

Research Article

A Torus-Chaotic System and Its Pseudorandom Properties

Jizhao Liu ¹, Xiangzi Zhang,² Qingchun Zhao ³, Jing Lian,⁴ Fangjun Huang ¹,
and Yide Ma⁵

¹School of Data and Computer Science, Sun Yat-sen University, Guangzhou, Guangdong 510006, China

²College of Information Science and Technology, Jinan University, Guangzhou, China

³School of Computer and Communication Engineering, Northeastern University, Qinhuangdao 066004, China

⁴School of Electronics and Information Engineering, Lanzhou Jiaotong University, 88 West Anning Road, Lanzhou, Gansu 730070, China

⁵School of Information Science and Engineering, Lanzhou University, Lanzhou, Gansu, China

Correspondence should be addressed to Fangjun Huang; 390766406@qq.com

Received 11 September 2019; Revised 1 April 2020; Accepted 23 May 2020; Published 6 July 2020

Academic Editor: Bernhard C. Geiger

Copyright © 2020 Jizhao Liu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Exploring and investigating new chaotic systems is a popular topic in nonlinear science. Although numerous chaotic systems have been introduced in the literature, few of them focus on torus-chaotic system. The aim of our short work is to widen the current knowledge of torus chaos. In this paper, a new torus-chaotic system is proposed, which has one positive Lyapunov exponent, two zero Lyapunov exponents, and two negative Lyapunov exponents. The dynamic behavior is investigated by Lyapunov exponents, bifurcations, and stability. The analysis shows that this system has an interesting route leading to chaos. Furthermore, the pseudorandom properties of output sequence are well studied and a random number generator algorithm is proposed, which has the potential of being used in several cyber security systems such as the verification code, secure QR code, and some secure communication protocols.

1. Introduction

Over the last four decades, chaos theory and its applications have been a central topic of nonlinear science [1]. As it is well known, chaos is associated with stochasticity, complex, irregular motion, and so on. It has some peculiar properties such as ergodicity, highly initial value sensitivity, non-periodicity, and long-term unpredictability. These pseudorandom features lead chaotic systems to enormous cryptographic applications like random number generator, image encryption, and secure communication, to name a few [2, 3].

There are two main paths for studying chaotic systems. The first path involves studying novel dynamic behaviors of chaotic systems. For example, Faghani et al. proposed some three-dimensional chaotic systems based on the general form of quadratic jerk systems. They analyzed the equilibrium, eigenvalue, and Lyapunov exponents of the proposed systems and proved that there

are 12 simple chaotic systems with identical eigenvalues. This is the first time that different chaotic systems with identical eigenvalues are described [4]. Qi and Liang investigated the angular momentum, torques, and Casimir energy of Qi system. They discovered different types of torques of the chaotic attractors [5]. Zhu et al. analyzed a sine-cosine compound function system. They proved that the proposed system satisfies Devaney's chaos definition and it has better unpredictability and more complex chaotic behaviors than classical sine map and Chebyshev map [6].

The second path proposes engineering applications of chaotic systems. For example, Liu et al. applied a simple chaotic system to differential chaos shift keying (DCSK) scheme. They demonstrated that the proposed spread spectrum communication scheme can reduce the bit error rate in the presence of noise [7]. Liu et al. proposed a chaos-based color image encryption scheme, which uses one-time keys from environmental noise [8]. Zhu et al. proposed a 2D

compound homogeneous hyperchaotic system (CHHCS). They demonstrated that the proposed scheme provides sufficient security against known attacks [9]. Hua et al. proposed a cosine-transform-based chaotic system (CTBCS). They proved that CTBCS can produce chaotic maps with complex dynamical behaviors. Therefore, the further proposed image encryption scheme provides a higher level of security than several advanced image encryption schemes [10].

In fact, the secure communication technology and data encryption technology based on chaos are essentially implemented using the pseudorandom nature of the chaotic systems. Therefore, the performance of the pseudorandom sequence generated by the chaotic system greatly affects the scores of these schemes. In recent years, a large number of studies have been conducted on random number generators (RNG). Singh et al. proposed a new chaotic oscillator by using a single op amp, two capacitors, one resistor, one inductor, and memristive diode bridge cascaded with an inductor. Based on this system, they designed a pseudorandom number generator and implemented it using Raspberry Pi 3 [11]. Alcín et al. proposed a novel type of high-speed true random number generator based on chaos and ANN and implemented in a Xilinx field-programmable gate array (FPGA) chip. They demonstrated that the implemented TRNG offers throughput up to 115.794 Mbps. Besides, the generated random numbers have been tested with the FIPS 140-1 and NIST 800.22 test suites [12]. Wang and Cheng proposed a pseudorandom number generator based on a modified logistic chaotic system. They proved that the pseudorandom sequence generated by this method has perfect randomness and cryptographic properties and can pass the statistical tests [13].

As it is well known, sensitive dependence on initial conditions, which can be quantified by Lyapunov exponent (LE), is the most important feature of chaos. For example, a three-dimensional bounded dynamic system can exhibit chaotic behavior if and only if its LEs are $(+, 0, -)$. When all the LEs are negative, the orbit starting from any point will eventually converge to a stable point. From another perspective, LEs can be regarded as the notion of divergence of orbits or degradation of information, the presence of positive LE suggests that the original information is lost, while zero LEs are equivalent to some form of invariant of two orbits or preserving the information of dynamic systems. Therefore, LEs can be a practical way to characterize and classify chaos [14]. According to Witold Kinser, a continuous-time system may have the following distinct dynamic behaviors [15]:

- (1) Limit cycle, whose LEs are $(0, -, \dots, -)$
- (2) Torus, whose LEs are $(0, \dots, 0, -, \dots, -)$
- (3) Chaos, whose LEs are $(+, 0, -, \dots, -)$
- (4) Hyperchaos, whose LEs are $(+, \dots, +, 0, -, \dots, -)$
- (5) Torus chaos, whose LEs are $(+, 0, \dots, 0, -, \dots, -)$

Compared with chaotic systems, hyperchaotic systems have more complex behavior. With more than one positive Lyapunov exponents, the dynamics of hyperchaotic systems are expanded in more than one direction giving rise to a more complex attractor. As Li demonstrated, hyperchaotic signals have great instability in two dimensions and

relatively more complicated dynamics, and because of this, hyperchaotic circuits can improve security which are useful in secure communications and radar engineering [16].

To the best of our knowledge, torus chaos has seldom been discussed among numerous proposed literatures. In 2009, Yang et al. proposed a 4D hyperchaotic system by adding a linear controller to the second equation of the 3D Lorenz system. They have shown that the proposed system can exhibit torus-chaos behavior when the parameters satisfied some special values [17]. In 2011, his team reported a 5D hyperchaotic system based on modified generalized Lorenz system. This system can also exhibit torus-chaos behavior [18]. In 2017, Singh and Roy proposed a simplest 4D dissipative autonomous chaotic system which is derived from Rossler type-IV 3D chaotic system. They proved that this system has chaotic 2-torus nature of Lyapunov exponents when bifurcation parameter satisfies some critical value [19]. However, the dynamic behavior of torus-chaotic system has not been well studied. This motivated us to further study torus-chaotic systems [20].

In this paper, we proposed a new torus-chaotic system. The dynamic behavior is investigated by Lyapunov exponents, bifurcations, and stability. The analysis shows that this system has an interesting route leading to chaos. A period-doubling behavior is observed in one subspace, but in other subspaces, there is no period-doubling behavior. It is like the saddle point: the system is stable in one direction but unstable in the other direction. Furthermore, the pseudorandom properties of output sequences are well studied. It is proved that the torus-chaotic system has worse pseudorandom properties than hyperchaotic system but has better pseudorandom properties than chaotic system. Based on its pseudorandom properties, a random number generator algorithm is proposed, which has the potential of being used in several cyber security systems such as the verification code, secure QR code, and some secure communication protocols.

The rest of this paper is organized as follows. In Section 2, the novel torus-chaotic system is introduced. The analysis of dissipativity, equilibrium, stability, and Lyapunov vectors was presented in Section 3. Route to chaos is discussed in Section 4. Section 5 is the pseudorandom properties of output sequence and the random number generator algorithm. Conclusions are finally drawn in Section 6.

