Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 1375346, 12 pages
https://doi.org/10.1155/2021/1375346

Research Article

Research on Pseudorandom Number Generator Based on Several New Types of Piecewise Chaotic Maps

Hongyan Zang, Yue Yuan, and Xinyuan Wei

Mathematics and Physics School, University of Science and Technology Beijing, Beijing 100083, China

Correspondence should be addressed to Hongyan Zang; zhylixiang@126.com

Received 27 May 2021; Revised 22 July 2021; Accepted 10 August 2021; Published 20 August 2021

Academic Editor: Cornelio Posadas-Castillo

This paper proposes three types of one-dimensional piecewise chaotic maps and two types of symmetrical piecewise chaotic maps and presents five theorems. Furthermore, some examples that satisfy the theorems are constructed, and an analysis and model of the dynamic properties are discussed. The construction methods proposed in this paper have a certain generality and provide a theoretical basis for constructing a new discrete chaotic system. In addition, this paper designs a pseudorandom number generator based on piecewise chaotic map and studies its application in cryptography. Performance evaluation shows that the generator can generate high quality random sequences efficiently.

1. Introduction

Chaos, as a nonlinear deterministic dynamic system with external complex phenomena due to its inherent randomness, has been widely considered and intensively studied. In the 1870s, the mathematician Li and his tutor Yorke put forward the definition of chaos in the famous article "Period Three Contains Chaos" [1], that is, the Li–Yorke chaos discrimination theorem. Then, a chaotic discrimination theorem, namely, Marotto's theorem, that is more suitable for high-dimensional discrete dynamic systems, was given by Marotto [2]. These two theorems provide an important theoretical basis on which later scholars have studied one-dimensional discrete chaotic systems [2–4]. Since 1989, chaotic systems have been widely used in the field of secure communication due to their sensitivity to the initial values or parameters, ergodicity, and randomness-like properties [5–8]. After constructing a new chaotic system, we can use it to design a new chaotic pseudorandom number generator (CPRNG). Therefore, it is of great theoretical and practical significance to study and construct a new chaotic system.

In many studies on one-dimensional discrete chaotic systems, piecewise chaotic mapping has gradually attracted scholars' attention. Among them, piecewise linear chaotic mapping has a simpler form in chaotic systems, and because of its relatively good uniformity, it is easy to implement by fixed point algorithms with limited digital precision, which is convenient for its application in the fields of cryptography and communication [9]. As a typical one-dimensional piecewise linear discrete system, the tent map is a basic example for the promotion and application of chaotic theory systems. Many scholars have constructed other chaotic systems based on the tent map. In [10], a new one-dimensional piecewise chaotic map was constructed by combining a tent map with a logistic map. In [11], a class of oblique tent maps was improved, and it was proved that the chaotic system has excellent dynamic key space and practicability, making it more suitable for secure communication and other fields [12], based on the deformation of a tent map, provides piecewise linear chaotic mapping, and uses the period three theorem and topological conjugation theory to construct quadratic polynomial chaotic mapping and realize homogenization of a chaotic sequence.

For the study of piecewise nonlinear mapping, most approaches involve theoretical analyses of a system's own dynamic characteristics and periodic phenomena [13, 14] or piecewise transformations based on known chaotic mapping. In [15], a class of one-dimensional piecewise nonlinear discrete dynamic systems under modulo operation is constructed, and the improved Marotto's theorem is used to give

a general theory of the chaotic behavior of piecewise nonlinear functions with nonzero origin. Reference [16] built a piecewise nonlinear chaotic mapping system based on logistic mapping so that the system parameters have a larger value range and better uniformity. Reference [17] discussed the branch of chaotic attractors in piecewise smooth one-dimensional mapping with a large number of switching manifolds based on different nonlinear smoothing models and applied it in the field of electronic science.

In the field of cryptography, the research of pseudorandom number generator based on chaotic system mainly focuses on the following aspects: proposing new chaotic system and designing controller to realize chaotic synchronization [18] and improving the existing chaotic system to enhance its complexity and make it have greater Lyapunov [19, 20]. Some mathematical methods are used to improve the random performance of pseudorandom number generator [21], the software and hardware implementation of pseudorandom number generator [22], and the encryption scheme and cryptosystem based on chaotic pseudorandom number generator [23, 24]. The one-dimensional discrete chaotic system has the advantages of simple structure and easy realization. Therefore, it is an important content to construct a large number of general one-dimensional discrete chaotic systems.

The structure of this article is as follows. Section 2 constructs several types of general one-dimensional discrete piecewise maps, and based on the Li–Yorke discriminant theorem and Marotto's theorem, sufficient conditions for chaotic mapping are given. One-dimensional discrete piecewise chaotic nonlinear mapping and a numerical simulation are performed. Section 3 gives two types of segmented chaotic mapping models with symmetry, and based on the proposed models, three examples of chaotic mapping satisfying the conditions are given. In Section 4, a new pseudorandom number generator based on piecewise chaotic map is designed, and the randomness and key sensitivity of the generator are analyzed. Finally, we conclude the full text in Section 5.

2. Three Types of One-Dimensional Discrete Piecewise Chaotic Maps

First, we introduce the Li–Yorke chaos discrimination theorem, which is expressed as follows.

Lemma 1 (see [1]). *Let J be an interval and let $f: J \longrightarrow J$ be continuous. If there is a point $a \in J$ for which the points $b = f(a)$, $c = f(b)$, and $d = f(c)$ satisfy $d \le a < b < c$ (or $d \ge a > b > c$), then it is a chaotic map in the sense of Li–Yorke.*

In addition, we introduce other related theories. Let $B_r(x^*)$ be a closed ball with point x^* as the center and radius r, if the fixed point x^* of the differentiable map g in R^n satisfies the following two conditions:

(1) There is a real number $r > 0$, such that the modulus of all the eigenvalues of the Jacobian matrix $Dg(x)$ of any point x in $B_r(x^*)$ is greater than 1.

(2) There is a point $x^0 \ne x^*$ and a natural number $m \ge 2$ in $B_r(x^*)$ such that $g^m(x^0) = x^*$, and point x^0 satisfies $\det\{Dg^m(x^0)\} \ne 0$.

Then, the fixed point x^* is a regressive repulsor of the mapping g [3].

Lemma 2 (Marotto's theorem [2]). *If the n-dimensional map $g: R^n \longrightarrow R^n$ has a regressive repellent, then the map g has chaotic behavior in the Li–Yorke sense.*

Next, based on the above two lemmas, several kinds of one-dimensional discrete piecewise chaotic maps are given.

2.1. Construction of One-Dimensional Discrete Piecewise Chaotic Map

Theorem 1. *Let f be a continuously differentiable strictly monotonically increasing function on the closed interval $[0, 1]$, let a be a real number on the open interval (0, 1), and define a function g_1 of the following form:*

$$g_1(x) = \begin{cases} \dfrac{f(x/a) - f(0)}{f(1) - f(0)}, & 0 \le x \le a, \\ \dfrac{f(1 - x/1 - a) - f(0)}{f(1) - f(0)}, & a < x \le 1. \end{cases} \tag{1}$$

If the function g_1 satisfies $|g_1'(x)| > 1$ in the interval $[0, a) \cup (a, 1]$, then g_1 is a chaotic map in the sense of Li–Yorke.

Proof of Theorem 1. The function f is continuous in the interval $[0, 1]$, and g_1 is a continuous function in $J: [0, 1] \longrightarrow J: [0, 1]$. Therefore, it is only necessary to prove that there are four points satisfying the conditions of the Li–Yorke theorem:

$$g_1(y_3) = y_4 \le y_1 < g_1(y_1) = y_2 < y_3 = g_1(y_2). \tag{2}$$

Let $F(x) = g_1(x) - x$, then $F'(x) = g_1'(x) - 1$, and in the interval $[0, a)$, $F'(x) = g_1'(x) - 1 \ge 0$ can be obtained from $g_1'(x) > 1$.

