Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 8250903, 17 pages
https://doi.org/10.1155/2019/8250903

Research Article

Robust Chaos of Cubic Polynomial Discrete Maps with Application to Pseudorandom Number Generators

Dandan Han,[1,2] **Lequan Min**,[2] **Hongyan Zang**,[2] **and Xiuping Yang**[2]

[1] *School of Mathematics and Statistics Science, Ludong University, Yantai 264025, China*
[2] *School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 10008, China*

Correspondence should be addressed to Dandan Han; hxu1204@163.com

Received 28 September 2018; Accepted 16 January 2019; Published 7 April 2019

Academic Editor: Rosa M. Benito

Based on the robust chaos theorem of S-unimodal maps, this paper studies a kind of cubic polynomial discrete maps (CPDMs) and sets up a novel theorem. This theorem gives general conditions for the occurrence of robust chaos in the CPDMs. By using the theorem, we construct a CPDM. The parameter regions of chaotic robustness of the CPDM are larger than these of Logistic map. By using a fixed point arithmetic, we investigate the cycle lengths of the CPDM and a Logistic map. The results show that the maximum cycle lengths of 1000 chaotic sequences with length 3×10^7 generated by different initial value conditions exponentially increase with the resolutions. When the resolutions reach $10^{-7} \sim 10^{-13}$, the maximum cycle lengths of the cubic polynomial chaotic sequences are significantly greater than these of the Logistic map. When the resolution reaches 10^{-14}, there is the situation without cycle for 1000 cubic polynomial chaotic sequences with length 3×10^7. By using the CPDM and Logistic map, we design four chaos-based pseudorandom number generators (CPRNGs): CPRNGI, CPRNGII, CPRNGIII, and CPRNGIV. The randomness of two 1000 key streams consisting of 20000 bits is tested, respectively, generated by the four CPRNGs. The result suggests that CPRNGIII based on the cubic polynomial chaotic generalized synchronic system has better performance.

1. Introduction

Chaos is one type of complex dynamic behaviors displaying similarly random happenings within a determined nonlinear system or process. Chaotic systems are mainly defined and analyzed in continuous or discrete phase spaces. And they exhibit properties such as sensitive dependent on initial conditions and system parameters and ergodicity and long time's chaotic behaviors are not predictable [1]. In 1975, Li-Yorke first formally introduced the term chaos into mathematics [2]. They established a criterion for the existence of chaos in one-dimensional difference equations and the famous example is that "period three implies chaos".

Pseudorandom numbers have wide range of applications in many fields, such as physical systems simulation [3–6], information encryption [7–13], entertainment [14, 15], and computer simulation [16–20]. In the practical applications, pseudorandom algorithm has almost replaced the stochastic indicator and random number generator based on the hardware. John von Neumann was the first scholar who has made outstanding contributions to designing computer-based pseudorandom number generator. Currently, the known statistical test criterions of random number generator/pseudorandom number generators (RNGs/PRNGs) contain DIEHARD test [21] and FIPS 140 test [22] and SP 800-22 test [23] released by the National Institute of Standards and Technology (NIST).

In order to construct a chaotic quadratic polynomial, Zhou and Song set up a necessary and sufficient condition to determine the 3-periodic points of a quadratic polynomial [24], based on Li-Yorke's criterion. This research is a perfect application of Li-Yorke's theorem, but it is not suitable for researching the chaotic properties of cubic polynomial. Based on the theorem given in [25], Andrecut and Ali derived some general conditions and practical procedures for generating robust chaos in smooth unimodal maps [26].

Based on the robust chaos theorem of S-unimodal maps, this paper sets up a chaos criterion theorem for cubic polynomial discrete maps and constructs a novel cubic polynomial discrete map. Using this theorem and numerical simulations verifies that the parameter regions of chaotic robustness of the cubic polynomial discrete map are larger than these of Logistic map. The maximum cycle lengths of the cubic polynomial chaotic sequences are significantly greater than these of Logistic map, when the resolutions reach $10^{-7} \sim 10^{-13}$. Using the cubic polynomial discrete map and Logistic map constructs two 6-dimensional chaotic generalized synchronic systems (6DCGSS). Four chaos-based pseudorandom number generators CPRNGI, CPRNGII, CPRNGIII, and CPRNGIV, respectively, are designed by the cubic polynomial discrete map, Logistic map, and two 6DCGSS. The results of pseudorandomness tests suggest that CPRNGIII has better performance.

The rest of this paper is organized as follows. Section 2 introduces the robust chaos theorem of S-unimodal maps, and sets up a chaos criterion theorem of cubic polynomial discrete maps. Section 3 constructs a novel cubic polynomial discrete map. Numerical simulations analyze bifurcation and cycle lengths of the novel cubic polynomial discrete map and Logistic map. Section 4 presents two 6DCGSS based on the GS theorem. Section 5 designs four chaos-based pseudorandom number generators CPRNGI, CPRNGII, CPRNGIII, and CPRNGIV and makes the statistic tests for the four CPRNGs. Finally, Section 6 concludes the article.

2. Robust Chaos of Cubic Polynomial Maps

Robust chaos refers that, during the system parameter disturbances in a certain range, the system can guarantee the characteristics of chaos and still does not change the overall performance of the system. The robust chaos theorem of S-unimodal maps is introduced as follows.

Theorem 1 (see [26]). *Letting $\varphi_v(x) : J = [a, b] \longrightarrow J$ be a parametric S-unimodal map with the unique maximum at $c \in (a, b)$ and $\varphi_v(c) = b$, $\forall v \in (v_{min}, v_{max})$, then $\varphi_v(x)$ generates robust chaos for $v \in (v_{min}, v_{max})$.*

Based on the above theorem, we set up the robust chaos theorem of cubic polynomial discrete maps.

Theorem 2. *Let a kind of cubic polynomial discrete maps have the following general form:*

$$f(x) = p_3x^3 + p_2x^2 + p_1x \tag{1}$$

If the parameters set $S = \{p_3, p_2, v\}$ this satisfies one of the following cases:

Case (1)

$$\begin{aligned} &p_3 > 0 \\ &p_2 < 0 \\ &v \geq \frac{25}{6} \\ &p_2^2 = vp_3p_1 \\ &p_1 = -\frac{27\left(1 - \sqrt{1 - 4/v}\right)}{v \cdot \left[4 - 18/v - 4\left(1 - 3/v\right)^{3/2}\right]} \end{aligned} \tag{2}$$

Case (2)

$$\begin{aligned} &p_3 < 0 \\ &p_2 > 0 \\ &v < 0 \\ &p_2^2 = vp_3p_1 \\ &p_1 = -\frac{27\left(1 + \sqrt{1 - 4/v}\right)}{v \cdot \left[4 - 18/v + 4\left(1 - 3/v\right)^{3/2}\right]} \end{aligned} \tag{3}$$

Case (3)

$$\begin{aligned} &p_3 < 0 \\ &p_2 < 0 \\ &v < 0 \\ &p_2^2 = vp_3p_1 \\ &p_1 = -\frac{27\left(1 - \sqrt{1 - 4/v}\right)}{v \cdot \left[4 - 18/v - 4\left(1 - 3/v\right)^{3/2}\right]} \end{aligned} \tag{4}$$

Then $f : J = [0, b] \longrightarrow J$ is the S-unimodal map. And it has the unique maximum at $c \in (0, b)$, and $f(c) = b$, $b = (-p_2 - \sqrt{p_2^2 - 4p_3p_1})/(2p_3)$, $c = (-p_2 - \sqrt{p_2^2 - 3p_3p_1})/(3p_3)$. f satisfies Theorem 1. That is, f is robust chaos. The proof progress is shown in the Appendix.

Three cases of robust chaos, respectively, correspond to the three surfaces. The robust chaos regions of case (1), (2) and (3) of the cubic polynomial discrete map are shown in Figure 1. The three surfaces are the robust chaos regions.

3. Comparison of Bifurcation and Cycle Lengths between the Cubic Polynomial Chaotic Map and Logistic Map

Based on the case (1) of Theorem 2, we construct a novel cubic polynomial discrete chaotic map:

$$x_{k+1} = p_3x_k^3 + p_2x_k^2 + p_1x_k \tag{5}$$

where $v = 5$, $p_1 = -\{27(1 - \sqrt{1 - 4/v})\}/\{v \cdot [4 - 18/v - 4(1 - 3/v)^{3/2}]\}$, $p_2 = -3$, $p_3 = p_2^2/(vp_1)$.

We consider Logistic map:

$$y_{k+1} = ay_k\left(1 - y_k\right) \tag{6}$$

where $a = 3.99$.

The evolution of state variables $k - x_k$ of the novel cubic polynomial discrete chaotic map with $v = 5$ is shown in Figure 2. The evolution of state variables $k - y_k$ of the Logistic map is shown in Figure 3. Extensive numerical simulations show that the dynamic behaviors of the chaotic map demonstrate chaotic attractor features.

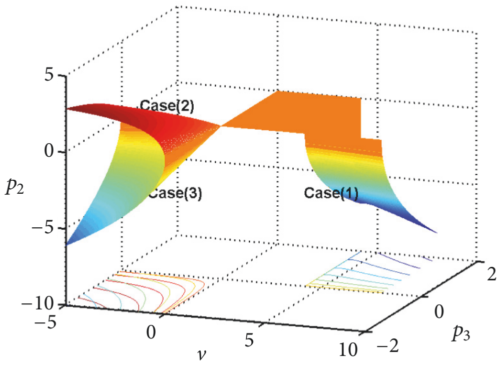


FIGURE 1: The robust chaos regions of cubic polynomial discrete map.

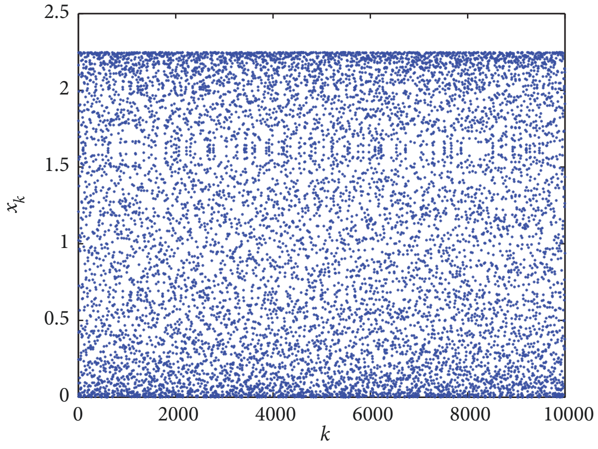


FIGURE 2: The evolution of state variables $k - x_k$.

3.1. Comparison of Bifurcation between the Cubic Polynomial Chaotic Map and Logistic Map. The calculated Lyapunov exponent of the chaotic maps (5) is 0.69135, which is bigger than 0.63927, and the Lyapunov exponent of Logistic map (6).

The chaotic map (5) is robust chaos for parameter $v > 25/6$ with $p_2 = -3$ from the case (1) of Theorem 2. The bifurcation diagram of the x as a function of the parameter v is shown in Figure 4.

In 2009, Zhou and Song set up a theorem for the necessary and sufficient condition of determination 3-periodic points of a quadratic polynomial.

Theorem 3 (see [24]). *A quadratic polynomial $f(x) = ax^2 + bx + c$ $(a \neq 0)$ has real 3-periodic points if and only if $b^2 - 4ac - 2b \geq 7$.*

Now we use the theorem to determine the parameter regions of robust chaos of Logistic map.

Proof. Let Logistic map $f(x) = -ax^2 + ax$, $0 < a < 4$, and $x \in I = [0, 1]$. Based on Theorem 3 and Li-Yorke's criterion that period three implies chaos, Logistic map is chaos if and only if

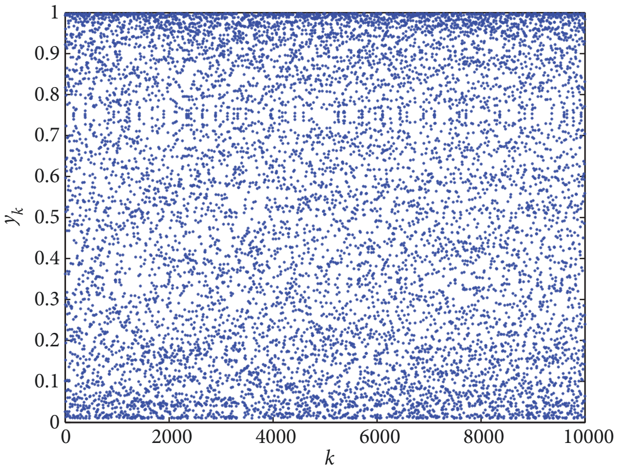


FIGURE 3: The evolution of state variables $k - y_k$.