2. A Novel Torus-Chaotic System

In 2018, Liu et al. introduced a general method to construct n th-order chaotic systems with hyperbolic sine nonlinearity [21]. When $n = 5$, there is a fifth-order chaotic system which is described by

$$\begin{cases} \dot{x}_1 = x_2 - x_1, \\ \dot{x}_2 = x_3 - x_2, \\ \dot{x}_3 = x_4, \\ \dot{x}_4 = x_5, \\ \dot{x}_5 = -x_5 - \rho \sinh(\varphi x_4) - 5x_3 - 5x_2 - 0.1x_1. \end{cases} \quad (1)$$

By introducing a nonlinear feedback controller to system equation (1), the following system which can exhibit torus-chaos behavior is obtained:

$$\begin{cases} \dot{x}_1 = x_2 - \rho \sinh(\varphi x_3), \\ \dot{x}_2 = x_3 - x_2, \\ \dot{x}_3 = x_4, \\ \dot{x}_4 = x_5, \\ \dot{x}_5 = -cx_5 - \rho \sinh(\varphi x_4) - 5x_3 - 5x_2 - 0.1x_1, \end{cases} \quad (2)$$

where x_1, x_2, x_3, x_4 , and x_5 are the state variables. $\sinh(\varphi x) = (e^{\varphi x} - e^{-\varphi x})/2$, $\rho = 1.2 \times 10^{-6}$, and $\varphi = 1/0.026$, which have been chosen to facilitate circuit implementation using diodes in future. c is considered as the bifurcation parameter.

To numerically calculate the phase space plots, Lyapunov exponents, and Poincaré sections, a fourth-order Runge–Kutta integrator with fixed step of 0.001 is utilized. To avoid transient response, the initial $1e6$ iterated data are omitted, and the following $2e6$ data are used in plotting phase space plots and Poincaré sections, while the following $1e9$ data are used in calculating some critical Lyapunov exponents.

When $c = 1.55$ and the initial conditions are set to be $(x_1, x_2, x_3, x_4, x_5) = (-0.1, -0.1, -0.1, -0.1, -0.1)$ and $(x_1, x_2, x_3, x_4, x_5) = (0.1, 0.1, 0.1, 0.1, 0.1)$, the system has two coexisting attractors as shown in Figures 1(a) and 1(b). When $(x_1, x_2, x_3, x_4, x_5) = (0.1, 0.1, 0.1, 0.1, 0.1)$, the Lyapunov exponents converged to $(0.47, 0, 0, -1.10, -1.37)$, which suggests that the system exhibits two-torus-chaotic behavior [22].

In order to catch the trajectory of the attractor, the Poincaré sections of $x_1 - x_3$ and $x_2 - x_3$ plane are plotted in Figure 2, of which $c = 1$ and initial conditions is set to be $(x_1, x_2, x_3, x_4, x_5) = (-3.5, -0.3, -0.3, -0.4, -1.5)$. From Figure 2, the system is exhibiting chaotic behavior.

3. Dynamical Behaviors of the Novel System

3.1. Dissipativity of the Novel System. For system equation (2), it is noticed that

$$\nabla V = \frac{\partial \dot{x}_1}{\partial x_1} + \frac{\partial \dot{x}_2}{\partial x_2} + \frac{\partial \dot{x}_3}{\partial x_3} + \frac{\partial \dot{x}_4}{\partial x_4} + \frac{\partial \dot{x}_5}{\partial x_5} = -1 - c. \quad (3)$$

When $c > -1$, the system is dissipative with an exponential contraction rate: $dV/dt = -1 - c$. In this situation, this system is an open system which has dissipative structures [23], all system orbits are ultimately confined to some subset of zero volumes as $t \rightarrow \infty$, and the asymptotic motion settles on some attractors [24].

3.2. Equilibrium and Stability. Suppose that the system $\dot{x} = f(x)$, $x \in R^n$, possesses an equilibrium point P . That is, $f(P) = 0$. Then $x = P$ is a solution for all of the time. Therefore, the equilibrium point can be solved by $\dot{x} = 0$.

For this system, the equilibrium points are given by

$$\begin{cases} \dot{x}_1 = 0, \\ \dot{x}_2 = 0, \\ \dot{x}_3 = 0, \\ \dot{x}_4 = 0, \\ \dot{x}_5 = 0. \end{cases} \quad (4)$$

Therefore, it has three equilibrium points, which are $E_1 = (0, 0, 0, 0, 0)$, $E_2 = (-34.48, 0.3448, 0.3448, 0, 0)$, and $E_3 = (34.48, -0.3448, -0.3448, 0, 0)$.

The Jacobian matrix at the equilibrium is

$$J(s) = \begin{pmatrix} 0 & 1 & -\rho \varphi \cosh(\varphi x_3) & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ -0.1 & -5 & -5 & -\rho \varphi \cosh(\varphi x_4) & -c \end{pmatrix}. \quad (5)$$

The characteristic equation of (5) is

$$\lambda^5 + (1 + c)\lambda^4 + c\lambda^3 + 5\lambda^2 + (10 + 0.1A)\lambda + 0.1A + 0.1 = 0, \quad (6)$$

where $A = \rho \varphi \cosh(\varphi x_3)$. When $c = 1$, (6) exhibits two-torus-chaos behavior with LEs of $(0.47, 0, 0, -1.10, -1.37)$. The eigenvalues of corresponding Jacobian matrix are

$$\begin{aligned} \lambda_1(E_1) &= 0.76 + 1.52i, \\ \lambda_2(E_1) &= 0.76 - 1.52i, \\ \lambda_3(E_1) &= -0.01, \\ \lambda_4(E_1) &= -1.76 + 0.58i, \\ \lambda_5(E_1) &= -1.76 - 0.58i, \end{aligned} \quad (7)$$

$$\begin{aligned} \lambda_1(E_2) &= 0.76 + 1.52i, \\ \lambda_2(E_2) &= 0.76 - 1.52i, \\ \lambda_3(E_2) &= -0.01, \\ \lambda_4(E_2) &= -1.76 + 0.58i, \\ \lambda_5(E_2) &= -1.76 - 0.58i. \end{aligned} \quad (8)$$

Since $\cosh(x)$ is an even function, the eigenvalues of equilibrium E_2 and E_3 are the same. Noticing that λ_1 and λ_2 of E_1, E_2 , and E_3 are all pairs of complex conjugate eigenvalues with positive real parts, λ_3 is all real eigenvalue and less than zero and λ_4 and λ_5 are all pairs of complex conjugate eigenvalues with negative real parts. Therefore, the three equilibrium points are all saddle points which have 1D knot manifold, 2D stable focus manifold, and 2D unstable focus manifold [25].

4. Visualization of Lyapunov Vectors

Lyapunov vectors, which have generally received less attention in the literature than Lyapunov exponents, are the time-dependent spatial structures associated with the corresponding Lyapunov exponents, which are in turn the asymptotic exponential growth rates of linear disturbances in general time-dependent flows. With the Lyapunov vectors, expanding/shrinking subspaces can be identified. In this section, we present the visualization of Lyapunov vectors in this torus-chaotic system, so that expanding/shrinking subspaces can be observed.

We utilize quiver function of Matlab to visualize Lyapunov vectors. As it is known, this system has five LEs, and

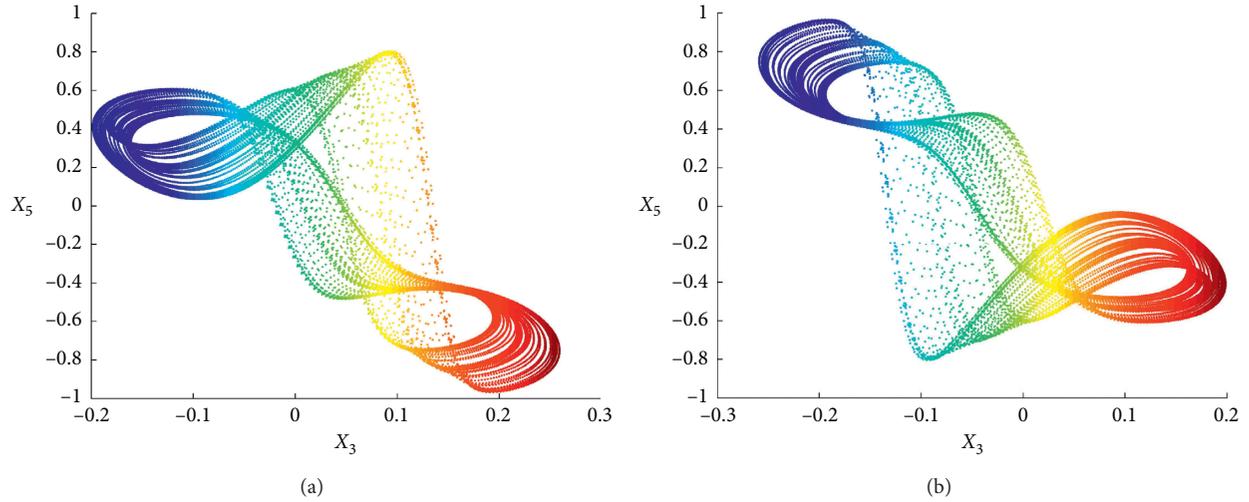


FIGURE 1: Phase space plots of $x_3 - x_5$ plane.