Therefore, in the interval $(0, a)$, $F(x) = g_1(x) - x > F(0) = 0$, that is, $g_1(x) > x$.

g_1 is a unimodal function, and its function image structure is shown in Figure 1.

Take $y_2 = a$, $y_3 = g_1(y_2) = g_1(a) = 1$, and $y_4 = g_1(y_3) = g_1(1) = 0$. Obviously there is

$$y_4 < y_2 < y_3. \tag{3}$$

Because of $g_1(0) = 0 < y_2 = a < 1 = g_1(y_2)$, from the continuity of g_1 and the intermediate value theorem $\exists y_1 \in (0, y_2)$, if $y_2 = g_1(y_1)$, then

$$y_4 < y_1 < y_2. \tag{4}$$

Combining equations (3) and (4), there are four points satisfying the conditions of the Li–Yorke theorem:

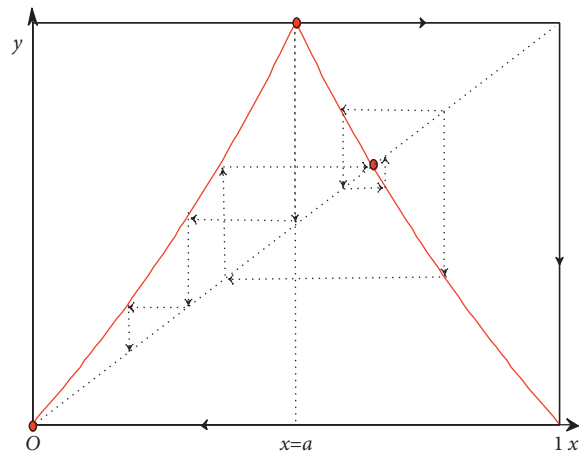

Figure 1: Rough function diagram of g_1.

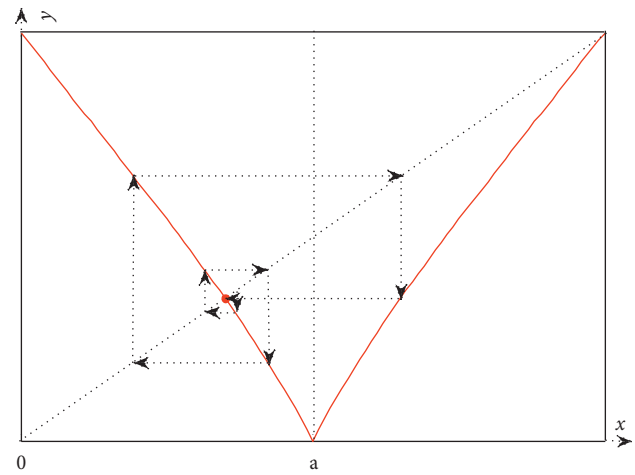

Figure 2: Rough function diagram of g_2.

$$g_1(y_3) = y_4 \le y_1 < g_1(y_1) = y_2 < y_3 = g_1(y_2). \quad (5)$$

In conclusion, the function g_1 satisfies the Li–Yorke discriminant theorem; thus, it is a chaotic map in the sense of Li–Yorke.

Analogous to the piecewise chaotic map constructed by Theorem 1, another one-dimensional discrete piecewise chaotic map is constructed below. □

Theorem 2. *Let f be a continuously differentiable strictly monotonically increasing function on the closed interval $[0, 1]$ and a be a real number on the open interval (0, 1), and define a function g_2 of the following form:*

$$g_2(x) = \begin{cases} 1 - \dfrac{f(x/a) - f(0)}{f(1) - f(0)}, & 0 \le x \le a, \\ 1 - \dfrac{f(1 - x/1 - a) - f(0)}{f(1) - f(0)}, & a < x \le 1. \end{cases} \quad (6)$$

If the function g_2 satisfies $|g_2'(x)| > 1$ in the interval $[0, a) \cup [a, 1)$, then g_2 is a chaotic map in the sense of Li–Yorke.

The proof process is similar. The function image structure of g_2 is shown in Figure 2.

Next, we discuss the relationship between Theorems 1 and 2. Let formula (1) be $A(x)$ and formula (3) be $B(x)$; we can know when $a = 0.5$ has $A(x) = 1 - B(x)$; $A(x)$ and $B(x)$ are symmetric piecewise mappings.

Based on this, we can find a homeomorphic mapping $C(x)$: $C(x) = 1 - x$, having

$$\begin{aligned} C \circ A &= C(1 - B(x)) = 1 - 1 + B(x) = B(x), \\ B \circ C &= B(C(x)) = B(1 - x), \end{aligned} \quad (7)$$

and because we know that $B(x)$ function is obviously symmetric with respect to $x = 0.5$, then there is $B(x) = B(1 - x)$ on $[0, 1]$, so $C \circ A = B \circ C$ holds. Then, there is a topological conjugate relationship between the mappings of Theorems 1 and 2. Furthermore, from the fact that homeomorphic mapping $C(x)$ is a linear mapping, we can see that Theorems 1 and 2 satisfy affine conjugation and therefore have the same dynamic behavior.

Theorem 3. *Let f be a continuously differentiable strictly monotonically increasing function on the closed interval $[0, 1]$ and a be a real number on the open interval (0, 1), and define a function g_3 of the following form:*

$$g_3(x) = \begin{cases} \dfrac{f(x/a) - f(0)}{f(1) - f(0)}, & 0 \le x < a, \\ 1 - \dfrac{f(1 - x/1 - a) - f(0)}{f(1) - f(0)}, & a \le x \le 1. \end{cases} \quad (8)$$

If the function g_3 satisfies $|g_3'(x)| > 1$ in the interval $[0, a) \cup [a, 1)$, then g_3 is a chaotic map in the sense of Li–Yorke.

Proof of Theorem 3. According to the conditions, the function image structure of function g_3 is shown in Figure 3.

According to the theorem, $g_3(0) = 0$; thus, $x^* = 0$ is the fixed point of $g_3(x)$. Since the derivative of function g_3 on [0, 1] is greater than 1, $x^* = 0$ is a repulsive fixed point.

(1) Consider the auxiliary function $h_1(x) = g_3(x)$, with $x \in [a, 1]$:

Choose $x_1 \in [a, 1]$ that satisfies $h(x_1) = g_3(x_1) = x^* = 0$ to obtain $x_1 = h^{-1}(x^*) = g_3^{-1}(x^*) = a$.

(2) Consider the auxiliary function $h_2(x) = g_3(x) - x_1$, $x \in [0, a)$:

Because $\lim_{x \to a^-} h_2(x) = \lim_{x \to a^-} g_3(x) = 1 > a = x_1$, there is $\delta_0 > 0$, and for $\forall x \in [a - \delta_0, a)$, there is always $h_2(x) = g_3(x) > x_1$.

Take $\overline{x} \in [a - \delta_0, a)$; then, $h(\overline{x}) = g_3(\overline{x}) - x_1 > 0$, and $h(0) = g_3(0) - x_1 = -x_1 < 0$.