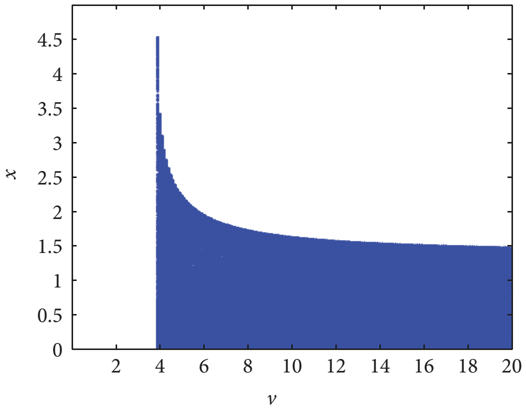


FIGURE 4: The bifurcation diagram showing the x as a function of the parameter v.

$$\begin{aligned} a^2 - 2a \geq 7 &\Longleftrightarrow \\ a &< 1 - 2\sqrt{2} \\ \text{or } a &> 1 + 2\sqrt{2} \end{aligned} \tag{7}$$

Thence Logistic map is chaos if and only if $1 + 2\sqrt{2} < a < 4$. □

The bifurcation diagram of Logistic map about the parameter a is shown in Figure 5. Logistic map is robust chaos for the parameter regions $a \in (1 + 2\sqrt{2}, 4)$. Compared with Logistic map, the bifurcation of chaotic map (5) is uniform distributed. And the cubic polynomial map is robust chaos for the parameter regions $v \in (25/6, +\infty)$ with $p_2 = -3$ from the case (1) of Theorem 2. Clearly, the parameter regions of robust chaos of the cubic polynomial discrete map are larger than these of Logistic map.

3.2. Comparison of Cycle Lengths between the Cubic Polynomial Chaotic Map and Logistic Map. When chaotic systems are realized under finite precision, the periodic cycles will

Table 1: Cycle lengths (CL) of the cubic polynomial chaotic map and Logistic map about resolutions.

resolutions		10^{-6}	10^{-7}	10^{-8}	10^{-9}	10^{-10}	10^{-11}	10^{-12}	10^{-13}	10^{-14}
Max CL	Map (5)	442	3,726	27,803	29,305	53,139	263,658	435,974	2,007,259	$> 3 \times 10^7$
	Map (6)	1,112	1,702	4,000	14,060	51,485	249,204	344,356	375,446	13,893,500
Mean CL	Map (5)	428	1,315	26,991	25,708	46,6337	220,644	177,736	1,599,595	11,960,668
	Map (6)	1,079	1,286	2,275	10,886	47,511	241,890	323,336	280,082	4,593,987
Min CL	Map (5)	63	71	820	1,525	4,417	24,689	80,581	878,343	4,593,987
	Map (6)	23	25	651	1,653	6,547	66,343	2,907	46,140	58,072

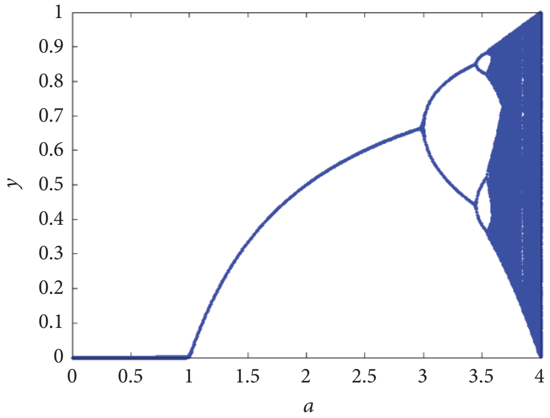


Figure 5: The bifurcation diagram of Logistic map about the parameter a.

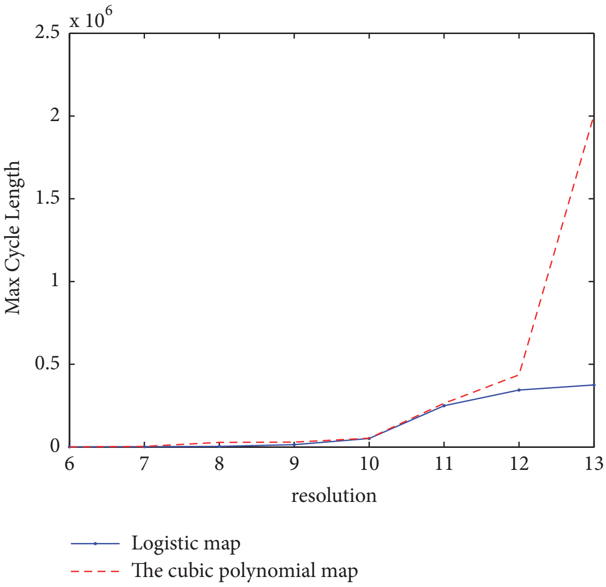


Figure 6: The change diagram of maximum of cycle lengths for different decimal resolutions from 6 to 13.

occur due to rounding errors. Reference [27] investigates the maximum cycle lengths of Logistic map with respect to different initial condition values.

Using the algorithm proposed in [27] for fixed point realizations analyzes the cycle lengths of the cubic polynomial chaotic map (5) and Logistic map (6). During analysis, 1000 uniformly distributed random initial condition values are used to generate 1000 chaotic sequences with length 3×10^7, where the resolutions are from 10^{-6} to 10^{-14}, and the rounding type selects rounded towards zero (fix) and regardless of the iteration to fixed point.

The maximum, mean, and minimum of the cycle lengths for the cubic polynomial chaotic sequences and Logistic sequences are listed in Table 1. The cycle lengths of chaotic sequences increase with the resolutions. When the resolution reaches 10^{-14}, there is the situation without cycle for 1000 cubic polynomial chaotic sequences with length 3×10^7. That is, the maximum of the cycle lengths for 1000 cubic polynomial chaotic sequences is larger than 3×10^7.

The change diagrams of maximum, mean, and minimum of cycle lengths are shown in Figures 6, 7, and 8, respectively. The red line represents the change of cycle lengths for the cubic polynomial chaotic map (5), and the blue line represents the change of cycle lengths for the Logistic map (6). According to the three figures, the maximum of cycle lengths exponentially increases with the resolutions. And the maximum of cycle lengths of cubic polynomial chaotic

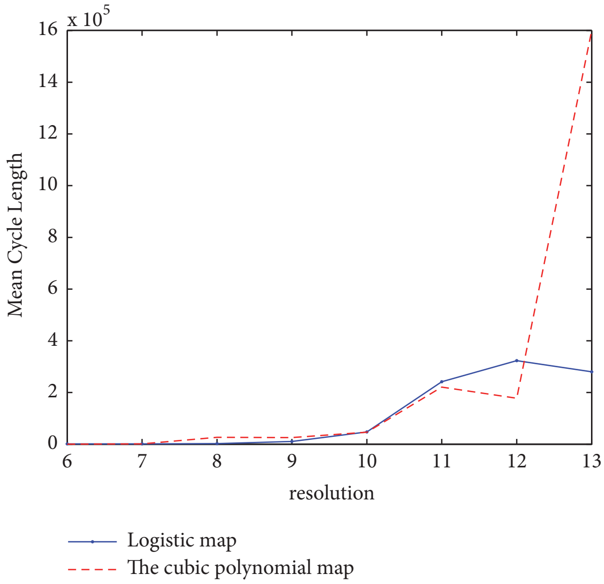


Figure 7: The change diagram of mean of cycle lengths for different decimal resolutions from 6 to 13.

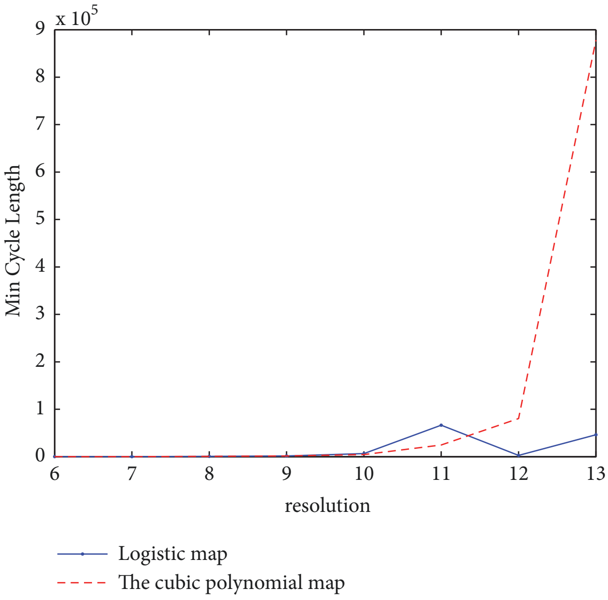


Figure 8: The change diagram of minimum of cycle lengths for different decimal resolutions from 6 to 13.

sequences is significantly larger than these of the Logistic sequences when resolutions are from 7 to 13.

4. 6-Dimensional Chaotic Generalized Synchronic Systems

Based on the cubic polynomial map (5) and the Logistic map (6), we consider the following 3-dimensional discrete chaotic map as the driving part:

$$\boldsymbol{X}(k+1)=\begin{bmatrix}x_1(k+1)\\x_2(k+1)\\x_3(k+1)\end{bmatrix}=\begin{bmatrix}p_3x_1(k)^3+p_2x_1(k)^2+p_1x_1(k)\\x_1(k)-2\sin(x_2(k))\sin(x_3(k))\\\sin(x_1(k))+2\sin(x_2(k)x_3(k))\end{bmatrix}\tag{8}$$

$$\boldsymbol{Z}(k+1)=\begin{bmatrix}z_1(k+1)\\z_2(k+1)\\z_3(k+1)\end{bmatrix}=\begin{bmatrix}3.99z_1(k)(1-z_1(k))\\z_1(k)-2\sin(z_2(k))\sin(z_3(k))\\\sin(z_1(k))+2\sin(z_2(k)z_3(k))\end{bmatrix}\tag{9}$$

where $v=5$, $p_1=-\{27(1-\sqrt{1-4/v})\}/\{v\cdot[4-18/v-4(1-3/v)^{3/2}]\}$, $p_2=-3$, and $p_3=p_2^2/(vp_1)$.

The calculated Lyapunov exponents of the chaotic map (8) are $\{0.69088, 0.39203, -0.81092\}$. The calculated Lyapunov exponents of the chaotic map (9) are $\{0.63823, 0.43349, -1.1883\}$.

In order to construct a GS driven system, define an invertible transformation : $\mathbb{R}^3\longrightarrow\mathbb{R}^3$:

$$H(\boldsymbol{X})=A\boldsymbol{X}\triangleq(h_1(\boldsymbol{X}),h_2(\boldsymbol{X}),h_3(\boldsymbol{X}))\tag{10}$$

$$H(\boldsymbol{Z})=A\boldsymbol{Z}\triangleq(h_1(\boldsymbol{Z}),h_2(\boldsymbol{Z}),h_3(\boldsymbol{Z}))\tag{11}$$

where

$$A=\begin{pmatrix}1&3&11\\2&4&-5\\-3&1&6\end{pmatrix}\tag{12}$$

is an invertible matrix. Now let the driven part have the form:

$$\boldsymbol{Y}(k+1)=\begin{bmatrix}y_1(k+1)\\y_2(k+1)\\y_3(k+1)\end{bmatrix}=\boldsymbol{AX}(k+1)-\frac{1}{7}(\boldsymbol{AX}(k)-\boldsymbol{Y}(k))\tag{13}$$

$$\boldsymbol{W}(k+1)=\begin{bmatrix}w_1(k+1)\\w_2(k+1)\\w_3(k+1)\end{bmatrix}=\boldsymbol{AZ}(k+1)-\frac{1}{7}(\boldsymbol{AZ}(k)-\boldsymbol{W}(k))\tag{14}$$

From (13) and (14), it follows that the error equations $q(\boldsymbol{X},\boldsymbol{Y})$ and $q(\boldsymbol{Z},\boldsymbol{W})$ can be represented by $\boldsymbol{e}(k)/7=(1/7)(\boldsymbol{AX}(k)-\boldsymbol{Y}(k))$ and $\boldsymbol{e}(k)/7=(1/7)(\boldsymbol{AZ}(k)-\boldsymbol{W}(k))$. It guarantees that the zero solution of the error equation is asymptotically stable. From the chaos generalized synchronization (GS) theorem [28], systems (8) and (13) as well as (9) and (14) are GS with respect to the transformation $\boldsymbol{H}=A$ for any initial value $(\boldsymbol{X}(0),\boldsymbol{Y}(0))\in\mathbb{R}^3\times\mathbb{R}^3$ and $(\boldsymbol{Z}(0),\boldsymbol{W}(0))\in\mathbb{R}^3\times\mathbb{R}^3$. Since H is invertible, systems (13) and (14) are also chaotic.