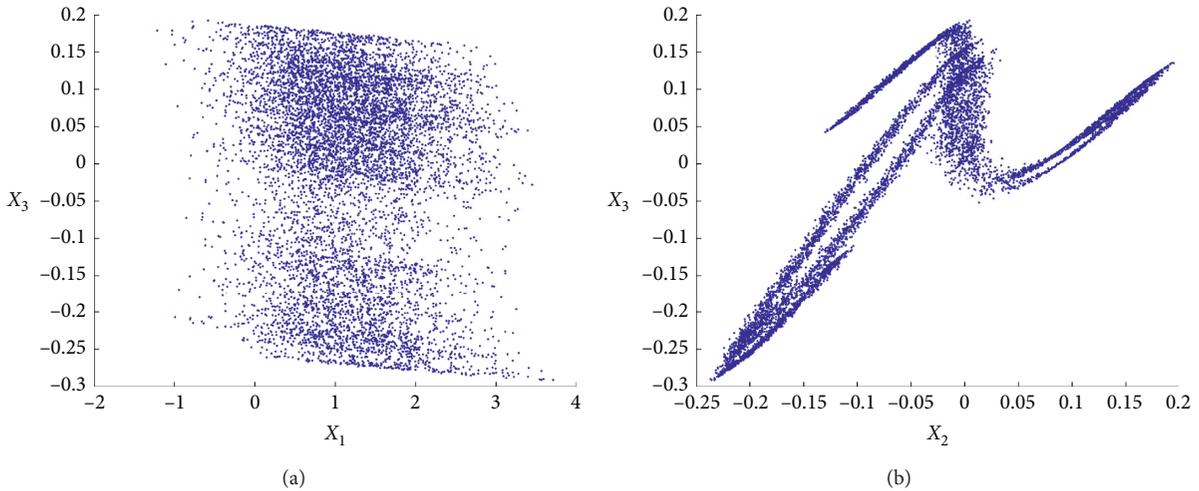


FIGURE 2: Poincaré sections of $x_1 - x_3$ and $x_2 - x_3$ plane.

each LE has five vector components. In this experiment, all initial conditions are set to be $(0.1, 0.1, 0.1, 0.1, 0.1)$. The positive Lyapunov vector, zero Lyapunov vectors, and negative Lyapunov vector are shown in Figures 3–5.

From Figures 3–8, the following can be observed:

- (1) All Lyapunov vectors rotate greatly along the orbit, which indicate that the expanding/shrinking subspaces changed along with the orbit.
- (2) Figures 4 and 5 describe two zero local Lyapunov vectors but none of them follows the tangent direction of the trajectory, which indicates that there is an expanding/shrinking mechanism along with the direction of the trajectory. When time approaches infinity, the average effect of expanding/shrinking of these two directions is zero.
- (3) Two close adjacent trajectories have completely different or even opposite Lyapunov vectors, which may suggest that chaotic system has multiple

stretching and folding mechanisms in infinitesimal neighborhoods.

5. Routes to Chaos

There are five important routes leading to chaos that have been identified and confirmed by numerical and physical experiments. They are period-doubling cascade, Ruelle–Takens–Newhouse, intermittency, crisis, and quasiperiodic routes.

The period-doubling cascade, which is also known as Feigenbaum’s route to chaos, is the most common behavior which exists in numerous chaotic systems. In this route to chaos, a fixed point loses stability to an attracting period-2 limit cycle as some parameters passed critical value. At later parameter value, this limit cycle also becomes unstable and turns into period-4 limit cycle. The new limit cycle then goes through a cascade of period doublings until chaos [26].

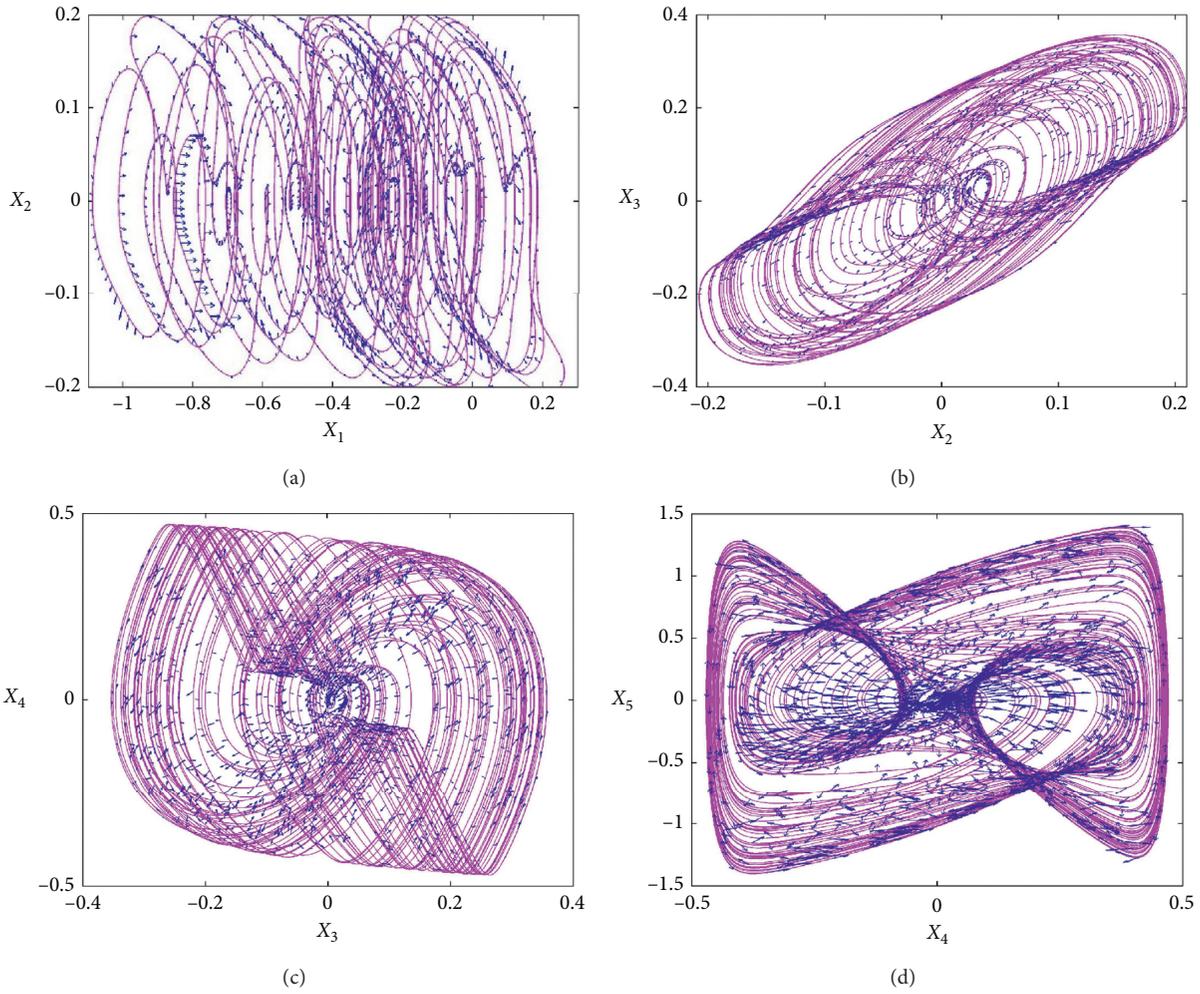


FIGURE 3: The positive Lyapunov vectors (LE1): (a) first and second components of positive Lyapunov vectors (LE1) in $x_1 - x_2$ plane; (b) second and third components of positive Lyapunov vectors (LE1) in $x_2 - x_3$ plane; (c) third and fourth components of positive Lyapunov vectors (LE1) in $x_3 - x_4$ plane; (d) fourth and fifth components of positive Lyapunov vectors (LE1) in $x_4 - x_5$ plane.