According to the one-dimensional intermediate value theorem, there is $x_0 \in (0, \overline{x})$ such that $h(x_0) = g_3(x_0) - x_1 = 0$, that is, $g_3(x_0) = x_1$. Then,

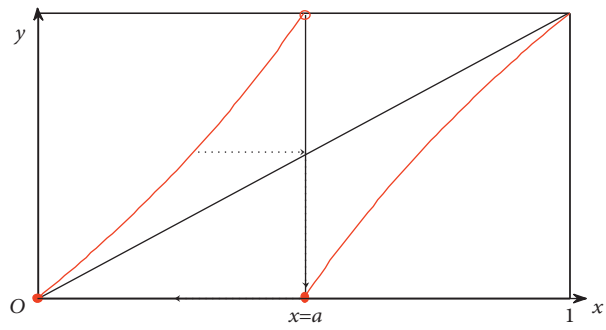

Figure 3: Rough function diagram of g_3.

$$\begin{aligned} g_3(x_0) = x_1 &\longrightarrow g_3(g_3(x_0)) = g_3(x_1) \\ &= x^* \longrightarrow g_3^2(x_0) = x^*. \end{aligned} \tag{9}$$

In conclusion, the fixed point $x^* = 0$ of $g_3(x)$ satisfies the following conditions:

(1) Take $r = x_1$ and satisfy $x_0 \in (0, \overline{x}) \in (0, x_1)$ such that $B_r(x^*)$ becomes a closed ball including x^*. Its Jacobian matrix is $Dg(x) = g_3'(x) > 1$. Thus, for any $x \in B_r(x^*)$, the modulus of the eigenvalue of $Dg(x)$ is greater than 1.

(2) There exists a point $0 < x_0 < 1$ and a natural number $m = 2$ in $B_r(x^*)$ such that $g_3^m(x_0) = x^*$, and x_0 is nondegenerate, that is, it satisfies

$$\begin{aligned} \det\{Dg^m(x_0)\} &= \det\{g_3(x_1)\} \cdot \det\{g_3(x_0)\} \\ &= g_3'(x_1) \cdot g_3'(x_0) \neq 0. \end{aligned} \tag{10}$$

Therefore, the point x^* is a regressive repulsor of map g_3 and thus is a chaotic map in the sense of Li–Yorke.

The proof is over. Next, we verify the above three theorems by a numerical simulation. □

2.2. Numerical Simulation of One-Dimensional Discrete Piecewise Chaotic Map. Substituting $f(x) = \sin e^{x-1}$ into Theorem 1, the image of function g_1, the bifurcation diagram of parameter a and the Lyapunov exponent diagram are as shown in Figures 4(a)–4(c). In Theorem 2, the image of function g_2, the bifurcation diagram of parameter a and the Lyapunov exponent diagram are as shown in Figures 4(d)–4(f). In Theorem 3, the image of function g_3, the bifurcation graph of parameter a and the Lyapunov exponent graph are as shown in Figures 4(g)–4(i).

Substituting $f(x) = e^{0.01 \sin x}$ into Theorem 1, the image of function g_1, the bifurcation diagram of parameter a and the Lyapunov exponent diagram are as shown in Figures 5(a)–5(c). In Theorem 2, the image of function g_2, the bifurcation diagram of parameter a and the Lyapunov exponent diagram are as shown in Figures 5(d)–5(f). In Theorem 3, the image of function g_3, the bifurcation graph of parameter a and the Lyapunov exponent graph are as shown in Figures 5(g)–5(i).

Substituting $f(x) = 0.3x \cos x + 0.1e^x$ into Theorem 1, the image of function g_1, the bifurcation diagram of parameter a, and the Lyapunov exponent diagram are as shown in Figures 6(a)–6(c). In Theorem 2, the image of function g_2, the bifurcation diagram of parameter a, and the Lyapunov exponent diagram are as shown in Figures 6(d)–6(f). In Theorem 3, the image of function g_3, the bifurcation graph of parameter a and the Lyapunov exponent graph are as shown in Figures 6(g)–6(i).

3. Two Types of Piecewise Chaotic Maps with Symmetric Properties

3.1. Construction of Symmetric Piecewise Chaotic Map. Based on the Li–Yorke chaotic discrimination theorem, a class of piecewise chaotic maps with symmetric properties are given below.

Theorem 4. *Let f be a continuous differentiable strictly monotone increasing function on a closed interval $[0, 1]$, and define the following piecewise mapping h_1:*

$$h_1(x) = \frac{f(|2x-1|) - f(0)}{f(1) - f(0)} = \begin{cases} \dfrac{f(-2x+1) - f(0)}{f(1) - f(0)}, & 0 \le x \le 0.5, \\ \dfrac{f(2x-1) - f(0)}{f(1) - f(0)}, & 0.5 < x \le 1. \end{cases} \tag{11}$$

If the function h_1 satisfies $h_1'(x) = 2f'(2x-1)/f(1) - f(0) > 1$ on $(0.5, 1]$, then h_1 is a chaotic map in the sense of Li–Yorke.

Proof of Theorem 3. From the fact that f is continuous in the interval $[0, 1]$, it is known that h_1 is a continuous function on $J\colon [0, 1] \longrightarrow J\colon [0, 1]$. Therefore, it is necessary to prove that there exist four points satisfying the conditions of the Li–Yorke theorem:

$$g(y_3) = y_4 \le y_1 < g(y_1) = y_2 < y_3 = g(y_2). \tag{12}$$

Let $F(x) = h_1(x) - x$, then $F'(x) = h_1'(x) - 1$, and in the interval $(0.5, 1]$, $F'(x) = h_1'(x) - 1 > 0$ can be obtained from $h_1'(x) = 2f'(2x-1)/f(1) - f(0) > 1$.

Therefore, $F(x) = h_1(x) - x \le F(1) = 0$, that is, on the interval $(0.5, 1]$, $h_1(x) \le x$.

Combined with the function h_1 as a unimodal function, taking $y_2 = 1/2$, $y_3 = h_1(y_2) = h_1(1/2) = 0$, and $y_4 = h_1(y_3) = h_1(0) = 1$, obviously

$$y_4 > y_2 > y_3. \tag{13}$$

Moreover, $h_1(1/2) = 0 < y_2 = 1/2 < 1 = h_1(1)$. Then, by the continuity of h_1 and the intermediate value theorem of continuous function $\exists y_1 \in (y_2, 1)$, such that $y_2 = g(y_1)$, one obviously has