4.1. Numerical Simulations. Select the following initial conditions:

$$\boldsymbol{X}(0)=\boldsymbol{Z}(0)=(0.3,0.01,0.1)^T\tag{15}$$

$$\boldsymbol{Y}(0)=A\boldsymbol{X}(0)+1\tag{16}$$

$$\boldsymbol{W}(0)=A\boldsymbol{Z}(0)+1\tag{17}$$

The chaotic orbits of the state variables $\{x_1,x_2,x_3\}$ for the first 5000 iterations are shown in Figures 9(a)–9(d). The evolutions of the state variables, $k-x_1(k)$, $k-x_2(k)$, and $k-x_3(k)$, are shown in Figures 10(a)–10(c). The chaotic orbits of the state variables $\{y_1,y_2,y_3\}$ for the first 5000 iterations are shown in Figures 11(a)–11(d). The evolutions of the state variables, $k-y_1(k)$, $k-y_2(k)$, and $k-y_3(k)$, are shown in Figures 12(a)–12(c). The dynamic behaviors of the chaotic map demonstrate chaotic attractor characteristics. Figures 13(a)–13(c) show that although the initial condition

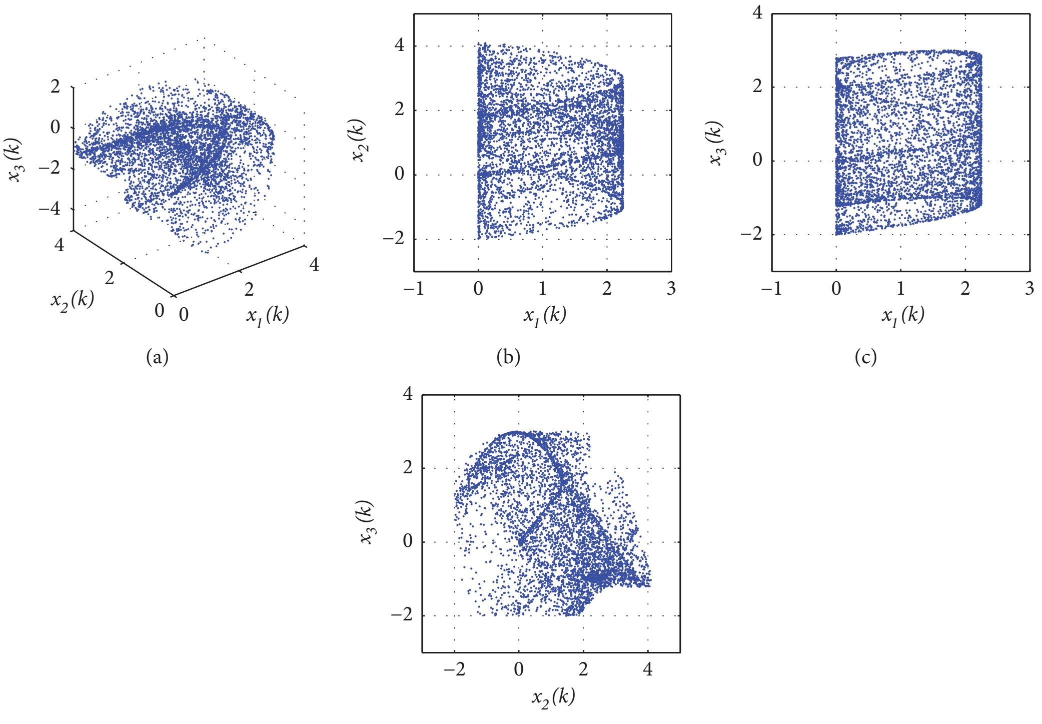


FIGURE 9: Chaotic trajectories of variables: (a) $x_1(k) - x_2(k) - x_3(k)$, (b) $x_1(k) - x_2(k)$, (c) $x_1(k) - x_3(k)$, and (d) $x_2(k) - x_3(k)$.

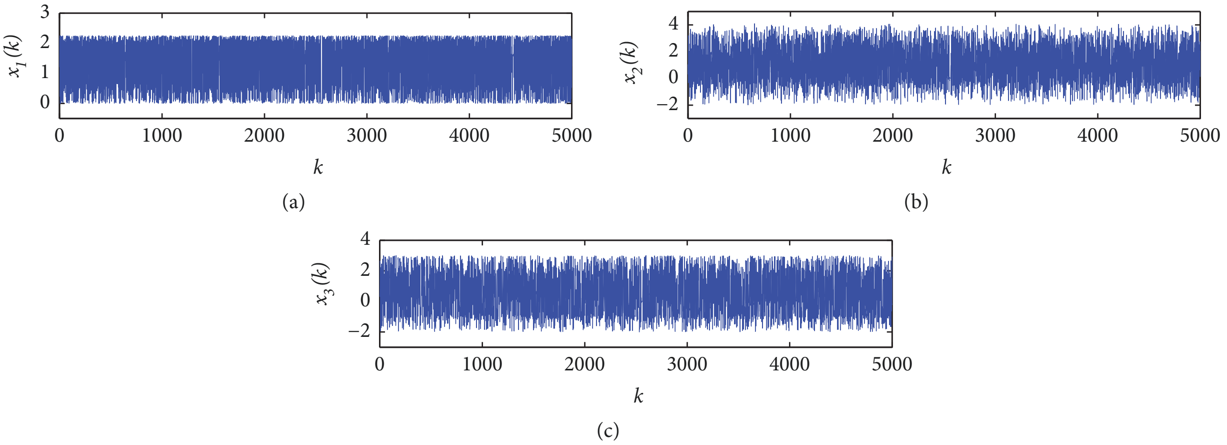


FIGURE 10: The evolution of state variables: (a) $k - x_1(k)$, (b) $k - x_2(k)$, and (c) $k - x_3(k)$.

(16) has a perturbation, $\boldsymbol{X}(k)$ and $\boldsymbol{Y}(k)$ are rapidly converting into generalized synchronization as the chaos GS theorem predicts.

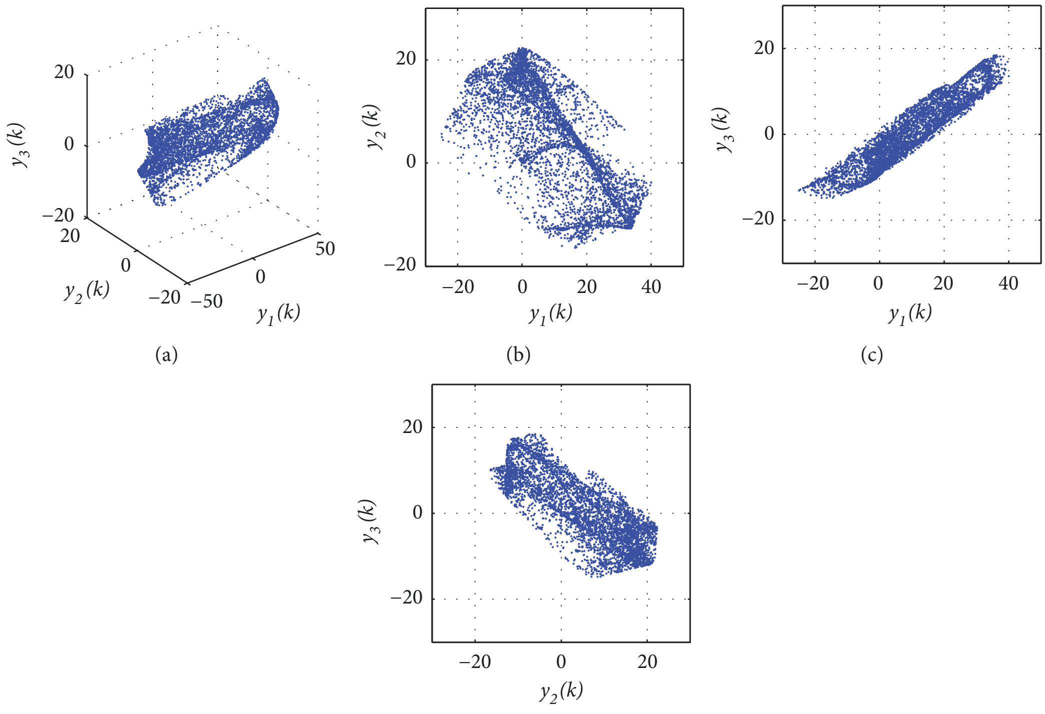
The chaotic orbits of the state variables $\{z_1, z_2, z_3\}$ for the first 5000 iterations are shown in Figures 14(a)–14(d). The evolutions of the state variables, $k - z_1(k)$, $k - z_2(k)$, and $k - z_3(k)$, are shown in Figures 15(a)–15(c). The chaotic orbits of the state variables $\{w_1, w_2, w_3\}$ for the first 5000 iterations are shown in Figures 16(a)–16(d). The evolutions of the state variables, $k - w_1(k)$, $k - w_2(k)$, and $k - w_3(k)$, are shown in Figures 17(a)–17(c). The dynamic behaviors of the chaotic map demonstrate chaotic attractor characteristics. Observe that Figures 18(a)–18(c) show that although the initial condition (17) has a perturbation, $\boldsymbol{Z}(k)$ and $\boldsymbol{W}(k)$ are rapidly converting into generalized synchronization as the chaos GS theorem predicts.

5. Chaotic Pseudorandom Number Generator and Pseudorandomness Tests

5.1. Chaotic Pseudorandom Number Generator. Denote

$$\boldsymbol{X}_i = \{x_i(k) \mid k = 1, 2, \ldots, N\} \quad (18)$$

$$\boldsymbol{Y}_i = \{y_i(k) \mid k = 1, 2, \ldots, N\} \quad (19)$$



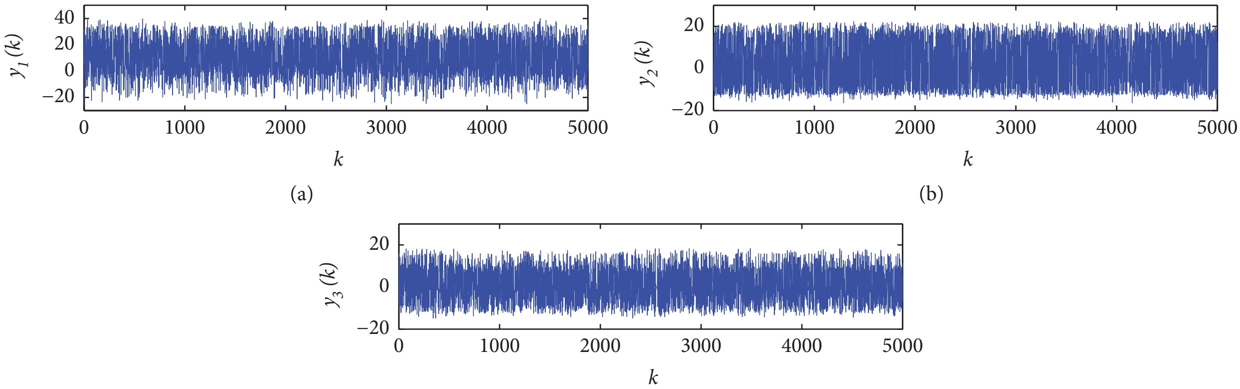
(a)

(b)

(c)

(d)

FIGURE 11: Chaotic trajectories of variables: (a) $y_1(k) - y_2(k) - y_3(k)$, (b) $y_1(k) - y_2(k)$, (c) $y_1(k) - y_3(k)$, and (d) $y_2(k) - y_3(k)$.