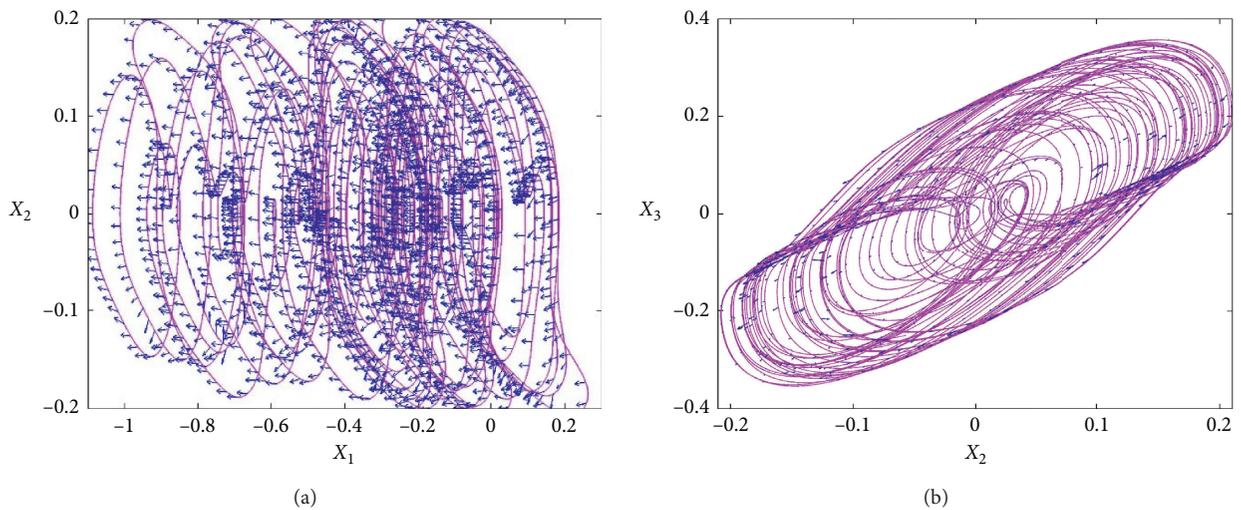


FIGURE 4: Continued.

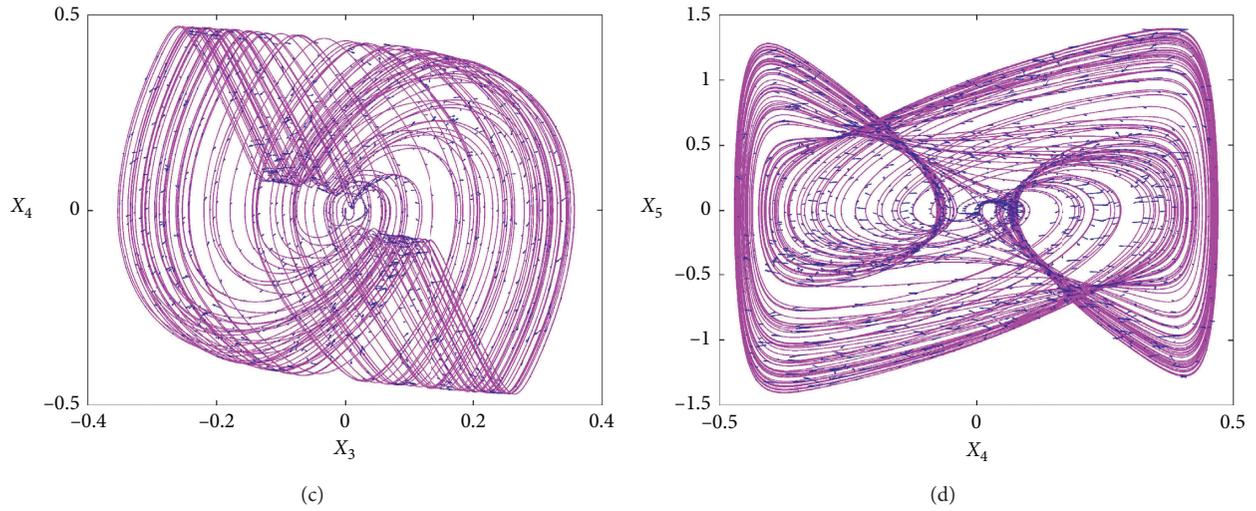


FIGURE 4: The zero Lyapunov vectors (LE2): (a) first and second components of zero Lyapunov vectors (LE2) in $x_1 - x_2$ plane; (b) second and third components of zero Lyapunov vectors (LE2) in $x_2 - x_3$ plane; (c) third and fourth components of zero Lyapunov vectors (LE2) in $x_3 - x_4$ plane; (d) fourth and fifth components of zero Lyapunov vectors (LE2) in $x_4 - x_5$ plane.

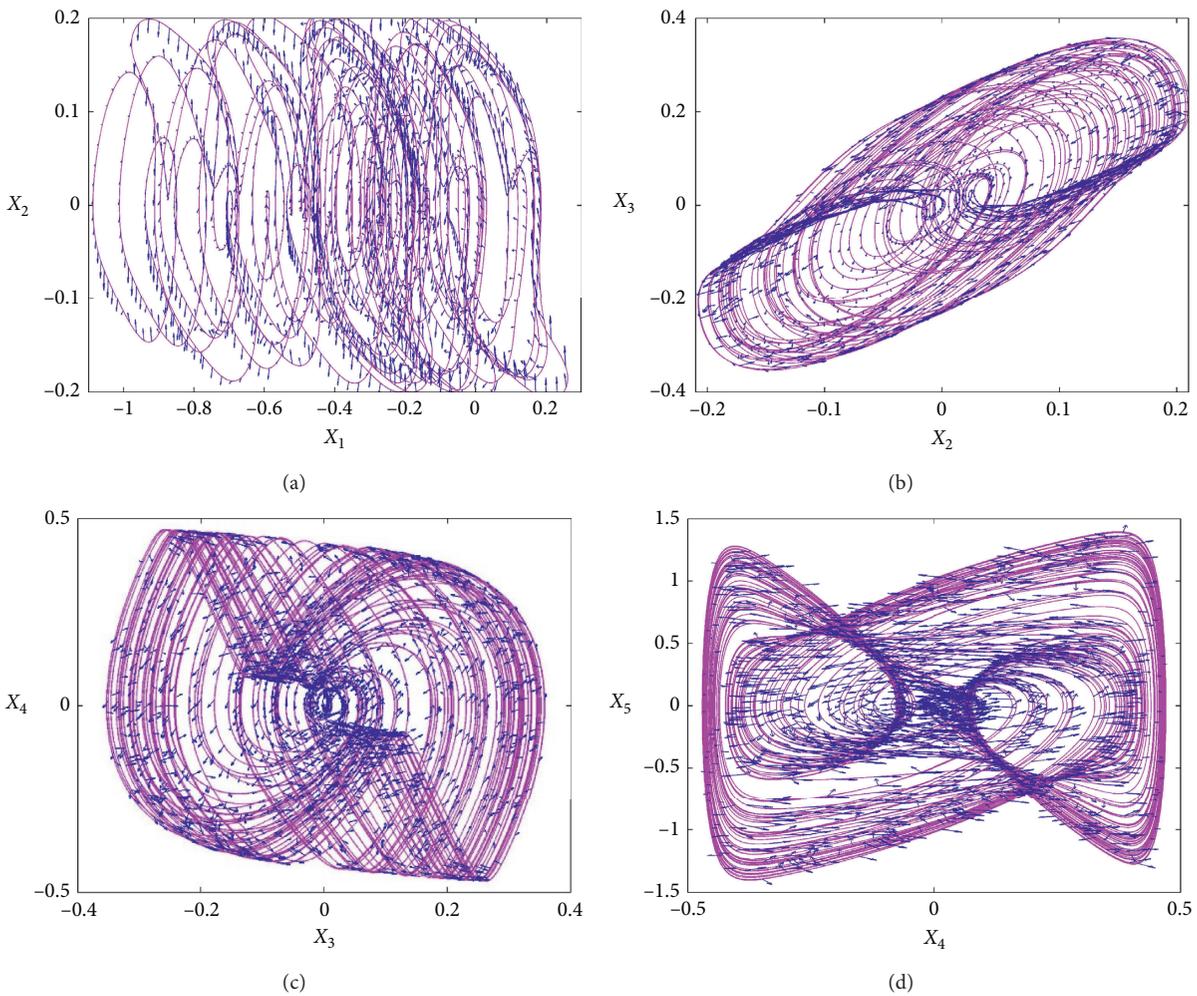


FIGURE 5: The zero Lyapunov vectors (LE3): (a) first and second components of zero Lyapunov vectors (LE3) in $x_1 - x_2$ plane; (b) second and third components of zero Lyapunov vectors (LE3) in $x_2 - x_3$ plane; (c) third and fourth components of zero Lyapunov vectors (LE3) in $x_3 - x_4$ plane; (d) fourth and fifth components of zero Lyapunov vectors (LE3) in $x_4 - x_5$ plane.

