x_{n+1}^1 = G_p\left(k_1 x_{n+1}^k\right), \\ x_{n+1}^2 = G_p\left(k_2 x_{n+1}^1\right), \\ \vdots \\ x_{n+1}^k = G_p\left(k_n x_{n+1}^{k-1}\right), \end{cases} \tag{10}$$

which can be of arbitrarily high dimensions. $k_1, k_2, \ldots, k_n$ are the system parameters. We choose the 4-dimensional linear map (4DLM) to be controlled by the Chua chaotic system. The control gain matrix is set as $B = \begin{pmatrix} \eta & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Then the controlled digital HDLM can be written as

$$\begin{cases} x_{n+1}^1 = G_p\left(k_1 x_n^4\right) + G_p\left(\eta x(t)\right) \bmod \alpha, \\ x_{n+1}^2 = G_p\left(k_2 x_n^1\right), \\ x_{n+1}^3 = G_p\left(k_3 x_n^2\right), \\ x_{n+1}^k = G_p\left(k_4 x_n^3\right), \end{cases} \tag{11}$$

where α, η are the constants, and $x(t)$ is the x-dimensional state variable of Chua chaotic system.

Set $k_1 = 2, k_2 = 0.8, k_3 = 0.7, k_4 = 0.6, \eta = 10, \alpha = 1, P = 2^{-16}$. Next, we use the same characteristics to highlight the effectiveness of the method for higher-dimensional digital chaotic system. As shown in Fig. 13, the size of the attractor depends on the system parameters $k_1, k_2, k_3, k_4, \alpha$. Figure 13 also shows that the 4DLM has a complicated attractor. Figure 14 depicts its good autocorrelation and decent frequency distribution, which conclude that the construction method of high-dimensional digital chaotic system is effective. As for approximate entropy experiments depicted in Figs. 15 and 7, the controlled HDLM outperforms the controlled 2DLM although their trends are consistent.

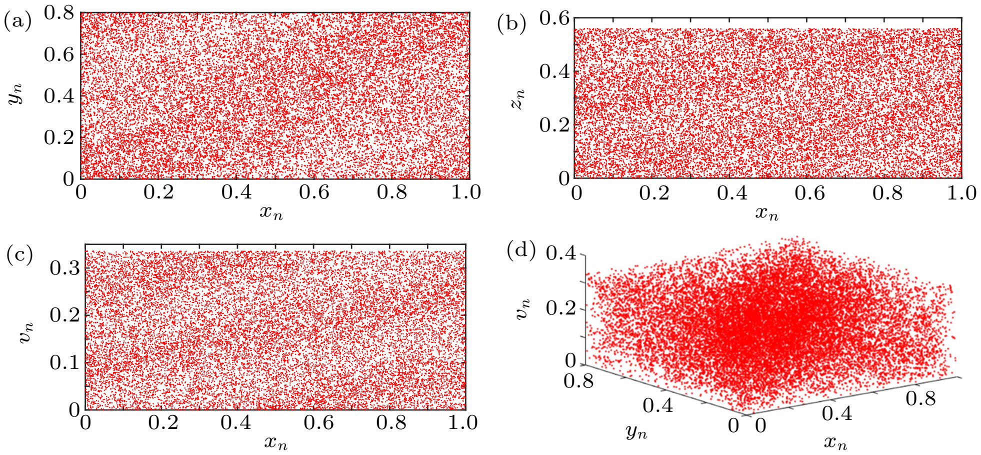


Fig. 13. Phase diagrams of the 4DLM: (a) x–y plane, (b) x–z plane, (c) x–v plane, (d) x–y–v space.