(a)

(b)

(c)

FIGURE 12: The evolution of state variables: (a) $k - y_1(k)$, (b) $k - y_2(k)$, and (c) $k - y_3(k)$.

$$\boldsymbol{Z}_i = \{z_i(k) \mid k = 1, 2, \ldots, N\} \tag{20}$$

$$\boldsymbol{W}_i = \{w_i(k) \mid k = 1, 2, \ldots, N\} \tag{21}$$

where $i = 1, 2, 3$, $x_i's$ and $y_i's$ are defined by (8) and (13), and $z_i's$ and $w_i's$ are defined by (9) and (14).

First, introduce transformations T_{11}, T_{12}, T_{13}, and T_{14}: $\mathbb{R} \longrightarrow \{0, 1, \ldots, 2^8 - 1\}$ which transform the chaotic streams of GS systems (18) and (19) as well as (20) and (21) into key streams.

$$T_{11}(\boldsymbol{X}_1) = \operatorname{mod}\left(round\left(L\frac{\boldsymbol{X}_1 - \min(\boldsymbol{X}_1)}{\max(\boldsymbol{X}_1) - \min(\boldsymbol{X}_1)}, 2^8\right)\right) \tag{22}$$

$$T_{12}(\boldsymbol{Y}_1) = \operatorname{mod}\left(round\left(L\frac{\boldsymbol{Y}_1 - \min(\boldsymbol{Y}_1)}{\max(\boldsymbol{Y}_1) - \min(\boldsymbol{Y}_1)}, 2^8\right)\right) \tag{23}$$

$$T_{13}(\mathbf{S}) = \operatorname{mod}\left(round\left(L\frac{\mathbf{S} - \min(\mathbf{S})}{\max(\mathbf{S}) - \min(\mathbf{S})}, 2^8\right)\right) \tag{24}$$

$$T_{14}(\overline{\mathbf{S}}) = \operatorname{mod}\left(round\left(L\frac{\overline{\mathbf{S}} - \min(\overline{\mathbf{S}})}{\max(\overline{\mathbf{S}}) - \min(\overline{\mathbf{S}})}, 2^8\right)\right) \tag{25}$$

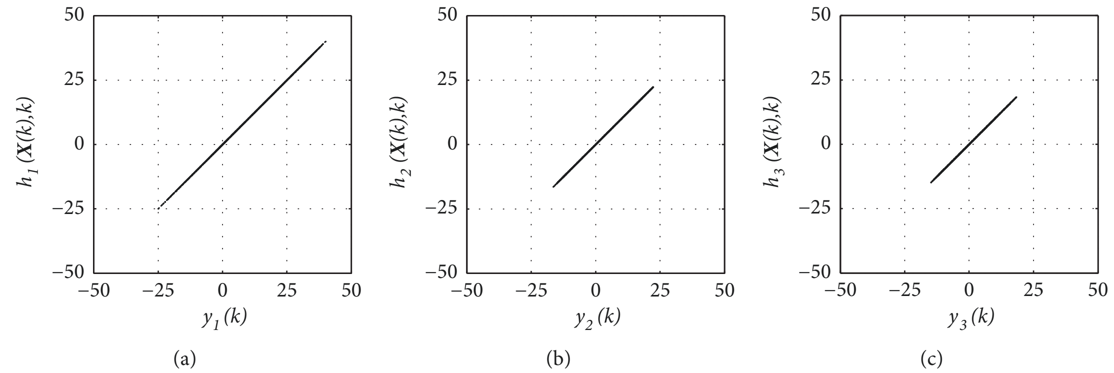


FIGURE 13: The state vectors $\mathbf{X}$ and $\mathbf{Y}$ are in generalized synchronization with respect to the transformation H: (a) $h_1(\mathbf{X}(k))$-$y_1(k)$, (b) $h_2(\mathbf{X}(k))$-$y_2(k)$, and (c) $h_3(\mathbf{X}(k))$-$y_3(k)$.

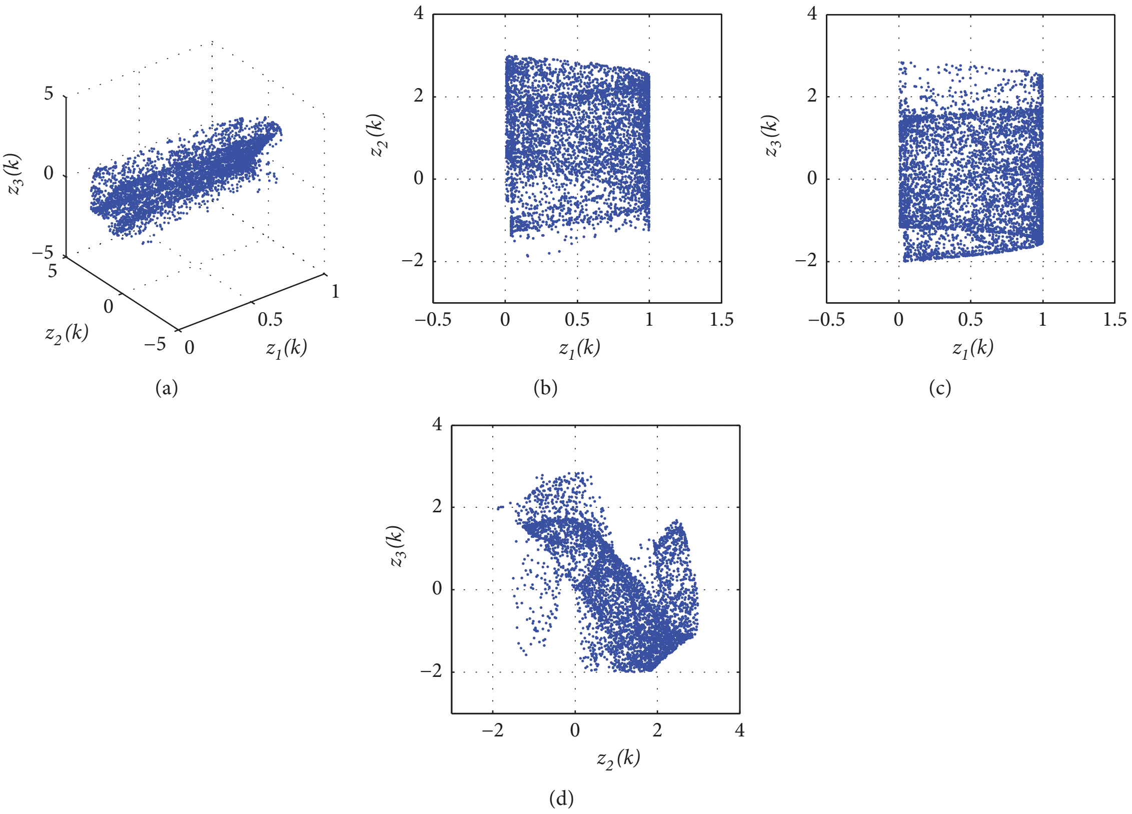


FIGURE 14: Chaotic trajectories of variables: (a) $z_1(k) - z_2(k) - z_3(k)$, (b) $z_1(k) - z_2(k)$, (c) $z_1(k) - z_3(k)$, and (d) $z_2(k) - z_3(k)$.

Here

$$\mathbf{S} = \left|\mathbf{X}_1 * \mathbf{X}_2 + \mathbf{X}_3 * \mathbf{Y}_1 - \mathbf{Y}_2\right| \tag{26}$$

$$\overline{\mathbf{S}} = \left|\mathbf{Z}_1 * \mathbf{Z}_2 + \mathbf{Z}_3 * \mathbf{W}_1 - \mathbf{W}_2\right| \tag{27}$$

where $L = 10^{15}$, $\mathbf{X} * \mathbf{Y}$ represents the dot product of vectors $\mathbf{X}$ *and* $\mathbf{Y}$, and $\mathbf{Z} * \mathbf{W}$ represents the dot product of vectors $\mathbf{Z}$ *and* $\mathbf{W}$.

Second, construct a transform T_2: $\{0, 1, \ldots, 2^8 - 1\} \longrightarrow \{0, 1\}$ which is defined by

$$T_2 = T_{22} \circ T_{21} \tag{28}$$

s.t. $\forall \boldsymbol{y} \in \{0, 1, \ldots, 2^8 - 1\}^N$

$$T_{21}(\boldsymbol{y}) = dec2bin(\boldsymbol{y}) \tag{29}$$

Letting $\boldsymbol{z} = dec2bin(\mathbf{Y})$, then

$$T_{22}(\boldsymbol{z}) = \boldsymbol{z}(:) \tag{30}$$

where dec2bin and $\boldsymbol{z}(:)$ are both Matlab commands.

Finally, transformations $\overline{T}_1, \overline{T}_2, \overline{T}_3$, and $\overline{T}_4 : \mathbb{R}^3 \longrightarrow \{0, 1\}$ are defined via

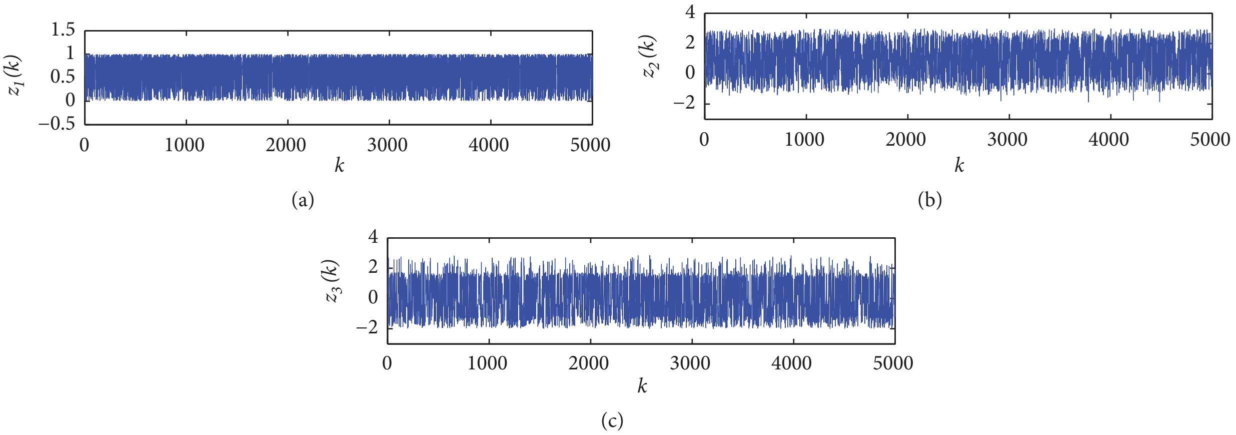


FIGURE 15: The evolution of state variables: (a) $k - z_1(k)$, (b) $k - z_2(k)$, and (c) $k - z_3(k)$.