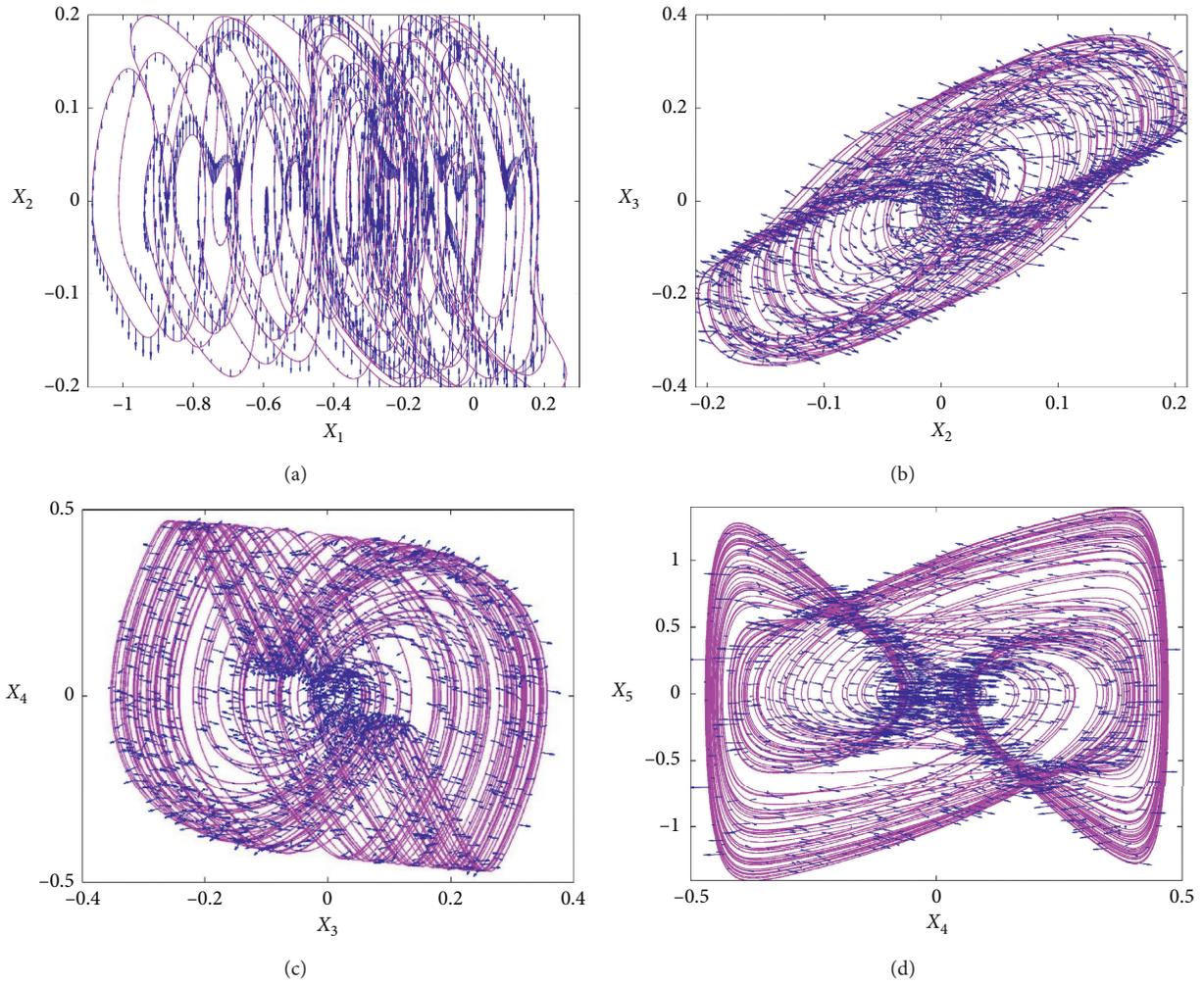


FIGURE 6: The negative Lyapunov vectors (LE4): (a) first and second components of negative Lyapunov vectors (LE4) in $x_1 - x_2$ plane; (b) second and third components of negative Lyapunov vectors (LE4) in $x_2 - x_3$ plane; (c) third and fourth components of negative Lyapunov vectors (LE4) in $x_3 - x_4$ plane; (d) fourth and fifth components of negative Lyapunov vectors (LE4) in $x_4 - x_5$ plane.

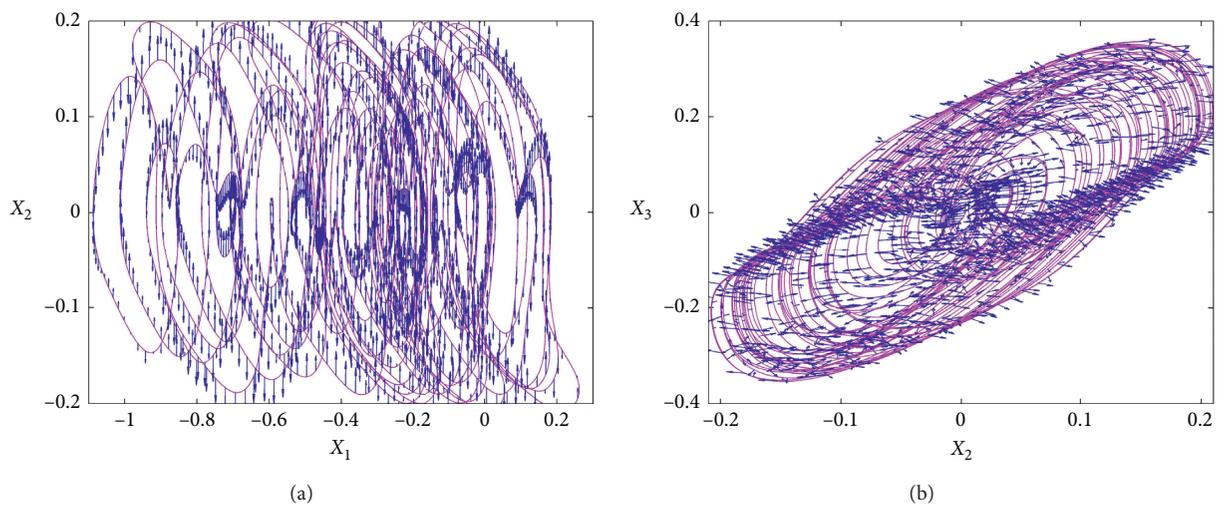


FIGURE 7: Continued.

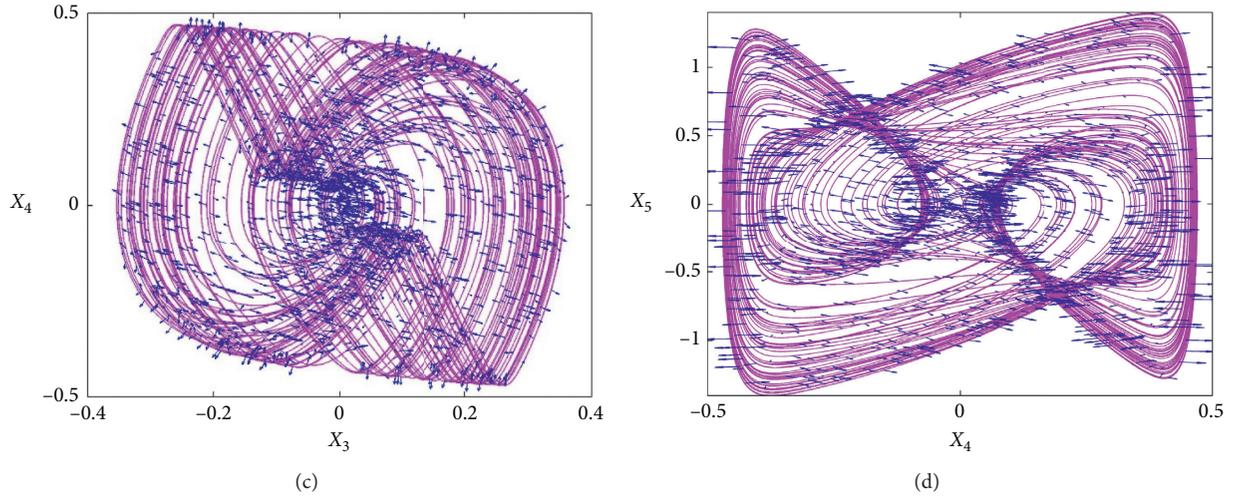


FIGURE 7: The negative Lyapunov vectors (LE5): (a) first and second components of negative Lyapunov vectors (LE5) in $x_1 - x_2$ plane; (b) second and third components of negative Lyapunov vectors (LE5) in $x_2 - x_3$ plane; (c) third and fourth components of negative Lyapunov vectors (LE5) in $x_3 - x_4$ plane; (d) fourth and fifth components of negative Lyapunov vectors (LE5) in $x_4 - x_5$ plane.