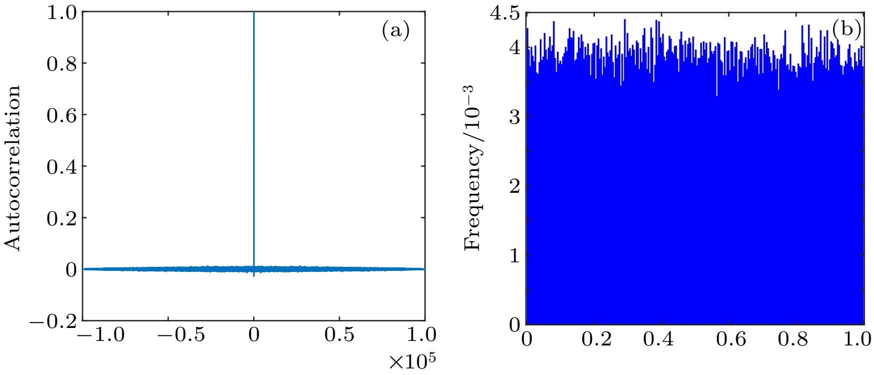


Fig. 14. (a) Auto-correlation functions of x-dimensional output of the controlled 4DLM. (b) The frequency distribution of x-dimensional output of the controlled 4DLM.

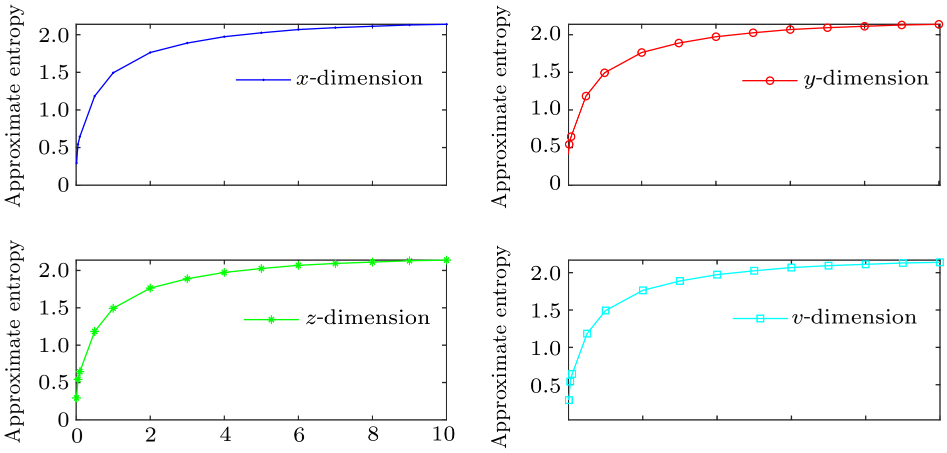


Fig. 15. Approximate entropy values of the controlled 4DLM with different control parameters λ.

5. An application of PRNG based on the controlled digital system

We can see that this method can be used to construct digital chaotic systems with any dimension. The controlled 4DLM has more optional parameters that can be used as secret keys in the given three HDDCS. And linear map is easy to implement. Therefore, a simple PRNG is proposed in this section based on the controlled 4DLM. The output of the controlled digital system is quantized, the binary sequence is generated by

$$s_n = \begin{cases} y_n + z_n, & x_n < 0.5, \\ y_n + v_n, & x_n \geqslant 0.5, \end{cases} \tag{12}$$

$$b_i = \begin{cases} 1, & \text{if } \bmod(100000 \times s_n, 1) > 0.5, \\ 0, & \text{otherwise,} \end{cases} \tag{13}$$

where b_i is the generated binary sequence, and x_n, y_n, z_n, v_n are the output sequences generated by the controlled 4DLM. The basic flowchart of the proposed PRNG is shown in Fig. 16.

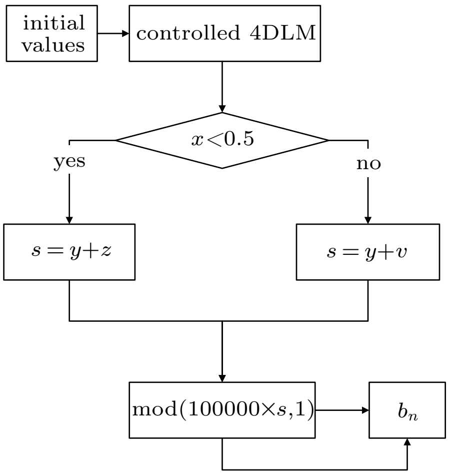


Fig. 16. Flowchart of the PRNG.