$$y_4 > y_1 > y_2. \tag{14}$$

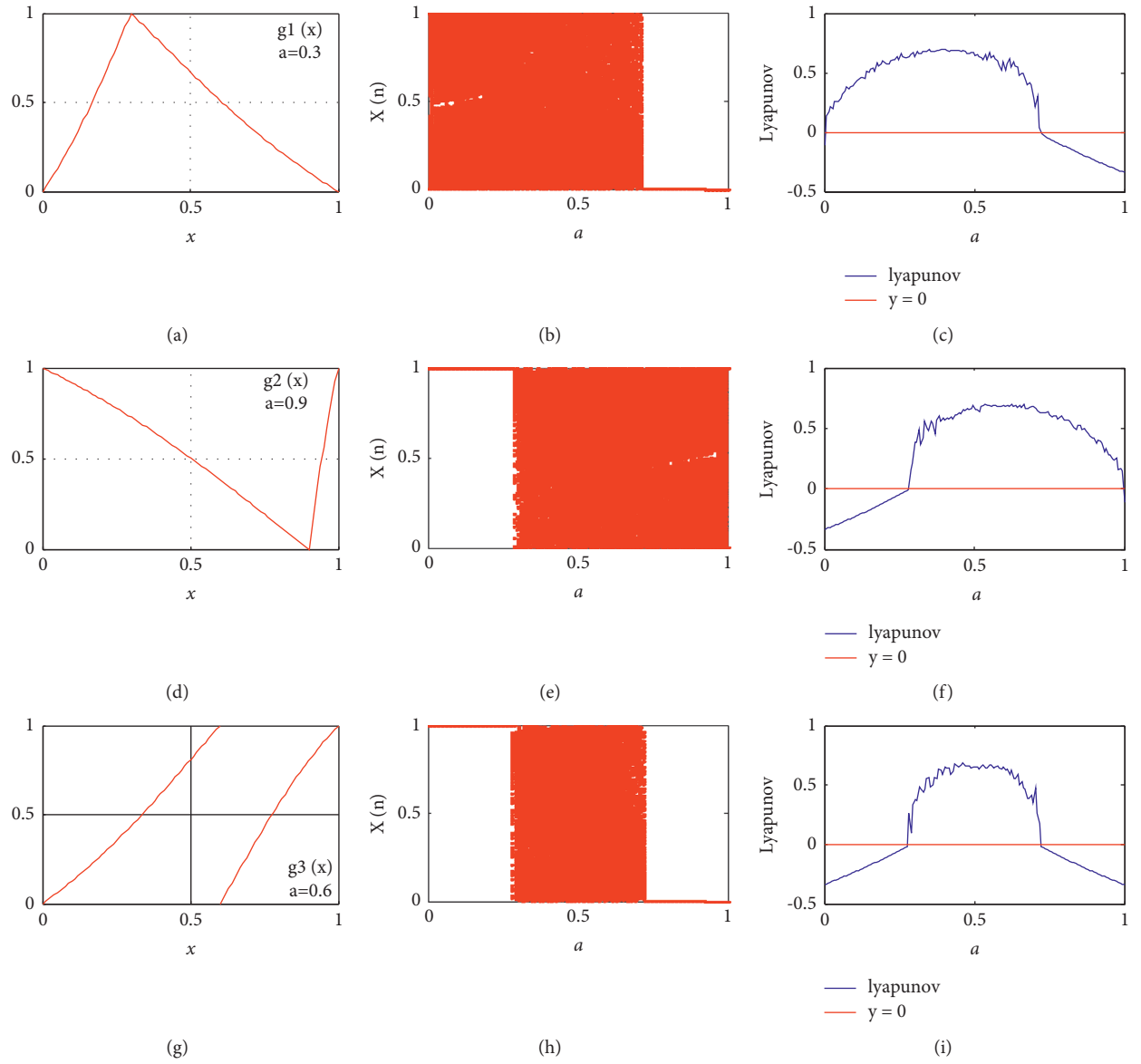

Figure 4: (a–c) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = \sin e^{x-1}$ in Theorem 1. (d–f) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = \sin e^{x-1}$ in Theorem 2. (g–i) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = \sin e^{x-1}$ in Theorem 3.

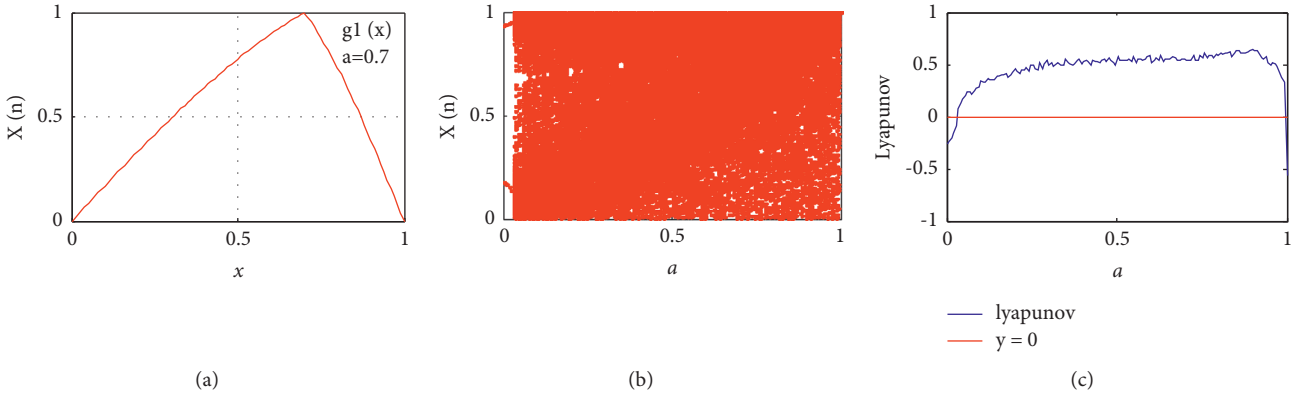

Figure 5: Continued.

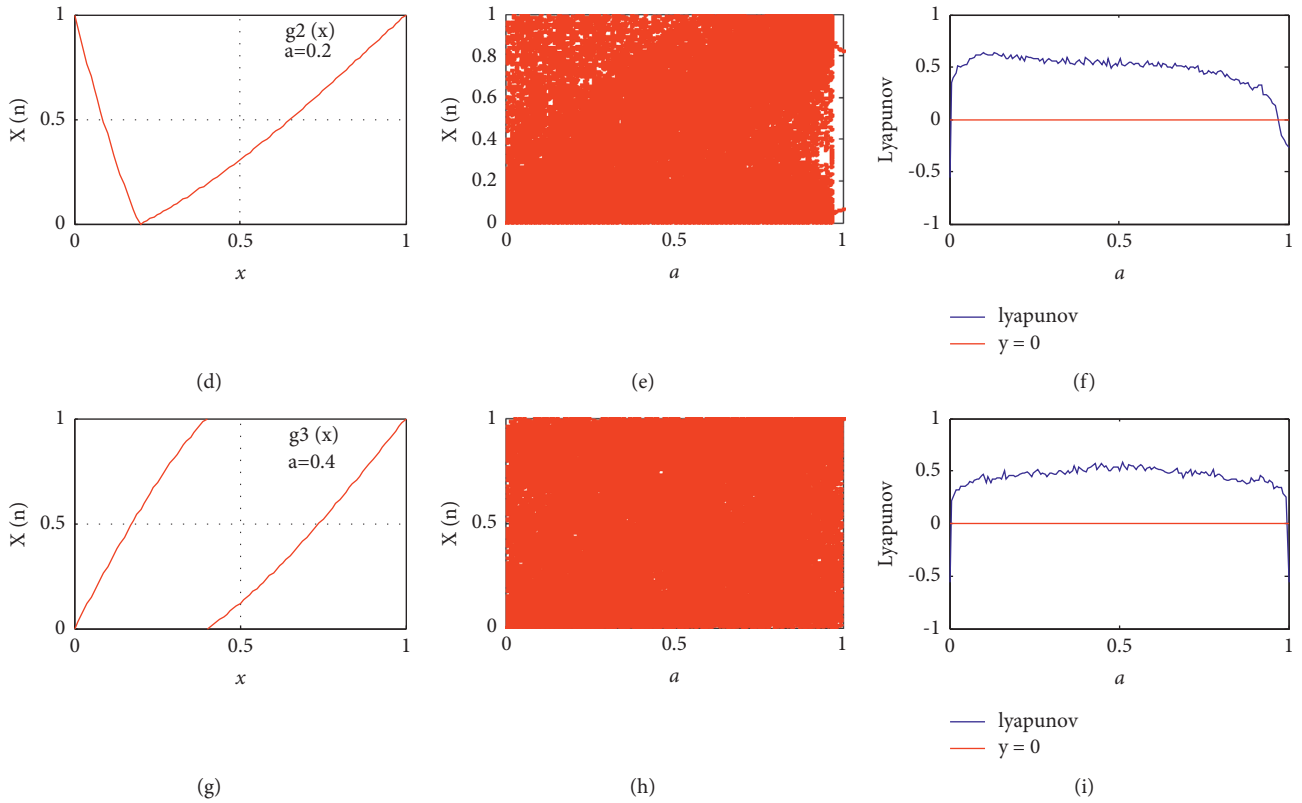

Figure 5: (a–c) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = e^{0.01 \sin x}$ in Theorem 1. (d–f) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = e^{0.01 \sin x}$ in Theorem 2. (g–i) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = e^{0.01 \sin x}$ in Theorem 3.