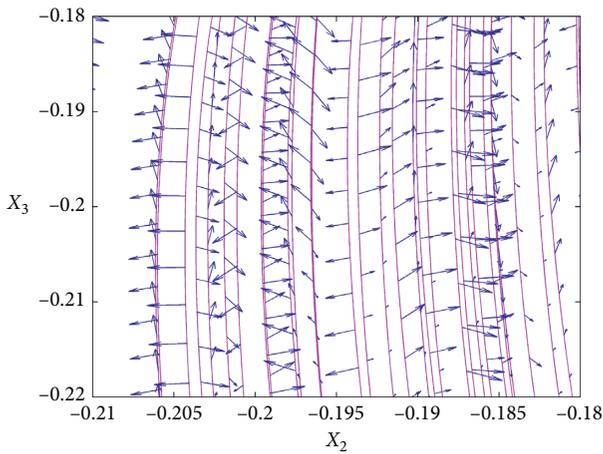


FIGURE 8: Zoom map of Figure 6(b).

Ruelle–Takens–Newhouse has proved that if the attractor of a system has three independent frequencies, then a small perturbation of this system has a hyperbolic strange attractor, a Plykin attractor. This scenario is called Ruelle–Takens–Newhouse route to chaos [27].

Intermittency denotes a type of behavior where the dynamics vary chaotically between two different phases of motion. One of these phases is regular (close to stationary, periodic, or quasiperiodic motion) and is called laminar phase. The laminar phase is interrupted by turbulent bursts, which corresponds to some irregular phases of motion. In chaotic systems, there exist different types of intermittencies. Pomeau and Manneville described three different types of intermittency. Each type of intermittency is related to a different kind of bifurcation, which are saddle-node bifurcation, subcritical Hopf bifurcation, and inverse period-doubling bifurcation [28].

In the crisis route, a chaotic attractor is suddenly created to replace a nonattracting chaotic saddle as the parameter

passes through the crisis value. Common types of crisis are boundary crisis, interior crisis, and symmetry restoring (breaking) crisis. These routes are due to the collision of the chaotic attractor with an unstable invariant set, typically an unstable periodic orbit (equivalently, a collision between a chaotic attractor and a coexisting unstable fixed point or periodic orbits) [29].

Quasiperiodic routes are also known as torus breakdown. In this mechanism, the torus (quasiperiodic orbit) loses its smoothness and gives birth to chaos as some parameter passes some critical value. This scenario has been observed in many natural and man-made systems including the Rayleigh–Benard convection [30], the Taylor–Couette flow [31], and electrical circuits [32].

In 2017, Singh and Roy proposed a 4D dissipative autonomous chaotic system which can exhibit 2-torus, 3-torus, and torus-chaos behavior. The numerical calculation shows that there are a period-doubling route and an intermittency route to chaos [19].

To study the route from torus to torus-chaos in this system, the LEs spectrum, Kaplan–Yorke dimension spectrum, and bifurcations [33] of (2) are plotted as the coefficient c is varied over the range $c \in [0.3, 2]$. Note that Figure 9(c) shows the value of x_2 every time x_2 reaches a local maximum or equivalently whenever x_2 crosses zero in the downward direction [34]. Figure 9(d) shows the value of x_5 every time x_2 reaches a local maximum or equivalently whenever x_2 crosses zero in the downward direction. Figure 9(e) shows the value of x_3 every time x_3 reaches a local maximum or equivalently whenever x_3 crosses zero in the downward direction. Figure 9(f) shows the value of x_5 every time x_3 reaches a local maximum or equivalently whenever x_3 crosses zero in the downward direction. Figure 9(g) shows the value of x_5 every time $x_2 = 0$. Figure 9(h) shows the value of x_5 every time $x_3 = 0$. According to the LEs spectrum, one can locate the region of torus chaos, and then the dimension of a torus-chaotic

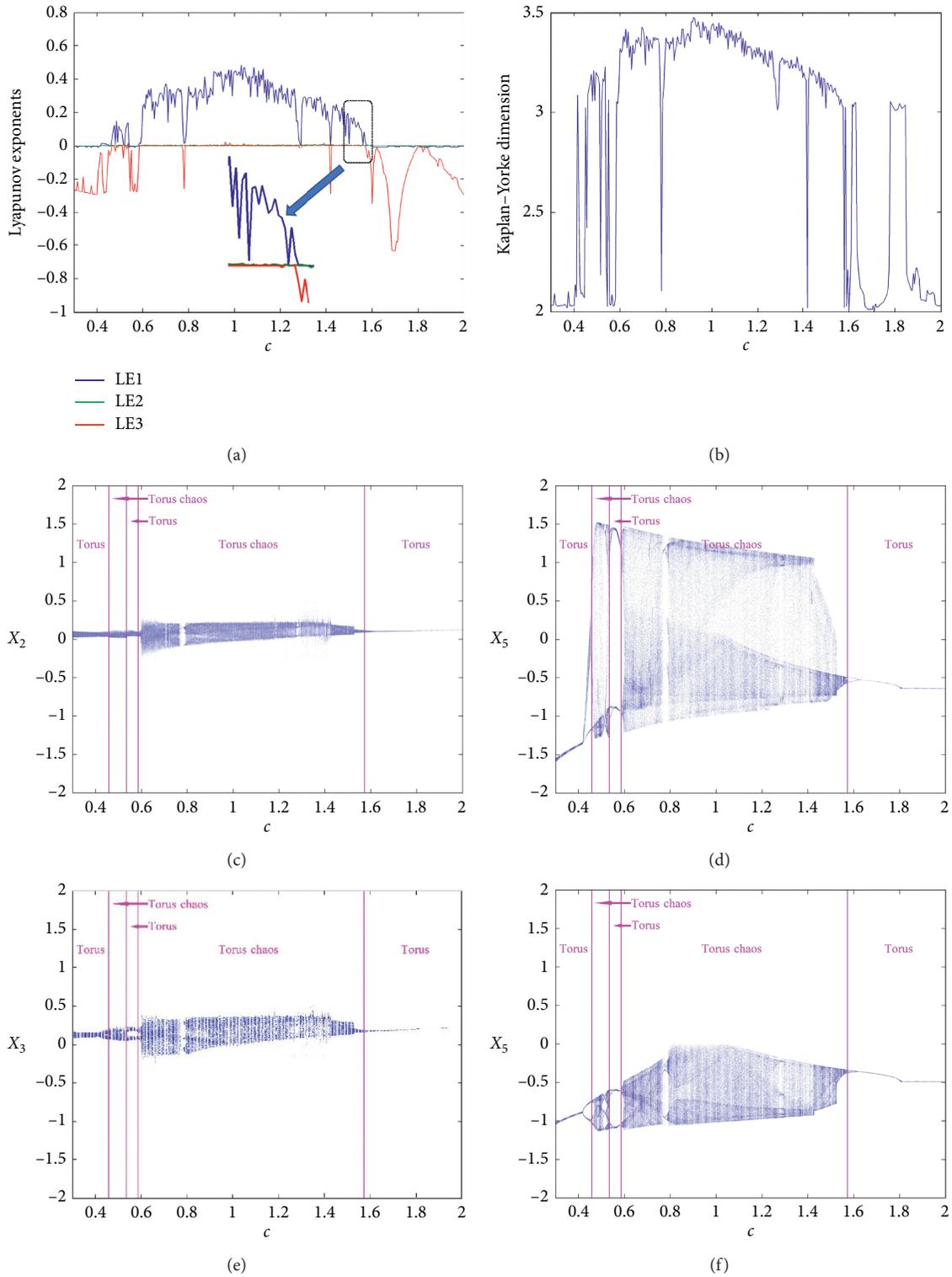


FIGURE 9: Continued.