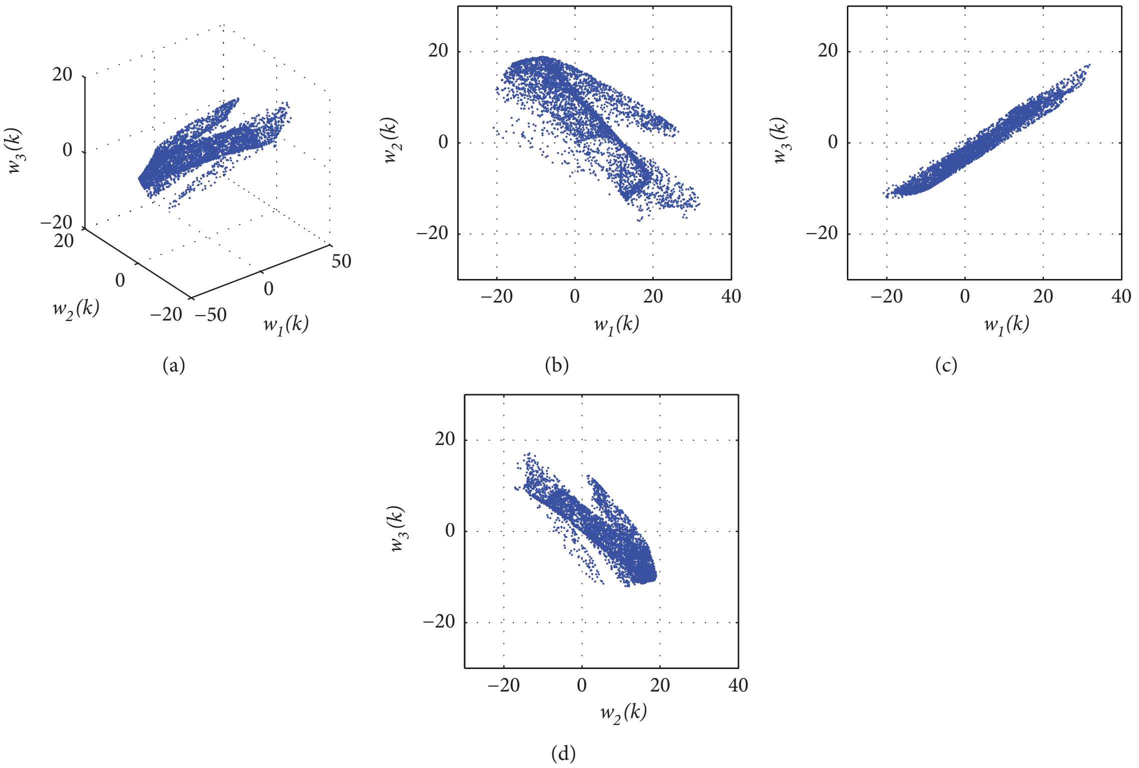


FIGURE 16: Chaotic trajectories of variables: (a) $w_1(k) - w_2(k) - w_3(k)$, (b) $w_1(k) - w_2(k)$, (c) $w_1(k) - w_3(k)$, and (d) $w_2(k) - w_3(k)$.

$$\overline{T}_1 = T_2 \circ T_{11} \quad (31)$$

$$\overline{T}_2 = T_2 \circ T_{12} \quad (32)$$

$$\overline{T}_3 = T_2 \circ T_{13} \quad (33)$$

$$\overline{T}_4 = T_2 \circ T_{14} \quad (34)$$

Now, based on the cubic polynomial chaotic map (5) and Logistic map (6), we design CPRNGI, CPRNGII, CPRNGIIII, and CPRNGIV.

$$\overline{S}_1 = \overline{T}_1 (\boldsymbol{X}_1) \quad (35)$$

$$\overline{S}_2 = \overline{T}_2 (\boldsymbol{Y}_1) \quad (36)$$

$$\overline{S}_3 = \overline{T}_3 (\boldsymbol{S}) \quad (37)$$

$$\overline{S}_4 = \overline{T}_4 (\overline{\boldsymbol{S}}) \quad (38)$$

are the key streams, respectively, generated via CPRNGI, CPRNGII, CPRNGIIII, and CPRNGIV.

5.2. Pseudorandomness Tests. The FIPS 140-2 test consists of four subtests: Monobit Test, Poker Test, Run Test, and Long Run Test. Each test needs a single stream of 20,000 one and

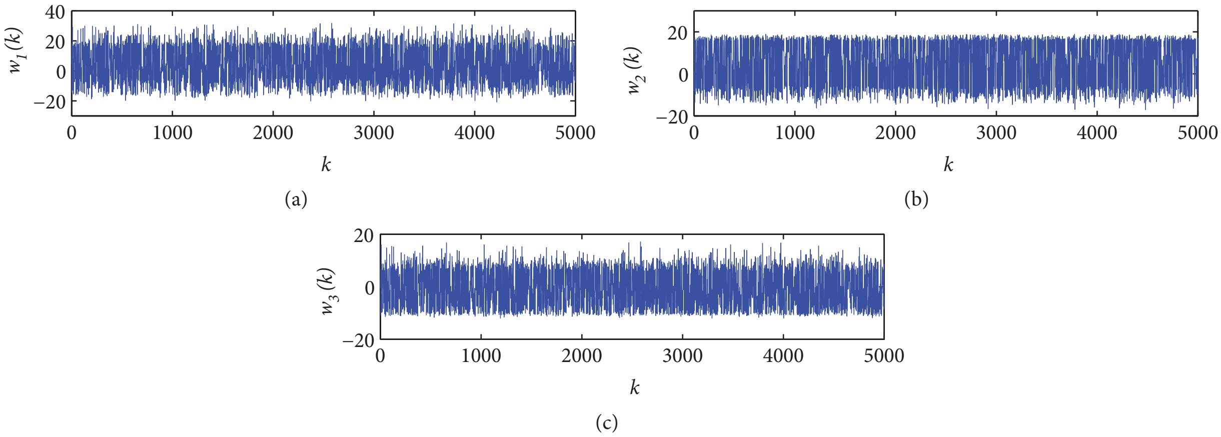


FIGURE 17: The evolution of state variables: (a) $k - w_1(k)$, (b) $k - w_2(k)$, and (c) $k - w_3(k)$.

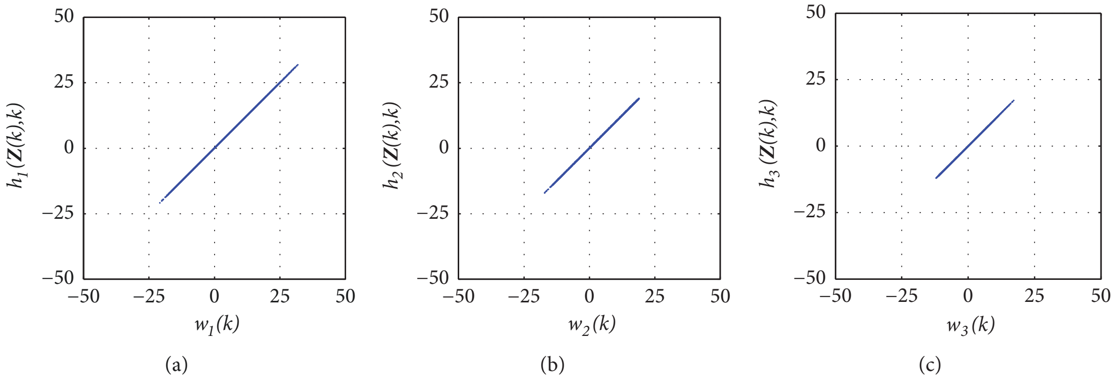


FIGURE 18: The state vectors $\boldsymbol{Z}$ and $\boldsymbol{W}$ are in generalized synchronization with respect to the transformation: (a) $h_1(\mathbf{Z}(k))$-$w_1(k)$, (b) $h_2(\mathbf{Z}(k))$-$w_2(k)$, and (c) $h_3(\mathbf{Z}(k))$-$w_3(k)$.

zero bits from the keystream generator. Any failure in the first three tests means that the corresponding quantity of the sequences falls out the required intervals listed in the second column in Table 2. The Long Run test is passed if there are no runs of length 26 or more.

It has been pointed out that the required intervals of the Monotone test and the Pork test correspond significantly to $\alpha = 10^{-4}$ for the normal cumulative distribution and the χ^2 distribution, respectively, and the required intervals of the Run tests correspond approximately the significant $\alpha = 1.6 \times 10^{-7}$ for the normal cumulative distribution [29, 30]. If we select the significant $\alpha = 10^{-4}$ of all tests, the corresponding accepted intervals are listed in the third column in Table 2. According to Golomb's three postulates on the randomness that ideal pseudorandom sequences should satisfy [31], and the ideal values of the first three tests should be those listed in the 4th column in Table 2.

The FIPS 140-2 test is used to check 1,000 keystreams randomly generated, respectively, by CPRNGI, CPRNGII, CPRNGIIII, and CPRNGIV, with perturbed randomly the parameters, the initial conditions $\boldsymbol{X}(0)$, $\boldsymbol{Y}(0)$, $\boldsymbol{Z}(0)$, and $\boldsymbol{W}(0)$, and the parameters of matrix $A = (\alpha_{i,j})$ in the range $|\epsilon| \in [10^{-16}, 10^{-1}]$. The test results are listed in the 2/3/4/5th column in Table 3. The statistic test results are listed in the 3/4/5/6th column in Table 4, in which the statistic results are described by mean values and standard deviation (Mean±SD).

The RC4 was designed by Rivest of the RSA Security in 1987, which has been widely used in popular protocols such as Secure Sockets. The RC4 Algorithm PRNG can be designed via Matlab commands:

$$N = 20000;$$

$$K = randi\left(\left[0 \quad 254\right], 1, 255\right);$$

$$S = [0 : 255 - 1]; \; j = 0;$$

$$for \; i = 1 : 255$$

$$j = \operatorname{mod}\left(j + S(i) + K(i), 255\right);$$

$$Sk = S\left(j + 1\right);$$

$$S\left(j + 1\right) = S(i);$$

$$S(i) = Sk;$$

$$end$$

$$C = zeros(1, N); \; j = 0; \; i = 0; \; k = 1;$$

Table 2: The required intervals of the FIPS 140-2 Monobit Test, Pork Tests, and Run Test. Here, MT, PT, and LT represent the Monobit Test, the Pork Test, and the Long Run Test, respectively. k represents the length of the run of a tested sequence. χ^2 DT represents χ^2 distribution.

Test Item	FIPS 140-2	$\alpha = 10^{-4}$	Golomb's
	Required Intervals	Accepted Intervals	Postulates
MT	9,725~10,275	9,725~10,275	10000
PT	2.16~46.17	2.16~46.17	χ^2 DT
LT	< 26	< 26	—
k	Run Test	Run Test	
1	2,315~2,685	2,362~2,638	2,500
2	1,114~1,386	1,153~1,347	1,250
3	527~723	556~694	625
4	240~384	264~361	313
5	103~209	122~191	156
6+	103~209	122~191	156

Table 3: The pass rate of CPRNGI/CPRNGII/CPRNGIII/CPRNGIV.

Pass rate	CPRNGI	CPRNGII	CPRNGIII	CPRNGIV	RC4
FIPS 140-2	100%	99.7%	100%	100%	99.9%
G FIPS 140-2 test	97.9%	98.0%	98.8%	98.4%	98.2%

$$\begin{aligned}
&for\ l = 1 : \frac{N}{8} \\
&i = \operatorname{mod}(i+1, 255); \\
&j = \operatorname{mod}\left(j + S(i+1), 255\right); \\
&Sk = S\left(j+1\right); \\
&S\left(j+1\right) = S(i+1); \\
&S(i+1) = Sk; \\
&C(l) = S\left(\operatorname{mod}\left(S\left(j+1\right) + S(i+1), 255\right) + 1\right); \\
&end \\
&C = (dec2bin(C))'; \\
&C = C(:); \\
&C = bin2dec(C);
\end{aligned} \tag{39}$$

where randi($[0\ 2^L-1],1,2^L$) generates a vector of uniformly distributed random integers $\{0, 1, \ldots, 2^L-1\}$ of dimension 2^L; mod means modulus after division; zeros$(1, N)$ is a zero raw vector of dimension N.

Consequently, the RC4 Algorithm based PRNG is designed. The FIPS 140-2 test is used to test the 1,000 keystreams randomly generated by RC4. The test result is listed in the 6th column in Table 3. The statistic test results are listed in the 7th column in Table 4. Observe that the statistical properties of the pseudorandomness of the sequences generated via the four CPRNGs and RC4 do not have significant differences. And compared with the other three CPRNSs, CPRNGIII based on the cubic polynomial chaotic generalized synchronic system has better performance.

5.3. Key Space. The key set parameters of CPRNGs includes the parameters $\{v, p_2, p_3, a\}$, the initial conditions $\boldsymbol{X}(0)$, $\boldsymbol{Y}(0)$, $\boldsymbol{Z}(0)$, and $\boldsymbol{W}(0)$, and the matrix $A = (\alpha_{i,j})$. It can be proved that if the perturbation matrix $\triangle = (\delta_{i,j})$ satisfies

$$\left|\delta_{i,j}\right| < 0.86 \tag{40}$$

the matrix $A + \triangle$ is still invertible. Therefore CPRNGI, CPRNGII, CPRNGIIII, and CPRNGIV, respectively, have $1 + 1$, $1+1$, $3+3+3+9$, $1+3+3+9$ key parameters denoted by

$$\mathbf{K}_{s1} = \left\{k_1, k_2\right\} \tag{41}$$

$$\mathbf{K}_{s2} = \left\{k_1, k_2\right\} \tag{42}$$

$$\mathbf{K}_{s3} = \left\{k_1, k_2, \ldots, k_{18}\right\} \tag{43}$$

$$\mathbf{K}_{s4} = \left\{k_1, k_2, \ldots, k_{16}\right\} \tag{44}$$

Let the key set be perturbed by

$$\mathbf{K}_{s1}(\Delta) = \mathbf{K}_{s1} + \left[\delta_1, \delta_2\right] \tag{45}$$

$$\mathbf{K}_{s2}(\Delta) = \mathbf{K}_{s2} + \left[\delta_1, \delta_2\right] \tag{46}$$

$$\mathbf{K}_{s3}(\Delta) = \mathbf{K}_{s3} + \left[\delta_1, \delta_2, \ldots, \delta_{18}\right] \tag{47}$$

$$\mathbf{K}_{s4}(\Delta) = \mathbf{K}_{s4} + \left[\delta_1, \delta_2, \ldots, \delta_{16}\right] \tag{48}$$

where

$$10^{-16} \leq \left|\delta_i\right| \leq 10^{-1}, \quad i = 1, \ldots, 16. \tag{49}$$

Table 4: The confident intervals of the FIPS 140-2 tested values of 1,000 key streams generated by CPRNGI/CPRNGII/CPRNGIII/CPRNGIV. Here, SD represents the standard deviation.