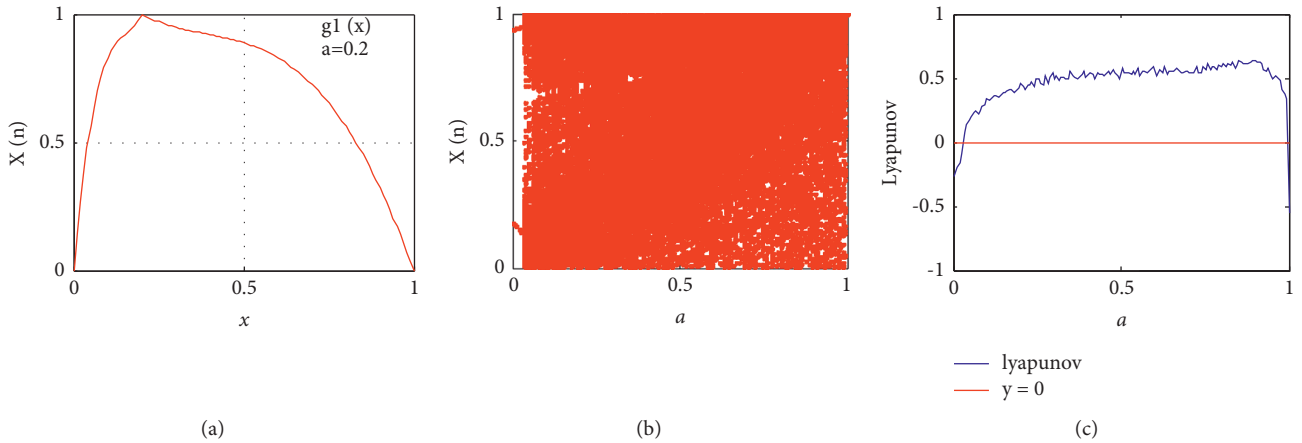

Figure 6: Continued.

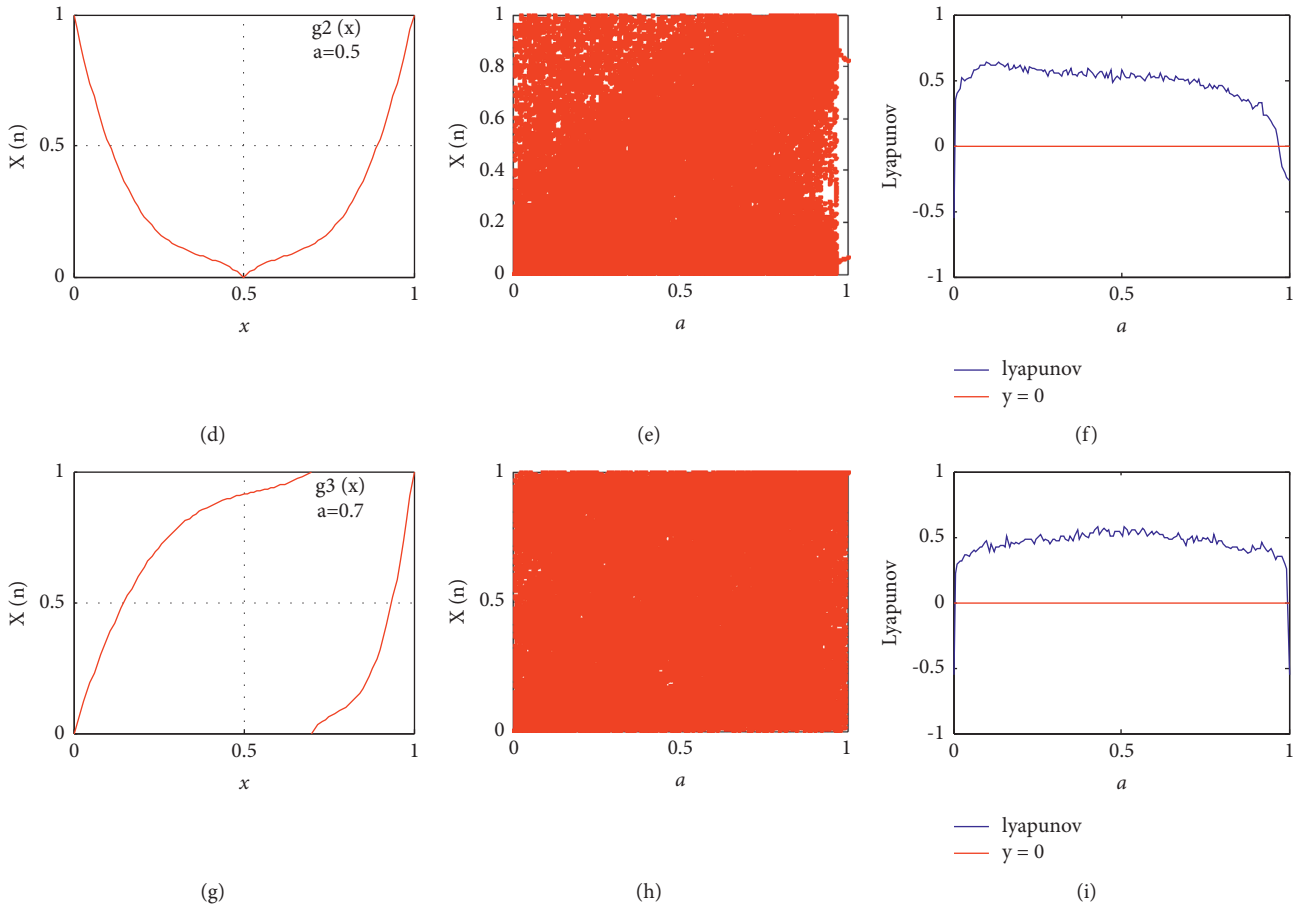

FIGURE 6: (a–c) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = 0.3x\cos x + 0.1e^x$ in Theorem 1. (d–f) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = 0.3x\cos x + 0.1e^x$ in Theorem 2. (g–i) The function image, bifurcation diagram, and Lyapunov exponent diagram obtained by making $f(x) = 0.3x\cos x + 0.1e^x$ in Theorem 3.

Combining equations (13) and (14) shows that there are four points that satisfy the conditions of the Li–Yorke theorem:

$$h_1(y_3) = y_4 \geq y_1 > h_1(y_1) = y_2 > y_3 = h_1(y_2). \tag{15}$$

In conclusion, the function h_1 satisfies the Li–Yorke discriminant theorem and is a chaotic map in the sense of Li–Yorke. Equation (11) is obviously symmetric about the straight line $x = 0.5$; thus, the function h_1 has symmetry.

Similar to Theorem 4, another class of one-dimensional discrete piecewise chaotic maps with symmetric properties is given below. □

Theorem 5. *Let f be a continuous differentiable strictly monotone increasing function on a closed interval $[0, 1]$, and define the following piecewise mapping h_2:*

$$h_2(x) = 1 - \frac{f(|2x-1|) - f(0)}{f(1) - f(0)} = \begin{cases} 1 - \dfrac{f(-2x+1) - f(0)}{f(1) - f(0)}, & 0 \leq x \leq 0.5, \\ 1 - \dfrac{f(2x-1) - f(0)}{f(1) - f(0)}, & 0.5 < x \leq 1. \end{cases} \tag{16}$$