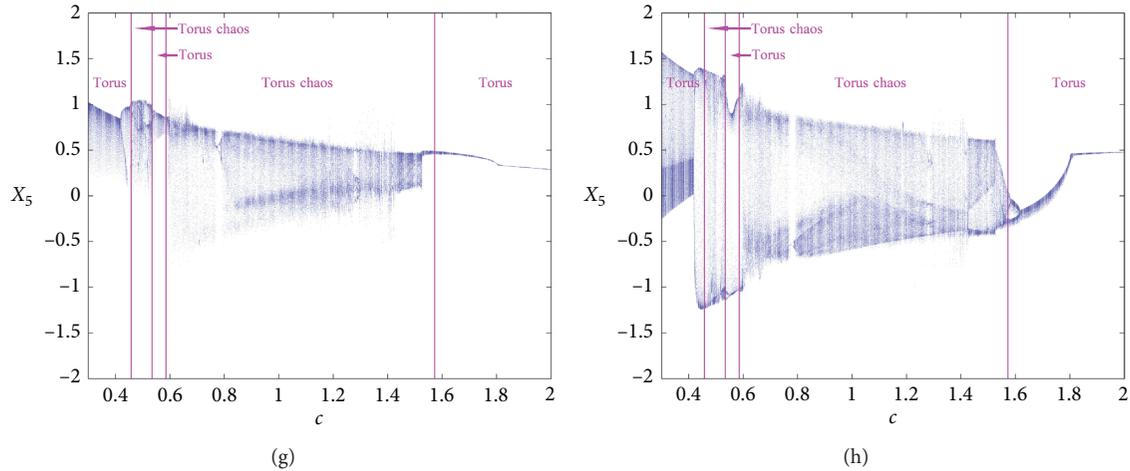


FIGURE 9: LEs spectrum, Kaplan–Yorke dimension spectrum, and bifurcations of (2) as the coefficient c is varied over the range $c \in [0.3, 2]$.

attractor determined the Kaplan–Yorke dimension spectrum. Since the system cannot exhibit hyperchaotic behavior within the parameters, the dimension of a torus-chaotic attractor is between 3.1 and 3.5, the dimension of 2-torus attractor is 2, and 3-torus attractor is 3.

Figure 9 suggests that this system has an interesting route leading to chaos:

- (1) When $c \in [0.3, 0.4639]$, there exists a period-doubling behavior along with \dot{x}_2 and \dot{x}_3 subspace. However, the system shows torus behavior along with x_2 and x_3 subspace. It is like saddle point; the system is stable in one direction but unstable in the other direction.
- (2) When $c \in [0.4640, 0.5574]$, the system exhibits two-torus-chaos behavior except for some 2-torus windows. When the parameter passed $c=0.4639$ to $c=0.4640$, two-torus chaos is born by replacing the 2-torus behavior. The LEs at these two critical values are $(LE1, LE2, LE3, LE4, LE5) = (0, 0, -0.01, -0.57, -0.88)$ for $c=0.4639$ and $(LE1, LE2, LE3, LE4, LE5) = (0.02, 0, 0, -0.60, -0.88)$ for $c=0.4640$. This may be caused by the period-doubling route along with \dot{x}_2 and \dot{x}_3 subspace.
- (3) When $c \in [0.5575, 0.5901]$, the system exhibits 2-torus behavior.
- (4) When $c \in [0.5902, 1.5575]$, the system exhibits two-torus-chaos behavior except for 2-torus windows. The route leading to chaos is similar to point 3.
- (5) When $c \in [1.5575, 2]$, the system exhibits 2-torus behavior, except for some 3-torus windows like $c=1.6157$.

6. Pseudorandom Properties

Since chaos is sensitive to initial conditions, it is very suitable to apply them to the purpose of random number generator. But before that, one should notice that the probability density distributions (PDDs) of chaotic systems are not

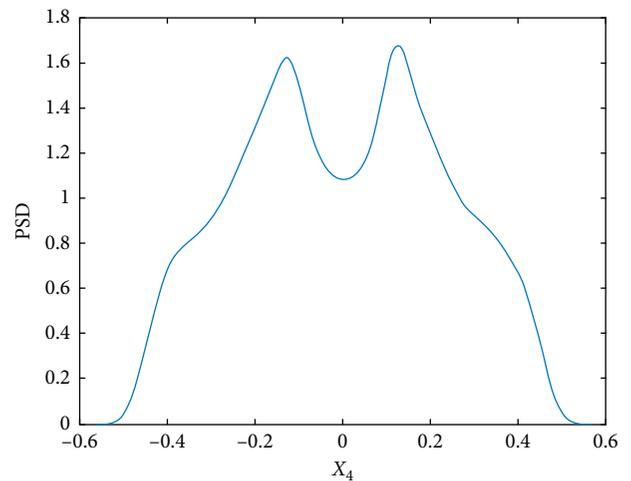


FIGURE 10: Probability density distributions of x_4 .

uniform distribution [35]. Figure 10 is the PDDs of x_4 , which indicates that it has physical characteristic. Thus, it cannot resist side channel attack.

In fact, all raw data generated by chaotic or hyperchaotic system cannot be used for cryptographic purposes. We compared pseudorandom properties of chaotic system, torus-chaotic system, and hyperchaotic system described in [36] and [18]. The results are shown in Tables 1~3.

The testing results indicate that hyperchaotic system has the best pseudorandom properties; it passed frequency, linear complexity, and cumulative sums tests. Chaotic system has worst pseudorandom properties which passed none of the tests. Torus-chaotic system passed overlapping template which means that its pseudorandom properties are better than chaotic system. However, all of these raw data cannot be used for cryptographic purposes because the physical characteristics have not been removed.

There are many ways to remove the physical characteristics of the output sequence; for example, in [11], the authors introduced an LSB-16 method to generate random

TABLE 1: Pseudorandom properties of chaotic system.

Test	P value	Result
Frequency	0	Failure
Block frequency	0	Failure
Longest run	0	Failure
Rank	0	Failure
FFT	0	Failure
Nonoverlapping template	0	Failure
Overlapping template	0	Failure
Linear complexity	0	Failure
Serial	0	Failure
Approximate entropy	0	Failure
Cumulative sums	0	Failure

TABLE 2: Pseudorandom properties of torus-chaotic system.

Test	P value	Result
Frequency	0	Failure
Block frequency	0	Failure
Longest run	0	Failure
Rank	0	Failure
FFT	0	Failure
Nonoverlapping template	0	Failure
Overlapping template	0.110698	Success
Linear complexity	0	Failure
Serial	0	Failure
Approximate entropy	0	Failure
Cumulative sums	0	Failure

TABLE 3: Pseudorandom properties of hyperchaotic system.

Test	P value	Result
Frequency	0.509254	Success
Block frequency	0	Failure
Longest run	0	Failure
Rank	0	Failure
FFT	0	Failure
Nonoverlapping template	0	Failure
Overlapping template	0	Failure
Linear complexity	0.706877	Success
Serial	0	Failure
Approximate entropy	0	Failure
Cumulative sums	0.373520	Success

number. In this manuscript, we utilize the following decorrelation operation:

$$S_{\text{out}} = S_{\text{in}} * 10^6 - \text{floor}(S_{\text{in}} * 10^6). \quad (9)$$

We tested the data of torus-chaotic system with decorrelation operation. The result is shown in Table 4.

From the testing results shown in Table 4, all output sequences passed fifteen kinds of random test of NIST 800-22, which indicated that the proposed method can be used as a part of some cyber security systems such as the verification code, secure QR code, and some secure communication protocols.

TABLE 4: Pseudorandom properties of torus-chaotic system with decorrelation operation.

Test	P value	Result
Frequency	0.841481	Success
Block frequency	0.900704	Success
Runs	0.744455	Success
Longest run	0.172897	Success
Rank	0.368065	Success
FFT	0.762020	Success
Nonoverlapping template	0.813121	Success
Overlapping template	0.532736	Success
Universal	0.856573	Success
Linear complexity	0.408679	Success
Serial	0.967366	Success
Approximate entropy	0.433157	Success
Cumulative sums	0.688582	Success
Random excursions	0.075229	Success
Random excursions variant	0.102049	Success

7. Conclusion

In this paper, we proposed a novel torus-chaotic system. The dynamic behavior is investigated by Lyapunov exponents, bifurcations, and stability. The analysis shows that this system has an interesting route leading to chaos. A period-doubling behavior is observed in one subspace, but in other subspaces, there is no period-doubling behavior. It is like saddle point: the system is stable in one direction but unstable in the other direction. Furthermore, the pseudorandom properties of output sequence are well studied. It is proved that the torus-chaotic system has worse pseudorandom properties than hyperchaotic system but has better pseudorandom properties than chaotic system. Based on its pseudorandom properties, a random number generator algorithm is proposed, which has the potential of being used in several cyber security systems such as the verification code, secure QR code, and some secure communication protocols.