Table 1. Results of NIST SP800-22 tests for test sequences.

Test index	Success proportion	Mean value of *P*-values
Approximate entropy	0.998	0.5793
Cumulative sums (forward)	0.988	0.6546
Cumulative sums (reverse)	0.988	0.5311
FFT	0.996	0.2088
Block frequency	0.997	0.8961
Frequency	0.989	0.4159
Linear complexity	0.999	0.4407
Longest runs	0.997	0.5460
Overlapping-templates	0.997	0.8215
Random excursions	0.992	0.5184
Random excursions variant	0.996	0.5202
Rank	0.999	0.6042
Runs	0.996	0.4210
Serial1	0.999	0.2362
Serial2	0.998	0.1439
Universal	0.999	0.5247

Some statistical tests are performed on the generated binary sequence. Statistical tests determine whether the sequences possess certain attributes that true random sequences would exhibit. In this paper, we use the National Institute of Standards and Technology (NIST) SP800-22 Test Suite, which is a statistical package consisting of 15 tests developed to test the randomness of binary sequences and to test the performance of generated binary sequences. For each test, a corresponding P-value is calculated and compared with a given level. If $P \geqslant 0.01$, then it can be concluded that the sequence passes the test. Here, we use Eq. (11) to generate binary sequences. Set $\eta = 20$, 1000 sequences are generated by choosing different initial values. The results of NIST tests are shown in Table 1. From the result, it can be concluded that the test sequences can pass the test suite, verifying the randomness of the PRNG.

As for the key space, the proposed PRNG utilizes the controlled 4DLM. With different initial values and parameters, the key space is $\left(2^{16}\right)^8 = 2^{128}$. Even under low computing precision 2^{-16}, the value is basically able to resist brute force attacks. If the precision is set at 10^{-15}, the key space is $\left(10^{15}\right)^8 = 10^{120}$, which is much larger than 2^{128}. Further, if the parameters of the continuous systems and the control terms are considered as a secret key, the key space will be greatly large.

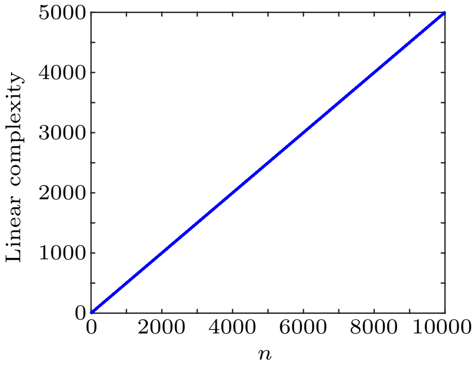


Fig. 17. Linear complexity of the generated bit sequence.

In addition, linear complexity is a significant indicator for ideal PRNG. For different lengths n, the numbers of 0s and 1s for bit sequences should be equal. Figure 17 shows the linear complexity of bit sequences generated by the proposed PRNG, which can be represented as an ideal straight line. This reflects the large linear complexity of the proposed PRNG.

6. Conclusion

Chaotic systems implemented on finite precision devices will suffer the problem of the dynamical degradation. In this paper, we propose a novel method of constructing high-dimensional digital chaotic systems on finite-state automata. Based on the external feedback anti-control theory, the continuous chaotic system, which owns infinite phase space, is sampled to anti-control the constructed digital systems. A rigorous proof is given that the controlled digital systems satisfy Devaney's definition of chaos. The simplest linear maps with different dimensions and nonlinear Henon map are taken as examples to show feasibility and effectiveness of the proposed method. The proposed method allows to construct high-dimensional digital chaotic systems with larger parameter space and more complex dynamical behaviors. In addition, the construction method can be applied to any given continuous chaotic systems. Meanwhile, the implementation cost of the construction method is low when designing simple and effective digital systems. Finally, a kind of PRNG is also proposed based on the constructed system. The test results show that the generated binary sequences have acceptable randomness, large key space, and high linear complexity. This work provides a good method of constructing higher-dimensional digital chaos on finite-state automata and may further promote applications such as chaotic cryptography, secure communication, and image encryption.