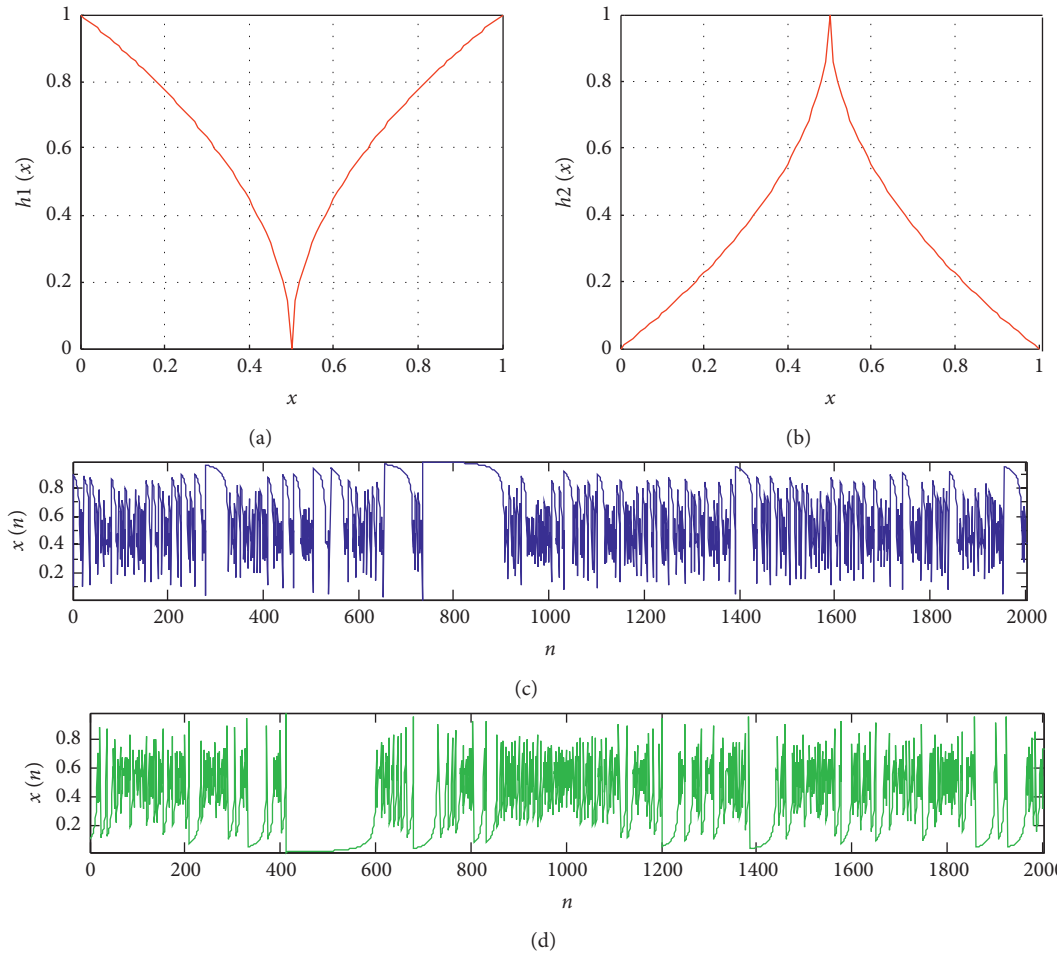

FIGURE 7: Inserting $f(x) = x^{1/2}$ into Theorems 4 and 5, and the function image (a, b) and the time-domain waveform diagram (c, d) are obtained.

If the function h_2 satisfies $h_2'(x) = 2f'(-2x+1)/f(1) - f(0) > 1$ on $[0, 0.5]$, then h_2 is a chaotic map in the sense of Li–Yorke.

Obviously, the mappings of Theorems 4 and 5 also have topological conjugation and satisfy affine conjugation. Therefore, the mappings of Theorems 4 and 5 have the same dynamic behavior.

The following constructs different functions f and inserts them into the above two theorems, yielding specific examples of the constructed functions through numerical simulation.

3.2. Numerical Simulation of Symmetric Piecewise Chaotic Map. Inserting $f(x) = x^{1/2}$ into Theorem 4, the function image and the time-domain waveform of h_1 are as shown in Figures 7(a) and 7(b); if instead substituted into Theorem 5, the function image and the time-domain waveform of h_2 are as shown in Figures 7(c) and 7(d).

Inserting $f(x) = x^5 + x$ into Theorem 4, the function image and the time-domain waveform of h_1 are as shown in Figures 8(a) and 8(b); inserting it into Theorem 5, the function image and the time-domain waveform of h_2 are as shown in Figures 8(c) and 8(d).

Inserting $f(x) = x \cdot (10 \sin x + e^x)$ into Theorem 4, the function image and time-domain waveform of h_1 are as shown in Figures 9(a) and 9(b); if instead substituted into Theorem 5, the function image and time-domain waveform of h_2 are as shown in Figures 9(c) and 9(d).

4. Design of PRNG

In order to design the pseudorandom number generator using the above construction system, we first give a chaotic example satisfying the chaotic condition.

Corollary 1. *Take* $f(x) = \sin x + p \cdot x$, $a = 0.5$, *then when* $p \geq \sin 2$, *the chaos condition can be satisfied in Theorems 1–5, so that equations (1)–(8) are chaotic maps.*

Therefore, if $p = 0.04 > \sin 2$ and $a = 0.5$ are introduced into formula (1), then

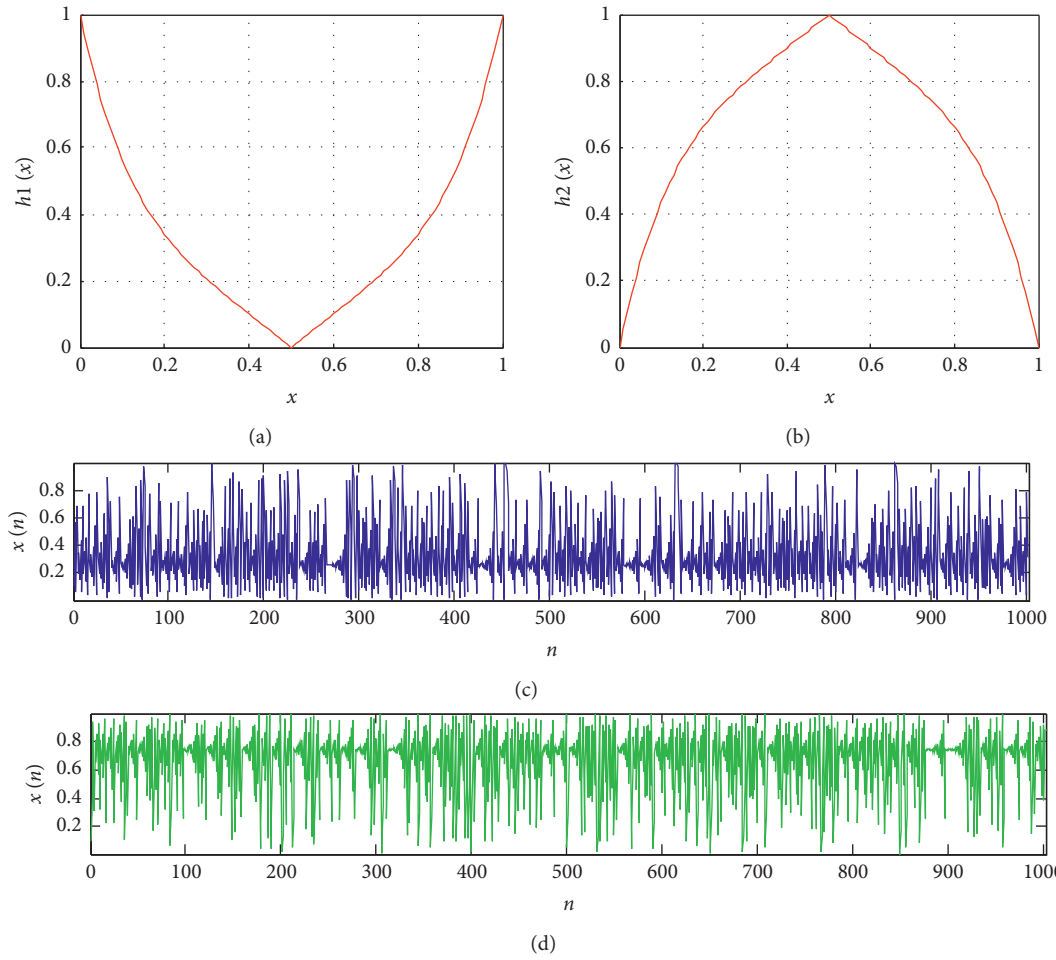

Figure 8: Inserting $f(x) = x^5 + x$ into Theorems 4 and 5, the function image (a, b) and the time-domain waveform diagram (c, d) are obtained.