Test item	bits	CPRNGI	CPRNGII	CPRNGIII	CPRNGIV	RC4
		Mean ± SD	Mean ± SD	Mean ± SD	Mean ± SD	Mean ± SD
MT	0	10007±69.605	10007± 71.590	10006±73.058	10007±71.965	9993.2±65.772
	1	9992.7 ± 69.605	9992.9±71.590	9993.1 ± 73.058	9992.4±71.965	10007±65.677
PT	–	15.098± 5.6493	15.144 ± 5.6130	15.188± 5.5703	15.197 ± 5.6712	14.874± 5.8308
LT	0	17.994 ±1.8567	18.142 ± 2.0430	13.908 ± 1.9165	13.864 ± 1.9388	13.900 ± 1.9201
	1	13.611 ± 1.8447	13.665 ± 1.9116	13.732 ± 2.0194	13.669 ± 1.9367	13.510±1.7085
k	bits	Run Test	Run Test	Run Test	Run Test	Run Test
1	0	2497.6±47.004	2497.4± 44.510	2495.3±46.303	2499.3± 48.263	2502.1±45.931
	1	2497.9± 47.282	2499.1± 46.161	2500.4± 47.228	2501.3± 4533.9	2499.3±46.735
2	0	1247.6±32.124	1248.4± 31.254	1251.0±31.376	1249.8± 31.976	1249.1±33.562
	1	1248.6±32.918	1248.2± 31.182	1246.7±32.313	1248.7± 32.022	1246.5 ±31.876
3	0	625.46±23.377	624.51± 22.498	624.52±23.838	623.57± 22.549	623.59±22.079
	1	624.95±23.373	623.06± 23.493	623.92±22.571	624.13± 22.838	625.66±25.016
4	0	312.53±16.690	312.44±15.625	312.20±16.847	312.21±16.735	312.23±15.121
	1	312.04± 16.512	311.96± 16.467	312.99± 16.423	311.91± 170.34	314.11±16.823
5	0	155.77±12.108	155.69±12.158	155.72±12.042	155.86±12.212	156.61±10.409
	1	156.02±12.011	156.64± 11.485	155.64±11.737	156.53± 12.220	156.96±12.530
6^+	0	156.69±12.031	157.01±12.004	157.47±11.758	157.67±11.880	156.32±13.331
	1	156.14±11.644	156.45±11.971	156.59±11.684	155.69±12.010	156.39±11.715

Therefore the key spaces of the four CPRNGs are, respectively, $10^{15\times 2}$, $10^{15\times 2}$, $10^{15\times 18}$, and $10^{15\times 16}$. The key space of CPRNGIII is larger than 2^{896}.

6. Conclusions

First, based on the robust chaos theorem of S-unimodal maps, this paper sets up a robust chaos theorem on a kind of cubic polynomial discrete maps. This theorem provides parameter inequalities to determine the robust chaos regions.

Second, using the Theorem 2 constructs a cubic polynomial map. The analysis results of the cycle lengths of 1000 cubic polynomial chaotic sequences show that when the resolutions reach $10^{-7} \sim 10^{-13}$, the maximum of cycle lengths of the cubic polynomial chaotic sequences is significantly greater than these of Logistic map. When the resolution reaches 10^{-14}, there is the situation without cycle for 1000 cubic polynomial chaotic sequences with length 3×10^7. The maximum of cycle lengths of Logistic sequences is less than 3×10^7.

Third, combining the robust chaos Theorems 2 and 3 and GS theorem proposes two 6DCGSS. The numerical simulations of two 6DCGSS have verified the effectiveness of theoretical results.

Finally, design four chaos-based pseudorandom number generators CPRNGI, CPRNGII, CPRNGIII, and CPRNGIV. Comparing the results of the FIPS 140-2 test for the keystreams generated via the four CPRNGs with the RC4 PRNG shows that the randomness of the sequences generated via the CPRNGIII has better performance. The simulations also suggest that the key space of the CPRNGIII is larger than 2^{896}, which is large enough to against brute-force attacks.

Appendix

Proof of Theorem 2. Case(1). First, we show that $f(x) : J = [0, b] \longrightarrow J$ has three order derivative function and $c \in (0, b)$ is the unique maximum point.

We now judge the symbol of $p_1 = -27(1 - \sqrt{1 - 4/v})/\{v \cdot [4 - 18/v - 4(1 - 3/v)^{3/2}]\}$.

(1) If $25/6 \le v \le 18/4$ implies

$$0 < 1 - \frac{4}{v} < 1,$$
$$-\frac{8}{25} \le 4 - \frac{18}{v} \le 0, \tag{A.1}$$
$$4\left(1 - \frac{3}{v}\right)^{3/2} > 0$$

then $4 - 18/v - 4(1 - 3/v)^{3/2} < 0$, $p_1 > 0$.

(2) If $v > 18/4$ implies

$$1 - \frac{4}{v} > 0,$$
$$4 - \frac{18}{v} > 0, \tag{A.2}$$
$$4\left(1 - \frac{3}{v}\right)^{3/2} > 0$$

then the judgement of $4 - 18/v - 4(1 - 3/v)^{3/2}$ is equivalent to the judgement of $(4 - 18/v)^2 - [4(1 - 3/v)^{3/2}]^2$.

Letting

$$\begin{aligned}&\left(4-\frac{18}{v}\right)^2-16\left(1-\frac{3}{v}\right)^3\\&=16-8\cdot\frac{18}{v}+\frac{18^2}{v^2}-16\left(1-\frac{9}{v}+\frac{27}{v^2}-\frac{27}{v^3}\right)\\&=-18\cdot\frac{6}{v^2}+16\cdot\frac{27}{v^3}<0\end{aligned} \tag{A.3}$$

then $4-18/v-4(1-3/v)^{3/2}<0,\ p_1>0$.

From $b=(-p_2-\sqrt{p_2^2-4p_3p_1})/(2p_3)$, $c=(-p_2-\sqrt{p_2^2-3p_3p_1})/(3p_3)$, $p_3>0$, $p_2<0$, $p_1>0$, and $p_2^2-3p_3p_1>p_2^2-4p_3p_1>0$, then

$$\begin{aligned}b-c&=\frac{-p_2-\sqrt{p_2^2-4p_3p_1}}{2p_3}-\frac{-p_2-\sqrt{p_2^2-3p_3p_1}}{3p_3}\\&=\frac{-3p_2-3\sqrt{p_2^2-4p_3p_1}+2p_2+2\sqrt{p_2^2-3p_3p_1}}{6p_3}\\&=\frac{-p_2-3\sqrt{p_2^2-4p_3p_1}+2\sqrt{p_2^2-3p_3p_1}}{6p_3}\\&>\frac{-p_2-3\sqrt{p_2^2-4p_3p_1}+2\sqrt{p_2^2-4p_3p_1}}{6p_3}\\&=\frac{-p_2-\sqrt{p_2^2-4p_3p_1}}{6p_3}>\frac{-p_2-|p_2|}{6p_3}=0\end{aligned} \tag{A.4}$$

Thence $0<c<b$.

Clearly, $f(x):J=[0,b]\longrightarrow J$ has three-order derivative function:

$$f'(x)=3p_3x^2+2p_2x+p_1 \tag{A.5}$$

$$f''(x)=6p_3x+2p_2 \tag{A.6}$$

$$f'''(x)=6p_3 \tag{A.7}$$

and c is the solution of $f'(x)=0$.

Since

$$\begin{aligned}f''(c)&=6p_3\cdot\frac{-p_2-\sqrt{p_2^2-3p_3p_1}}{3p_3}+2p_2\\&=-2p_2-2\sqrt{p_2^2-3p_3p_1}+2p_2\\&=-2\sqrt{p_2^2-3p_3p_1}<0\end{aligned} \tag{A.8}$$

then c is the maximum point.

Second, we proof $f(0)=f(b)=0$, and $f(x)$ is strictly increasing on $x\in(0,c)$ and strictly decreasing on $x\in(c,b)$.

Letting

$$\begin{aligned}f(x)&=p_3x^3+p_2x^2+p_1x\\&=p_3x\left(x^2+\frac{p_2}{p_3}\cdot x+\frac{p_1}{p_3}\right)=0\end{aligned} \tag{A.9}$$

it has three solutions:

$$\begin{gathered}0,\\b=\frac{\left(-p_2-\sqrt{p_2^2-4p_3p_1}\right)}{(2p_3)},\\x_1=\frac{\left(-p_2+\sqrt{p_2^2-4p_3p_1}\right)}{(2p_3)}\end{gathered} \tag{A.10}$$

and $b<x_1$, then $f(0)=f(b)=0$.

Solving $f'(x)=0$ has the other solution:

$$c_1=\frac{\left(-p_2+\sqrt{p_2^2-3p_3p_1}\right)}{(3p_3)} \tag{A.11}$$

Since $p_2^2=vp_3p_1$, $v>25/6$, $p_2<0$, $p_2^2-3p_3p_1>p_2^2-4p_3p_1$, then

$$\begin{aligned}&b-c_1\\&=\frac{-p_2-\sqrt{p_2^2-4p_3p_1}}{2p_3}-\frac{-p_2+\sqrt{p_2^2-3p_3p_1}}{3p_3}\\&=\frac{-3p_2-3\sqrt{p_2^2-4p_3p_1}+2p_2-2\sqrt{p_2^2-3p_3p_1}}{6p_3}\\&=\frac{-p_2-3\sqrt{p_2^2-4p_3p_1}+2\sqrt{p_2^2-3p_3p_1}}{6p_3}\\&<\frac{-p_2-5\sqrt{p_2^2-4p_3p_1}}{6p_3}\\&=\frac{-p_2-5|p_2|\sqrt{1-4/v}}{6p_3}=\frac{-p_2+5p_2\sqrt{1-4/v}}{6p_3}\\&=\frac{p_2\left(5\sqrt{1-4/v}-1\right)}{6p_3}<0\end{aligned} \tag{A.12}$$

thence $b<c_1$. Since c is the unique maximum at $J=[0,b]$ and $f(0)=f(b)=0$, then $f(x)$ is strictly increasing on $x\in(0,c)$ and strictly decreasing on $x\in(c,b)$.

Third, we proof $f(x)$ has negative Schwarzian derivative on J. For every $x \in J$

$$\begin{aligned} S_f &= \frac{f'''}{f'} - \frac{3}{2}\left(\frac{f''}{f'}\right)^2 \\ &= \frac{6p_3}{3p_3x^2 + 2p_2x + p_1} - \frac{3}{2}\left(\frac{6p_3x + 2p_2}{3p_3x^2 + 2p_2x + p_1}\right)^2 \\ &= \frac{12 \cdot p_3\left(3p_3x^2 + 2p_2x + p_1\right) - 3\left(6p_3x + 2p_2\right)^2}{2\left(3p_3x^2 + 2p_2x + p_1\right)^2} \\ &= \frac{6\left(3p_3^3x^2 + 2p_3p_2x + p_3p_1\right) - 6\left(9p_3^2x^2 + 6p_3p_2x + p_2^2\right)}{\left(3p_3x^2 + 2p_2x + p_1\right)^2} \\ &= -6 \cdot \frac{6p_3^2x^2 + 4p_3p_2x - p_3p_1 + p_2^2}{\left(3p_3x^2 + 2p_2x + p_1\right)^2} \\ &= -6 \cdot \frac{6\left(p_3x + p_2/3\right)^2 - 2/3 \cdot p_2^2 - p_3p_1 + p_2^2}{\left(3p_3x^2 + 2p_2x + p_1\right)^2} \\ &= -6 \cdot \frac{6\left(p_3x + p_2/3\right)^2 + \left(p_2^2 - 3p_3p_1\right)/3}{\left(3p_3x^2 + 2p_2x + p_1\right)^2} \end{aligned} \tag{A.13}$$

and $p_2^2 - 3p_3p_1 > 0$; thence $f(x)$ has negative Schwarzian derivative on J.