Data Availability

All data are generated by the authors. One can repeat their results by the description provided in this manuscript.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors would like to thank Professor Julien Clinton Sprott for helpful discussion. Jizhao Liu had received research grants from Sun Yat-sen University. This study was supported by the Fundamental Research Funds for the Central Universities (no. 19lgpy230).

References

- [1] X. Zhang, Y. Li, and Ma. Shouliang, *Nonlinear Circuit-Based Analysis and Design*, Higher Education Press, Beijing, China, 2011.

- [2] 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.
- [3] Q. Gan, S. Yu, C. Li, J. Lü, Z. Lin, and P. Chen, "Design and arm-embedded implementation of a chaotic map-based multicast scheme for multiuser speech wireless communication," *International Journal of Circuit Theory and Applications*, vol. 45, no. 11, pp. 1849–1872, 2017.
- [4] Z. Faghani, F. Nazarimehr, S. Jafari, and J. C. Sprott, "A new category of three-dimensional chaotic flows with identical eigenvalues," *International Journal of Bifurcation and Chaos*, vol. 30, no. 02, Article ID 2050026, 2020.
- [5] G. Qi and X. Liang, "Force analysis of Qi chaotic system," *International Journal of Bifurcation and Chaos*, vol. 26, no. 14, Article ID 1650237, 2016.
- [6] H. Zhu, W. Qi, J. Ge, and Y. Liu, "Analyzing Devaney chaos of a sine-cosine compound function system," *International Journal of Bifurcation and Chaos*, vol. 28, no. 14, p. 1850176, 2018.
- [7] J. Liu, J. Clinton Sprott, S. Wang, and Y. Ma, "Simplest chaotic system with a hyperbolic sine and its applications in dcsk scheme," *IET Communications*, vol. 12, no. 7, pp. 809–815, 2018.
- [8] H. Liu, A. Kadir, and X. Sun, "Chaos-based fast colour image encryption scheme with true random number keys from environmental noise," *IET Image Processing*, vol. 11, no. 5, pp. 324–332, 2017.
- [9] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dynamics*, vol. 89, no. 1, pp. 61–79, 2017.
- [10] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Information Sciences*, vol. 480, pp. 403–419, 2019.
- [11] J. P. Singh, J. Koley, A. Akgul, B. Gurevin, and B. K. Roy, "A new chaotic oscillator containing generalised memristor, single op-amp and RLC with chaos suppression and an application for the random number generation," *The European Physical Journal Special Topics*, vol. 228, no. 10, pp. 2233–2245, 2019.
- [12] M. Alcin, I. Koyuncu, M. Tuna, M. Varan, and I. Pehlivan, "A novel high speed artificial neural network-based chaotic true random number generator on field programmable gate array," *International Journal of Circuit Theory and Applications*, vol. 47, no. 3, pp. 365–378, 2019.
- [13] L. Wang and H. Cheng, "Pseudo-random number generator based on logistic chaotic system," *Entropy*, vol. 21, no. 10, p. 960, 2019.
- [14] R. Brown and L. O. Chua, "Clarifying chaos: examples and counterexamples," *International Journal of Bifurcation and Chaos*, vol. 06, no. 02, pp. 219–249, 1996.
- [15] W. Kinsner, "Characterizing chaos through lyapunov metrics," *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, vol. 36, no. 2, pp. 141–151, 2006.
- [16] C. Li, A. Akgul, J. C. Sprott, H. H. C. Iu, and W. J.-C. Thio, "A symmetric pair of hyperchaotic attractors," *International Journal of Circuit Theory and Applications*, vol. 46, no. 12, pp. 2434–2443, 2018.
- [17] Q. Yang, K. Zhang, and G. Chen, "Hyperchaotic attractors from a linearly controlled lorenz system," *Nonlinear Analysis: Real World Applications*, vol. 10, no. 3, pp. 1601–1617, 2009.
- [18] Q. Yang and M. Bai, "A new 5d hyperchaotic system based on modified generalized lorenz system," *Nonlinear Dynamics*, vol. 88, no. 1, pp. 189–221, 2017.
- [19] J. P. Singh and B. K. Roy, "The simplest 4-D chaotic system with line of equilibria, chaotic 2-torus and 3-torus behaviour," *Nonlinear Dynamics*, vol. 89, no. 3, pp. 1845–1862, 2017.
- [20] J. C. Sprott, "A proposed standard for the publication of new chaotic systems," *International Journal of Bifurcation and Chaos*, vol. 21, no. 09, pp. 2391–2394, 2011.
- [21] J. Liu, J. Ma, J. Lian, P. Chang, and Y. Ma, "An approach for the generation of an nth-order chaotic system with hyperbolic sine," *Entropy*, vol. 20, no. 4, p. 230, 2018.
- [22] J. P. Singh and B. K. Roy, "The nature of Lyapunov exponents is (+,+,−). Is it a hyperchaotic system?" *Chaos, Solitons & Fractals*, vol. 92, pp. 73–85, 2016.
- [23] J. C. Sprott, *Elegant Chaos: Algebraically Simple Chaotic Flows*, World Scientific, Singapore, 2010.
- [24] J. C. Sprott and W. G. Hoover, "Harmonic oscillators with nonlinear damping," *International Journal of Bifurcation and Chaos*, vol. 27, no. 11, p. 1730037, 2017.
- [25] X. Zhang and G. Chen, "A geometric criterion for the existence of chaos based on periodic orbits in continuous-time autonomous systems," 2019, <http://arxiv.org/abs/1906.05405>.
- [26] J. Argyris, G. Faust, and M. Haase, "Routes to chaos and turbulence. a computational introduction," *Philosophical Transactions of the Royal Society of London. Series A: Physical and Engineering Sciences*, vol. 344, no. 1671, pp. 207–234, 1993.
- [27] A. M. Guzmán and C. H. Amon, "Transition to chaos in converging-diverging channel flows: Ruelle-takens – newhouse scenario," *Physics of Fluids*, vol. 6, no. 6, pp. 1994–2002, 1994.
- [28] Y. Fan, X. Huang, Z. Wang, and Y. Li, "Nonlinear dynamics and chaos in a simplified memristor-based fractional-order neural network with discontinuous memductance function," *Nonlinear Dynamics*, vol. 93, no. 2, pp. 611–627, 2018.
- [29] J. P. Singh and B. K. Roy, "Crisis and inverse crisis route to chaos in a new 3-d chaotic system with saddle, saddle foci and stable node foci nature of equilibria," *Optik*, vol. 127, no. 24, pp. 11982–12002, 2016.
- [30] R. Chertovskikh, E. V. Chimanski, and E. L. Rempel, "Route to hyperchaos in Rayleigh-Bénard convection," *EPL (Europhysics Letters)*, vol. 112, no. 1, p. 14001, 2015.
- [31] L. Oteski, Y. Duguet, L. Pastur, and P. Le Quéré, "Quasiperiodic routes to chaos in confined two-dimensional differential convection," *Physical Review E*, vol. 92, no. 4, Article ID 043020, 2015.
- [32] T. Matsumoto, L. Chua, and R. Tokunaga, "Chaos via torus breakdown," *IEEE Transactions on Circuits and Systems*, vol. 34, no. 3, pp. 240–253, 1987.
- [33] B. Munmuangsaen, J. C. Sprott, W. J.-C. Thio, A. Buscarino, and L. Fortuna, "A simple chaotic flow with a continuously adjustable attractor dimension," *International Journal of Bifurcation and Chaos*, vol. 25, no. 12, Article ID 1530036, 2015.
- [34] J. C. Sprott, "A new chaotic jerk circuit," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 58, no. 4, pp. 240–243, 2011.
- [35] J. Liu, S. Tang, J. Lian, Y. Ma, and X. Zhang, "A novel fourth order chaotic system and its algorithm for medical image encryption," *Multidimensional Systems and Signal Processing*, vol. 30, no. 4, pp. 1637–1657, 2019.
- [36] J. Liu, Y. Ma, S. Li, J. Lian, and X. Zhang, "A new simple chaotic system and its application in medical image encryption," *Multimedia Tools and Applications*, vol. 77, no. 17, pp. 22787–22808, 2018.