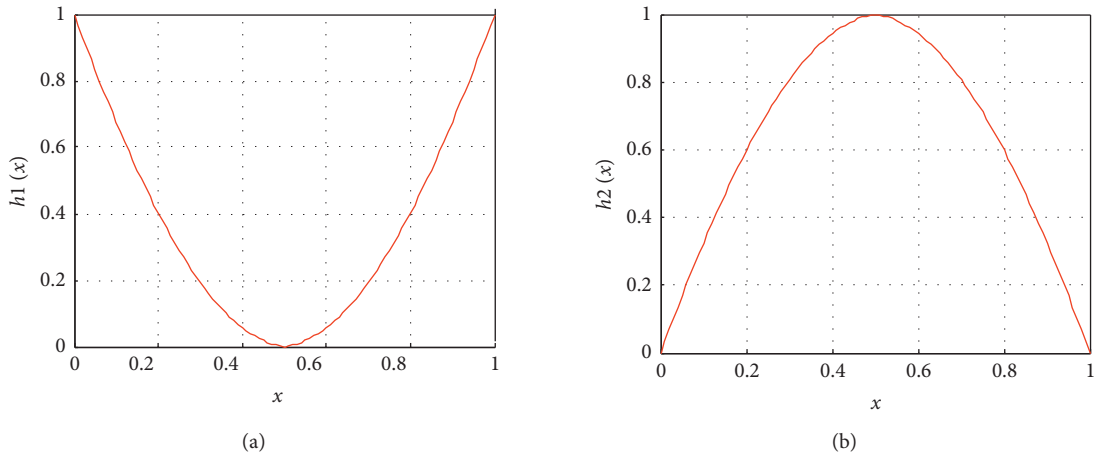

Figure 9: Continued.

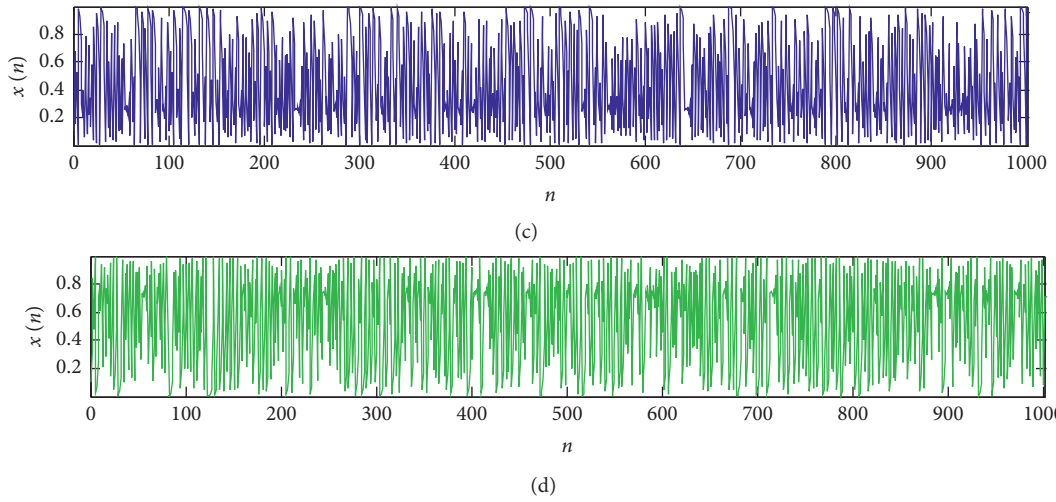

Figure 9: Inserting $f(x) = x \cdot (10 \sin x + e^x)$ into Theorems 4 and 5, the function image (a, b) and the time-domain waveform diagram (c, d) are obtained.

Table 1: The test results of NIST SP800-22.

No.	Test index	PRNG based on system (17)		
		Proportion	P value	Result
1	Frequency	0.9930	0.544254	Success
2	Block frequency	0.9920	0.869278	Success
3	Cumulative sums[1]	0.9920	0.361938	Success
4	Runs	0.9910	0.966626	Success
5	Longest run	0.9920	0.757790	Success
6	Rank	0.9920	0.916599	Success
7	FFT	0.988	0.973718	Success
8	Nonoverlapping template[1]	0.9810	0.678686	Success
9	Overlapping template	0.9900	0.516113	Success
10	Universal	0.9900	0.721777	Success
11	Approximate entropy	0.9860	0.295391	Success
12	Random excursions[1]	0.9983	0.186164	Success
13	Random excursion variant[1]	0.9811	0.202783	Success
14	Serial[1]	0.9920	0.984881	Success
15	Linear complexity	0.9910	0.735908	Success

[1]The test item contains several submodules, of which the worst results are listed here.

$$g_1(x) = \begin{cases} \dfrac{2 \sin x + 0.08x}{\sin 1 + 0.08}, & 0 \le x \le 0.5, \\ \dfrac{2 \sin(1-x) - 0.08x + 0.08}{\sin 1 + 0.08}, & 0.5 < x \le 1. \end{cases} \tag{17}$$

It is a chaotic system.

Based on system (17), a transformation of binary pseudorandom sequence is proposed,

$$\begin{aligned} \mathrm{Tran}(X_k) &= \mathrm{mod}(\mathrm{round}(X_k), 256), \\ s(k) &= \mathrm{binary}(\mathrm{Tran}(X_k)), \end{aligned} \tag{18}$$

where $L = 255\sqrt{2} \times 10^8$, function round$(X)$ means to round x to get an integer, mod(x, n) means to modulo n operation on x, and function binary(x) means to convert integer x into binary number.

4.1. Randomness Test of PRNG. PRNG plays an important role in most chaotic cryptosystems. Because PRNG with good performance is unpredictable and similar to pseudorandom sequence, it has good statistical performance. The following mainly used NIST SP800-22 detection standard [25] proposed by NIST to test the random property of binary pseudorandom sequences generated by chaotic system.

According to system (17), we select 1000 groups of different parameters and initial values, generate 1000 groups of different binary pseudorandom sequences by PRNG, and test the randomness of NIST SP800-22. The results are shown in Table 1.

In Table 1, we give the pass rate of the detection sequence and the P value of the uniformity test (denoted as the UP value). If the pass rate is in the interval $[(1-\alpha) - 3\sqrt{\alpha/n}, (1-\alpha) + 3\sqrt{\alpha/n}]$ and all UP values are greater than α, the PRNG is considered to have passed the

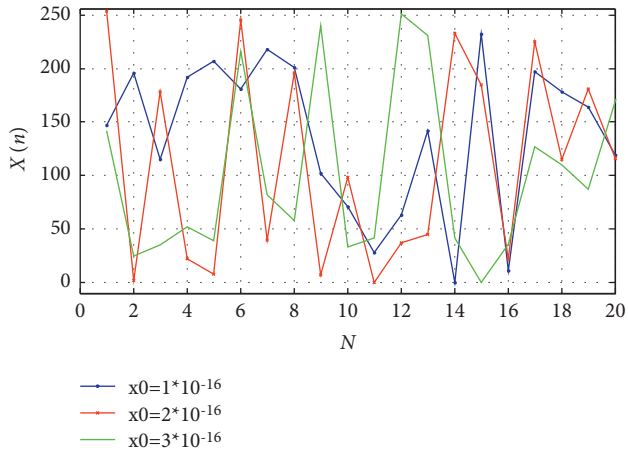

Figure 10: The sequences under different initial secret key.

detection, where α is the significant level, $\alpha = 0.01$ is taken here.