References

[1] Motter A E and Campbell D K 2013 *Phys. Today* **66** 27

[2] Li T Y and Yorke J A 1975 *Am. Math. Mon.* **82** 985

[3] Alvarez G and Li S 2006 *Int. J. Bifurcation Chaos* **16** 2129

[4] Millerioux G, Amigo J M, Daafouz J, *et al.* 2008 *IEEE Trans. Circuits Syst. I-Regul. Pap.* **55** 1695

[5] Ozkaynak F 2018 *Nonlinear Dyn.* **92** 305

[6] Yin R, Wang J, Yuan J, *et al.* 2012 *Sci. Chin. Inf. Sci.* **55** 1162

[7] Gao X J, Cheng M F, Deng L, *et al.* 2020 *Opt. Express* **28** 10847

[8] Ozkaynak F 2014 *Nonlinear Dyn.* **78** 2015

[9] Li S, Chen G, Mou X, *et al.* 2005 *Int. J. Bifurcation Chaos* **15** 3119

[10] Kwok H S and Tang W K 2007 *Chaos Solitons Fractal* **32** 1518

[11] Yang B and Liao X 2017 *Sci. Chin. Inf. Sci.* **60** 022302

[12] Liu L, Lin J, Miao S, *et al.* 2017 *Int. J. Bifurcation Chaos* **27** 1750103

[13] Wang C and Ding Q 2019 *Complexity* **2019** 5942121

[14] Liu H, Zhang Y, Kadir A, *et al.* 2019 *Appl. Math. Comput.* **360** 83

[15] Alawida M, Samsudin A, Teh J S, *et al.* 2019 *Signal Process* **160** 45

[16] Antonelli M, De Micco L, Larrondo H A, *et al.* 2018 *Entropy* **20** 135

[17] Sun C C, Xu Q C and Sui Y 2013 *Chin. Phys. B* **22** 030507

[18] Hu H, Xu Y and Zhu Z 2008 *Chaos Solitons Fractal.* **38** 439

[19] Tutueva A V, Andreev V S, Karimov A I, *et al.* 2020 *Chaos Solitons Fractals.* **133** 109615

[20] Moysis L, Tutueva A, Volos C, *et al.* 2020 *Symmetry* **12** 829

[21] Guyeux C and Bahi J M 2010 *International Joint Conference on neural network (IJCNN)*, July 18–23, 2010, Barcelona, Spain, pp. 1–7

[22] Wang Q, Yu S, Guyeux C, *et al.* 2014 *Int. J. Bifurcation Chaos* **24** 1450128

[23] Wang Q, Yu S, Guyeux C, *et al.* 2015 *Chin. Phys. B* **24** 060503

[24] Alawida M, Teh J S, Samsudin A, *et al.* 2019 *Signal Process.* **164** 249

[25] Alawida M, Samsudin A, Teh J S, *et al.* 2019 *Nonlinear Dyn.* **98** 2403

[26] Zheng J, Hu H, Ming H, *et al.* 2020 *Chaos Solitons Fractals* **138** 109863

[27] Lv X, Liao X, Yang B, *et al.* 2018 *Nonlinear Dyn.* **94** 325

[28] Fu C, Wen Z K, Zhu Z L, *et al.* 2016 *Int. J. Comput. Sci. Eng.* **12** 113

[29] Banks J, Brooks J, Cairns G, *et al.* 1992 *Am. Math. Mon* **99** 332

[30] Marwan N, Romano M C, Thiel M, *et al.* 2007 *Phys. Rep.* **438** 237

[31] Pincus S M 1991 *Proc. Nat Acad. Sci. USA* **88** 2297