Finally, we proof the maximum value $f(c) = b$ on J. Substituting c into $f(x)$,

$$\begin{aligned} f(c) &= p_3c\left(c^2 + \frac{p_2}{p_3} \cdot c + \frac{p_1}{p_3}\right) \\ &= p_3 \cdot \frac{-p_2 - \sqrt{p_2^2 - 3p_3p_1}}{3p_3} \cdot \left\{\frac{p_2^2 + p_2^2 - 3p_3p_1 + 2p_2\sqrt{p_2^2 - 3p_3p_1}}{9p_3^2} + \frac{-p_2^2 - p_2\sqrt{p_2^2 - 3p_3p_1}}{3p_3^2} + \frac{p_1}{p_3}\right\} \\ &= p_3 \cdot \frac{-p_2 - \sqrt{p_2^2 - 3p_3p_1}}{3p_3} \cdot \frac{2p_2^2 - 3p_3p_1 + 2p_2\sqrt{p_2^2 - 3p_3p_1} - 3p_2^2 - 3p_2\sqrt{p_2^2 - 3p_3p_1} + 9p_3p_1}{9p_3^2} \\ &= \frac{-p_2 - \sqrt{p_2^2 - 3p_3p_1}}{3} \cdot \frac{-p_2^2 + 6p_3p_1 - p_2\sqrt{p_2^2 - 3p_3p_1}}{9p_3^2} \\ &= \frac{p_2^3 - 6p_3p_2p_1 + p_2^2\sqrt{p_2^2 - 3p_3p_1} + p_2^2\sqrt{p_2^2 - 3p_3p_1} - 6p_3p_1\sqrt{p_2^2 - 3p_3p_1}}{27p_3^2} + \frac{p_2\left(p_2^2 - 3p_3p_1\right)}{27p_3^2} \\ &= \frac{2p_2^3 - 9p_3p_2p_1 + 2p_2^2\sqrt{p_2^2 - 3p_3p_1} - 6p_3p_1\sqrt{p_2^2 - 3p_3p_1}}{27p_3^2} = \frac{2p_2^3 - 9p_3p_2p_1 + \left(2p_2^2 - 6p_3p_1\right)\sqrt{p_2^2 - 3p_3p_1}}{27p_3^2} \end{aligned} \tag{A.14}$$

Since $p_2 < 0$, $p_2^2 = \nu p_3p_1$, $p_1 = -\{27(1 - \sqrt{1 - 4/\nu})\}/\{\nu \cdot [4 - 18/\nu - 4(1 - 3/\nu)^{3/2}]\}$, then

$$\begin{aligned} f(c) - b &= \frac{2p_2^3 - 9p_3p_2p_1 + \left(2p_2^2 - 6p_3p_1\right)\sqrt{p_2^2 - 3p_3p_1}}{27p_3^2} - \frac{-p_2 - \sqrt{p_2^2 - 4p_3p_1}}{2p_3} \\ &= \frac{4p_2^3 - 18p_3p_2p_1 + 4\left(p_2^2 - 3p_3p_1\right)\sqrt{p_2^2 - 3p_3p_1} + 27p_3p_2}{54p_3^2} + \frac{27p_3\sqrt{p_2^2 - 4p_3p_1}}{54p_3^2} \\ &= \frac{4p_2^3 - 18p_2 \cdot p_2^2/\nu + 4\left(1 - 3/\nu\right)p_2^2 \cdot \sqrt{1 - 3/\nu} \cdot \left|p_2\right| + 27p_3p_2 + 27p_3 \cdot \sqrt{1 - 4/\nu} \cdot \left|p_2\right|}{54p_3^2} \\ &= \frac{4p_2^3 - 18/\nu \cdot p_2^3 - 4\left(1 - 3/\nu\right)^{3/2}p_2^3 + 27p_3p_2 - 27p_3p_2\sqrt{1 - 4/\nu}}{54p_3^2} \end{aligned}$$

$$
\begin{aligned}
&= \frac{\left[4 - 18/v - 4\left(1 - 3/v\right)^{3/2}\right] p_2^3 + 27 p_3 p_2 \left(1 - \sqrt{1 - 4/v}\right)}{54 p_3^2} \\
&= p_2 \cdot \frac{\left[4 - 18/v - 4\left(1 - 3/v\right)^{3/2}\right] p_2^2 + 27 p_3 \left(1 - \sqrt{1 - 4/v}\right)}{54 p_3^2} = 0
\end{aligned}
\tag{A.15}
$$

Therefore $f(x) : J \longrightarrow J$ is the S-unimodal map and satisfies Theorem 1.

Case(2). First, we show that $f(x) : J = [0, b] \longrightarrow J$ has three order derivative function and $c \in (0, b)$ is the unique maximum point.

Since $v < 0$, obviously $p_1 = -\{27(1 + \sqrt{1 - 4/v})\}/\{v \cdot [4 - 18/v + 4(1 - 3/v)^{3/2}]\} > 0$, $p_2^2 = v p_3 p_1 > 0$.

From $p_3 < 0$, $p_2 > 0$, $p_1 > 0$, $p_2^2 - 4p_3 p_1 > p_2^2 - 3p_3 p_1$, then

$$
\begin{aligned}
b - c &= \frac{-p_2 - 3\sqrt{p_2^2 - 4p_3 p_1} + 2\sqrt{p_2^2 - 3p_3 p_1}}{6p_3} \\
&> \frac{-p_2 - 3\sqrt{p_2^2 - 3p_3 p_1} + 2\sqrt{p_2^2 - 3p_3 p_1}}{6p_3} \\
&= \frac{-p_2 - \sqrt{p_2^2 - 3p_3 p_1}}{6p_3} > 0
\end{aligned}
\tag{A.16}
$$

thence $0 < c < b$.

Similar to the proof given in case (1), $f(x)$ has first-order derivative function (A.5), second-order derivative function (A.6), and third-order derivative function (A.7). Solving $f'(x) = 0$ has one solution c. From (A.8), $f''(c) < 0$ and thus c is the maximum point.

Second proof that $f(0) = f(b) = 0$ and $f(x)$ is strictly increasing on $x \in (0, c)$ and strictly decreasing on $x \in (c, b)$. From (A.10), $f(x)$ has three solutions: $\{0, b, x_1\}$, and $x_1 < 0 < b$, and then $f(0) = f(b) = 0$. Letting $f'(x) = 0$, we get the other solution c_1 (A.11) and $c_1 < 0 < c < b$. Thence $f(x)$ is strictly increasing on $x \in (0, c)$ and strictly decreasing on $x \in (c, b)$.

Third, form (A.13) and $p_2^2 - 3p_3 p_1 > 0$, we proof that $f(x)$ has negative Schwarzian derivative on J.

Finally, from (A.14), and $p_2 > 0, p_2^2 = v p_3 p_1$, $p_1 = -\{27(1 + \sqrt{1 - 4/v})\}/\{v \cdot [4 - 18/v + 4(1 - 3/v)^{3/2}]\}$, then

$$
\begin{aligned}
f(c) - b &= \frac{2p_2^3 - 9p_3 p_2 p_1 + \left(2p_2^2 - 6p_3 p_1\right)\sqrt{p_2^2 - 3p_3 p_1}}{27 p_3^2} - \frac{-p_2 - \sqrt{p_2^2 - 4p_3 p_1}}{2p_3} \\
&= \frac{4p_2^3 - 18p_3 p_2 p_1 + 4\left(p_2^2 - 3p_3 p_1\right)\sqrt{p_2^2 - 3p_3 p_1} + 27 p_3 p_2}{54 p_3^2} + \frac{27 p_3 \sqrt{p_2^2 - 4p_3 p_1}}{54 p_3^2} \\
&= \frac{4p_2^3 - 18p_2 \cdot p_2^2/v + 4\left(1 - 3/v\right) p_2^2 \cdot \sqrt{1 - 3/v} \cdot \left|p_2\right| + 27 p_3 p_2 + 27 p_3 \cdot \sqrt{1 - 4/v} \cdot \left|p_2\right|}{54 p_3^2} \\
&= \frac{4p_2^3 - 18/v \cdot p_2^3 + 4\left(1 - 3/v\right)^{3/2} p_2^3 + 27 p_3 p_2 + 27 p_3 p_2 \sqrt{1 - 4/v}}{54 p_3^2} \\
&= \frac{\left[4 - 18/v + 4\left(1 - 3/v\right)^{3/2}\right] p_2^3 + 27 p_3 p_2 \left(1 + \sqrt{1 - 4/v}\right)}{54 p_3^2} \\
&= p_2 \cdot \frac{\left[4 - 18/v + 4\left(1 - 3/v\right)^{3/2}\right] p_2^2 + 27 p_3 \left(1 + \sqrt{1 - 4/v}\right)}{54 p_3^2} = 0
\end{aligned}
\tag{A.17}
$$

Therefore $f(x) : J \longrightarrow J$ is the S-unimodal map and satisfies Theorem 1.

Case(3). First, we show that $f(x) : J = [0, b] \longrightarrow J$ has three-order derivative function, and $c \in (0, b)$ is the unique maximum point.

We now judge the symbol of $p_1 = -\{27(1 - \sqrt{1 - 4/v})\}/\{v \cdot [4 - 18/v - 4(1 - 3/v)^{3/2}]\}$.

By $v < 0$, then

$$
1 - \frac{4}{v} > 1,
$$

$$
\begin{gathered}
4-\frac{18}{v}>0, \\
4\left(1-\frac{3}{v}\right)^{3/2}>0
\end{gathered}
\tag{A.18}
$$

and thence the judgement of $4-18/v-4(1-3/v)^{3/2}$ is equivalent to the judgement of $(4-18/v)^2-[4(1-3/v)^{3/2}]^2$. From (A.3), clearly $4-18/v-4(1-3/v)^{3/2}<0$, and then $p_1>0$.

From $p_3<0$, $p_2<0$, $p_1>0$, $p_2^2-4p_3p_1>p_2^2-3p_3p_1$, then

$$
\begin{aligned}
b-c &= \frac{-p_2-3\sqrt{p_2^2-4p_3p_1}+2\sqrt{p_2^2-3p_3p_1}}{6p_3} \\
&> \frac{-p_2-3\sqrt{p_2^2-4p_3p_1}+2\sqrt{p_2^2-4p_3p_1}}{6p_3} \\
&= \frac{-p_2-\sqrt{p_2^2-4p_3p_1}}{6p_3} > \frac{-p_2-\left|p_2\right|}{6p_3} = 0
\end{aligned}
\tag{A.19}
$$

and thus $0<c<b$.

Similar to the proof given in case (1), $f(x)$ has first-order derivative function (A.5), second-order derivative function (A.6), and third-order derivative function (A.7). Solving $f'(x)=0$ has one solution c. From (A.8), $f''(c)<0$ and thus c is the maximum point.

Second, we proof that $f(0)=f(b)=0$, and $f(x)$ is strictly increasing on $x\in(0,c)$ and strictly decreasing on $x\in(c,b)$. From (A.10), $f(x)$ has three solutions: $\{0,b,x_1\}$, and $x_1<0<b$, and then $f(0)=f(b)=0$. Letting $f'(x)=0$, we get the other solution c_1 (A.11), and $c_1<0<c<b$. Thence $f(x)$ is strictly increasing on $x\in(0,c)$ and strictly decreasing on $x\in(c,b)$.

Third, form (A.13) and $p_2^2-3p_3p_1>0$, we proof that $f(x)$ has negative Schwarzian derivative on J.