It can be seen from Table 1 that the passing rate of each data of PRNG based on system (17) is within the acceptable range, and it has passed the NIST SP800-22 randomness test, so it is suitable for the design of PRNG and has good randomness.

4.2. Key Sensitivity Analysis. Key sensitivity means that the small change of key will also lead to the substantial change of output. A well-designed PRNG should have good key sensitivity; even if a bit changes, it will output completely different sequences. Therefore, it is necessary to detect and analyze the key sensitivity.

After fixing $n = 1050$, we disturb the initial value of the key. For the three generated sequences, the first 20 arrays are extracted and plotted in Figure 10. It is obvious that the sensitivity of the key to the initial value is above 10^{-16}, and slight changes in the initial value will lead to great differences in the sequence. Therefore, the above test results and analysis show that our generator has strong key sensitivity.

5. Conclusions

In this work, we construct three types of one-dimensional discrete piecewise maps, and based on the Li–Yorke discriminant theorem and Marotto's theorem, we provide sufficient conditions for these three types of maps to become chaotic maps. Then, we design f and further construct several specific examples, after which numerical simulations are carried out. The bifurcation diagram and Lyapunov exponent diagram of the function with the change in parameters are given.

In view of the construction method of the one-dimensional discrete piecewise chaotic maps proposed in this paper, considering the piecewise chaotic map with symmetric properties, we construct the functions on this basis. Sufficient conditions for them to become chaotic maps are given, several examples satisfying the theorem conditions are given, the theory is verified by numerical simulation, and the design idea is proved to be correct. This method can provide a theoretical basis for further constructing a new one-dimensional discrete chaotic system.

Finally, from the perspective of cryptographic application, the PRNG algorithm proposed in this paper is tested. The test results show that the PRNG designed in this paper has passed the sp800-22 randomness test, and the test index value is equivalent to that of the literature [18, 19, 22, 23]. The random performance and key sensitivity are analyzed. The results show that the proposed pseudorandom sequence generator can meet the performance requirements of good PRNG and has strong key sensitivity. Therefore, the PRNG proposed in this paper is practical and reliable and can further design a high security encryption scheme, which has high application potential.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

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

Acknowledgments

This project was supported by "The Fundamental Research Funds for the Central Universities" of China (06108236).

References

[1] T.-Y. Li and J. A. Yorke, "Period three implies chaos," *The American Mathematical Monthly*, vol. 82, no. 10, pp. 985–992, 1975.

[2] F. R. Marotto, "Snap-back repellers imply chaos in Rn," *Journal of Mathematical Analysis and Applications*, vol. 63, no. 1, pp. 199–223, 1975.

[3] I. Sánchez, M. Sanchis, and H. Villanueva, "Chaos in hyperspaces of nonautonomous discrete systems," *Chaos, Solitons & Fractals*, vol. 94, pp. 68–74, 2017.

[4] R. L. Devaney and J. P. Eckmann, "An introduction to chaotic dynamical systems," *Acta Applicandae Mathematicae*, vol. 40, no. 7, p. 72, 1987.

[5] W. Zhou, G. Wang, Y. Shen, F. Yuan, and S. Yu, "Hidden coexisting attractors in a chaotic system without equilibrium point," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 28, no. 7, 2018.

[6] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Processing*, vol. 148, pp. 124–144, 2018.

[7] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyperchaotic system," *Nonlinear Dynamics*, vol. 84, no. 4, pp. 2333–2356, 2016.

[8] M. A. Dastgheib and M. Farhang, "A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period," *Nonlinear Dynamics*, vol. 89, no. 1, pp. 1–10, 2017.

[9] A. Zahedi, H. Timasi, A. Kasaeian, and S. A. Mirnezami, "Design and construction of a new dual CHP-type renewable energy power plant based on an improved parabolic trough solar collector and a biofuel generator," *Renewable Energy*, vol. 135, no. 5, pp. 485–495, 2019.

[10] D. Biswas, S. Seth, and M. Bor, "A study of the dynamics of a new piecewise smooth map," *International Journal of Bifurcation and Chaos*, vol. 30, 2020.

[11] R. Qumsieh, M. Farajallah, and R. Hamamreh, "Joint block and stream cipher based on a modified skew tent map," *Multimedia Tools and Applications*, vol. 78, no. 23, pp. 33527–33547, 2019.

[12] H. Y. Zang and H. Y. Chai, "Homogenization and entropy analysis of a quadratic polynomial chaotic system," *Acta Physica Sinica*, vol. 56, no. 3, 2016.

[13] L. Gardini and W. Tikjha, "Dynamics in the transition case invertible/non-invertible in a 2D piecewise linear map," *Chaos, Solitons & Fractals*, vol. 137, 2020.

[14] W. Tikjha and L. Gardini, "Bifurcation sequences and multistability in a two-dimensional piecewise linear map," *International Journal of Bifurcation and Chaos*, vol. 30, no. 6, 2020.

[15] J. Li, H. Zang, and X. Wei, "On the construction of one-dimensional discrete chaos theory based on the improved version of Marotto's theorem," *Journal of Computational and Applied Mathematics*, vol. 380, 2020.

[16] X. F. Zhang and J. L. Fan, "A new piecewise nonlinear chaotic map and its performance," *Acta Physica Sinica*, vol. 59, no. 4, pp. 2298–2304, 2010.

[17] V. Avrutin, Z. T. Zhusubaliyev, D. Suissa, and A. El Aroudi, "Non-observable chaos in piecewise smooth systems," *Nonlinear Dynamics*, vol. 99, no. 3, pp. 2031–2048, 2020.

[18] E. Zambrano-Serrano, S. Bekiros, M. A. Platas-Garza et al., "On chaos and projective synchronization of a fractional difference map with no equilibria using a fuzzy-based state feedback control," *Physica A: Statistical Mechanics and its Applications*, vol. 578, no. 5, pp. 126100–126115, 2021.

[19] L. Moysis, A. Tutueva, C. Volos, D. Butusov, J. M. Munoz-Pacheco, and H. Nistazakis, "A two-parameter modified logistic map and its application to random bit generation," *Symmetry*, vol. 12, no. 5, pp. 829–840, 2020.

[20] L. Moysis, C. Volos, S. Jafari et al., "Modification of the logistic map using fuzzy numbers with application to pseudorandom number generation and image encryption," *Entropy*, vol. 22, no. 4, pp. 474–494, 2020.

[21] E. E. García-Guerrero, E. Inzunza-González, O. R. López-Bonilla, J. R. Cárdenas-Valdez, and E. Tlelo-Cuautle, "Randomness improvement of chaotic maps for image encryption in a wireless communication scheme using PIC-microcontroller via Zigbee channels," *Chaos, Solitons & Fractals*, vol. 133, pp. 109646–109659, 2020.

[22] L. Fraga, E. Torres-Pérez, E. Tlelo-Cuautle et al., "Hardware implementation of pseudo-random number generators based on chaotic maps," *Nonlinear Dynamics*, vol. 90, no. 2, pp. 1661–1670, 2017.

[23] M. A. Platas-Garza, E. Zambrano-Serrano, J. R. Rodríguez-Cruz et al., "Implementation of an encrypted-compressed image wireless transmission scheme based on chaotic fractional-order systems," *Chinese Journal of Physics*, vol. 71, no. 4, pp. 22–37, 2020.

[24] L. Fraga, C. Mancillas-López, and E. Tlelo-Cuautle, "Designing an authenticated Hash function with a 2D chaotic map," *Nonlinear Dynamics*, vol. 104, no. 1, pp. 4569–4580, 2021.

[25] Y. Wang, Z. Liu, J. Ma, and H. He, "A pseudorandom number generator based on piecewise logistic map," *Nonlinear Dynamics*, vol. 83, no. 4, pp. 2373–2391, 2016.