Finally, from (A.14) and $p_2<0, p_2^2=vp_3p_1, p_1=-\{27(1-\sqrt{1-4/v})\}/\{v\cdot[4-18/v-4(1-3/v)^{3/2}]\}$, then

$$
\begin{aligned}
f(c)-b &= \frac{2p_2^3-9p_3p_2p_1+\left(2p_2^2-6p_3p_1\right)\sqrt{p_2^2-3p_3p_1}}{27p_3^2}-\frac{-p_2-\sqrt{p_2^2-4p_3p_1}}{2p_3} \\
&= \frac{4p_2^3-18p_3p_2p_1+4\left(p_2^2-3p_3p_1\right)\sqrt{p_2^2-3p_3p_1}+27p_3p_2}{54p_3^2}+\frac{27p_3\sqrt{p_2^2-4p_3p_1}}{54p_3^2} \\
&= \frac{4p_2^3-18p_2\cdot p_2^2/v+4\left(1-3/v\right)p_2^2\cdot\sqrt{1-3/v}\cdot\left|p_2\right|+27p_3p_2+27p_3\cdot\sqrt{1-4/v}\cdot\left|p_2\right|}{54p_3^2} \\
&= \frac{4p_2^3-18/v\cdot p_2^3-4\left(1-3/v\right)^{3/2}p_2^3+27p_3p_2-27p_3p_2\sqrt{1-4/v}}{54p_3^2} \\
&= \frac{\left[4-18/v-4\left(1-3/v\right)^{3/2}\right]p_2^3+27p_3p_2\left(1-\sqrt{1-4/v}\right)}{54p_3^2} \\
&= p_2\cdot\frac{\left[4-18/v-4\left(1-3/v\right)^{3/2}\right]p_2^2+27p_3\left(1-\sqrt{1-4/v}\right)}{54p_3^2} = 0
\end{aligned}
\tag{A.20}
$$

Therefore $f(x): J\longrightarrow J$ is the S-unimodal map, and satisfies Theorem 1. This completes the proof. □

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This project is jointly supported by the National Natural Science Foundation of China (Grant No. 61170037) and Research Award Fund for Natural Science Foundation of Shandong Province No. ZR2017BA022.

References

[1] J. C. Sprott, *Chaos and Time-Series Analysis*, Oxford University Press, Oxford, UK, 2003.

[2] T. Y. Li and J. A. Yorke, "Period three implies chaos," *The American Mathematical Monthly*, vol. 985, pp. 82–90, 1975.

[3] K. Binder and D. W. Heermann, *Monte Carlo Simulation in Statistical Physics: An Introduction*, Springer, 4th edition, 2002.

[4] K. Zuev, O. Eisenberg, and D. Krioukov, "Exponential random simplicial complexes," *Journal of Physics A: Mathematical and General*, vol. 48, no. 46, Article ID 465002, pp. 1–5, 2015.

[5] J. Melià-Seguí, J. Garcia-Alfaro, and J. Herrera-Joancomartí, "J3Gen: a PRNG for low-cost passive RFID," *Sensors*, vol. 13, no. 3, pp. 3816–3830, 2013.

[6] A. Shen, "Complete convergence for weighted sums of END random variables and its application to nonparametric regression models," *Journal of Nonparametric Statistics*, vol. 28, no. 4, pp. 702–715, 2016.

[7] N. Ferguson, B. Schneier, and T. Kohno, *Cryptography Engineering: Design Principles and Practical Applications*, Wiley Publishing, Inc., 2010.

[8] D. G. Marangon, A. Plews, M. Lucamarini et al., "Long-term test of a fast and compact quantum random number generator," *Journal of Lightwave Technology*, vol. 36, no. 17, pp. 3778–3784, 2018.

[9] K. Antoniadis, P. Blanchard, R. Guerraoui, and J. Stainer, "The entropy of a distributed computation random number generation from memory interleaving," *Distributed Computing*, vol. 31, no. 5, pp. 389–417, 2018.

[10] C. Abellán, W. Amaya, D. Mitrani, V. Pruneri, and M. W. Mitchell, "Generation of fresh and pure random numbers for loophole-free bell tests," *Physical Review Letters*, vol. 115, no. 25, Article ID 250403, pp. 1–5, 2015.

[11] H. de Faria, M. G. C. Resende, and D. Ernst, "A biased random key genetic algorithm applied to the electric distribution network reconfiguration problem," *Journal of Heuristics*, vol. 23, no. 6, pp. 533–550, 2017.

[12] X. P. Yang, L. Q. Min, and X. Wang, "A cubic map chaos criterion theorem with applications in generalized synchronization based pseudorandom number generator and image encryption," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 25, no. 5, Article ID 053104, 2015.

[13] L. Min, X. Lan, L. Hao, and X. Yang, "A 6 dimensional chaotic generalized synchronization system and design of pseudorandom number generator with application in image encryption," in *Proceedings of the 10th International Conference on Computational Intelligence and Security (CIS '14)*, pp. 356–362, IEEE, Kunming, China, November 2014.

[14] I. T. Chen, "Random numbers generated from audio and video sources," *Mathematical Problems in Engineering*, vol. 2013, Article ID 285373, 7 pages, 2013.

[15] J. Self and M. C. Mackey, "Random numbers from a delay equation," *Journal of Nonlinear Science*, vol. 26, no. 5, pp. 1311–1327, 2016.

[16] K. Horbacz, "Strong law of large numbers for continuous random dynamical systems," *Statistics & Probability Letters*, vol. 118, pp. 70–79, 2016.

[17] D. E. Knuth, *The art of Computer Programming, Seminumerical Algorithms*, Addision-Wesley, Boston, USA, 3rd edition, 1997.

[18] K. Wallace, K. Moran, E. Novak, G. Zhou, and K. Sun, "Toward sensor-based random number generation for mobile and IoT devices," *IEEE Internet of Things Journal*, vol. 3, no. 6, pp. 1189–1201, 2016.

[19] Z. Yuan, H. Li, Y. Miao, W. Hu, and X. Zhu, "Digital-analog hybrid scheme and its application to chaotic random number generators," *International Journal of Bifurcation and Chaos*, vol. 27, Article ID 1750210, pp. 1–7, 2017.

[20] S. Harase, "On the $\mathbb{F}_2$-linear relations of mersenne twister pseudorandom number generators," *Mathematics and Computers in Simulation*, vol. 100, pp. 103–113, 2014.

[21] G. Marsaglia, "The Marsaglia Random number CDROM including the Diehard," software available at http://www.stat.fsu.edu/pub/diehard/.

[22] NIST, "FIPS PUB 140: Security requirements for cryptographic modules," Tech. Rep., NIST, Gaithersburg, MD, USA, 2001.

[23] A. Rukhin, J. Sota, J. Nechvatal et al., "A statistical test suite for random and pseudorandom number generator for cryptographic applications," Tech. Rep., NIST Special Publication, Gaithersburg, MD, USA, 2001.

[24] H. L. Zhou and E. B. Song, "Discrimination of the 3-periodic points of a quadratic polynomial," *Journal of Sichuan University. Natural Science Edition*, vol. 46, no. 3, pp. 561–564, 2009.

[25] D. Singer, "Stable orbits and bifurcation of maps of the interval," *SIAM Journal on Applied Mathematics*, vol. 35, no. 2, pp. 260–267, 1978.

[26] M. Andrecut and M. K. Ali, "On the occurrence of robust chaos in a smooth system," *Modern Physics Letters B*, vol. 15, no. 12-13, pp. 391–395, 2001.

[27] İ. Öztürk and R. Kiliç, "Cycle lengths and correlation properties of finite precision chaotic maps," *International Journal of Bifurcation and Chaos*, vol. 24, no. 9, Article ID 1450107, 14 pages, 2014.

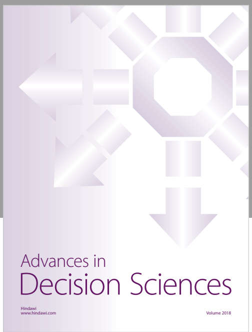
[28] H. Zang, L. Min, and G. Zhao, "A generalized synchronization theorem for discrete-time chaos system with application in data encryption scheme," in *Proceedings of the International Conference on Communications, Circuits and Systems (ICCCAS '07)*, pp. 1325–1329, IEEE, Kokura, Japan, July 2007.

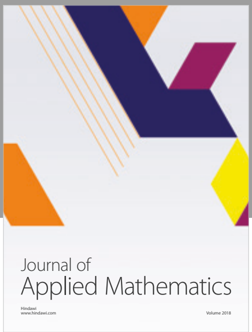
[29] L. Q. Min, T. Chen, and H. Y. Zang, "Analysis of FIPS 140-2 test and chaos-based pseudorandom number generator," in *Proceedings of the 5th Chaotic Modeling and Simulation International Conference*, pp. 345–352, Antens, Greece, 2012.

[30] L. Min, L. Hao, and L. Zhang, "Statistical test for string pseudorandom number generators," *Lecture Notes Artificial Intelligence*, vol. 7888, pp. 278–287, 2013.

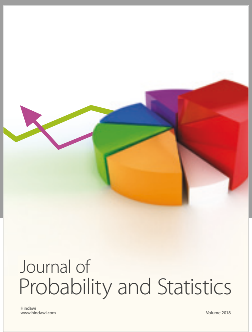
[31] S. W. Golomb, *Shift Register Sequences*, Laguna Hills, Aegean Park, CA, USA, 1982.

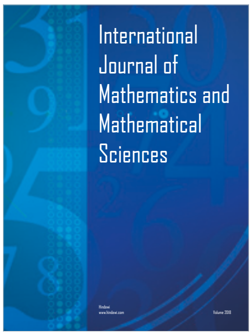
Advances in
Operations Research


Advances in
Decision Sciences

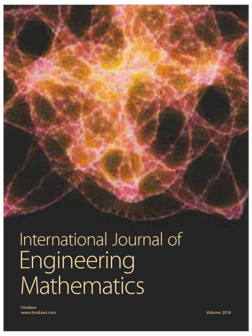

Journal of
Applied Mathematics

The Scientific
World Journal

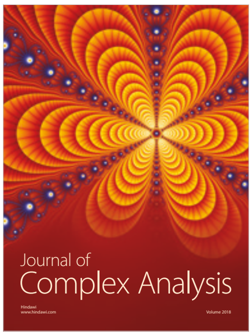

Journal of
Probability and Statistics

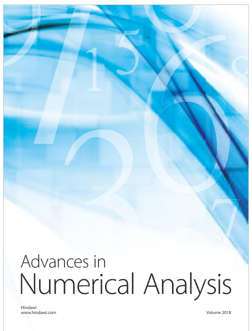

International
Journal of
Mathematics and
Mathematical
Sciences

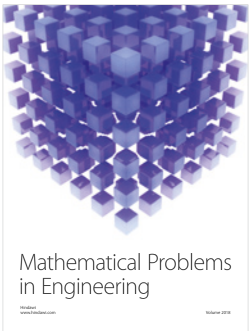
Journal of
Optimization

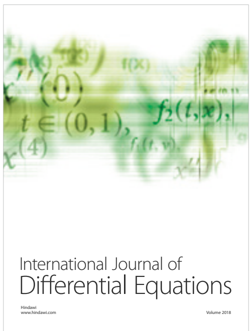

International Journal of
Engineering
Mathematics

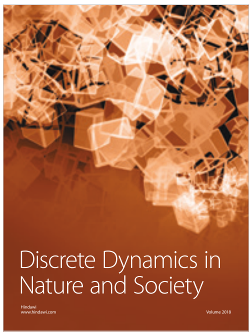
International Journal of
Analysis

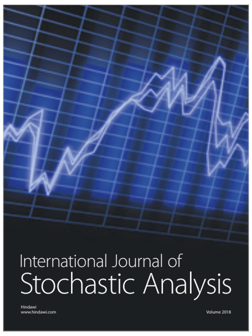

Journal of
Complex Analysis


Advances in
Numerical Analysis


Mathematical Problems
in Engineering

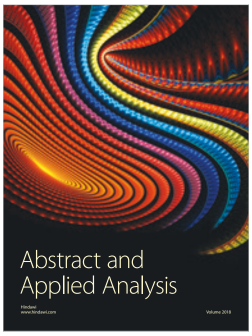

International Journal of
Differential Equations

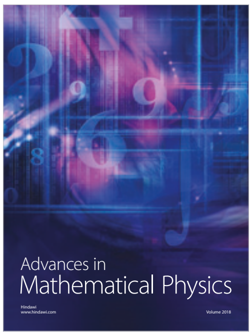

Discrete Dynamics in
Nature and Society


International Journal of
Stochastic Analysis

Journal of
Mathematics

Journal of
Function Spaces


Abstract and
Applied Analysis


Advances in
Mathematical Physics