Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 1496329, 14 pages
http://dx.doi.org/10.1155/2016/1496329

Research Article

A Chaos Robustness Criterion for 2D Piecewise Smooth Map with Applications in Pseudorandom Number Generator and Image Encryption with Avalanche Effect

Dandan Han,[1] Lequan Min,[2] and Longjie Hao[2]

[1] *Schools of Automation and Electrical Engineering, University of Science and Technology Beijing, Beijing 100083, China*
[2] *School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China*

Correspondence should be addressed to Lequan Min; minlequan@sina.com

Received 28 August 2015; Revised 3 January 2016; Accepted 24 January 2016

Academic Editor: Jonathan N. Blakely

This study proposes a chaos robustness criterion for a kind of 2D piecewise smooth maps (2DPSMs). Using the chaos robustness criterion, one can easily determine the robust chaos parameter regions for some 2DPSMs. Combining 2DPSM with a generalized synchronization (GS) theorem, this study introduces a novel 6-dimensional discrete GS chaotic system. Based on the system, a 2^{16}-word chaotic pseudorandom number generator (CPRNG) is designed. The key space of the CPRNG is larger than 2^{996}. Using the FIPS 140-2 test suit/generalized FIPS 140-2 test suit tests the randomness of the 1000 key streams consists of 20,000 bits generated by the CPRNG, the RC4 algorithm, and the ZUC algorithm, respectively. The numerical results show that the three algorithms do not have significant differences. The CPRNG and a stream encryption scheme with avalanche effect (SESAE) are used to encrypt an image. The results demonstrate that the CPRNG is able to generate the avalanche effects which are similar to those generated via ideal CPRNGs. The SESAE with one-time-pad scheme makes any attackers have to use brute attacks to break our cryptographic system.

1. Introduction

The dynamic behaviors of chaotic systems have some specific features, such as their extreme sensitivity to the variables of initial conditions and system parameters, pseudorandom property, and ergodic and topological transitivity. Particularly, the property of sensitive dependence on initial conditions and parameters and robustness are suitably used in information security field [1–4].

Piecewise smooth dynamical systems (PSDSs) can exhibit complex dynamic phenomena, including chaos. PSDSs are particularly relevant in many areas of engineering and applied science. As early as in the last seventies, Feigin published his pioneering work on the analysis of C-bifurcations in n-dimensional PWS systems (e.g., see [5–7]), which proposed the classification of the piecewise linear normal form for two- and three-dimensional piecewise smooth continuous maps. It makes it possible to follow closely the process of emergence of complex structures due to parameter variation.

In 1999, Banerjee and Grebogi [8] redeveloped the classification proposed by Feigin, putting his earlier results in the context of modern bifurcation analysis. Banerjee and Grebogi investigated the various types of border collision bifurcations that can occur in piecewise smooth maps by deriving a piecewise affine approximation of the map in the neighborhood of the border. In di Bernardo et al.'s book [9], the authors offer a very good survey of the rapidly developing area of the dynamics of nonsmooth systems and many beautiful examples of chaotic dynamics induced by nonsmooth phenomena.

Practical applications in chaos-based cryptography require the corresponding chaotic dynamical systems to be robust with respect to system parameters. In [10], Banerjee et al. have shown that such robust chaos can occur in piecewise smooth maps and obtained the conditions of existence of robust chaos. In [8], Banerjee and Grebogi have researched two-dimensional piecewise smooth maps and proposed the corresponding robust chaos theorems.

Since Matthews first proposed a chaotic encryption algorithm [11], there are increasing researches of chaotic encryption technology [12–21]. In [14], a fast chaos-based image encryption system with stream cipher structure is proposed. The major core of the encryption system is a pseudorandom key stream generator based on a cascade of chaotic maps, serving the purpose of sequence generation and random mixing. In [18], a novel image encryption scheme was presented, which uses a chaotic random bits generator. The chaotic random bits generator is based on the coexistence of two different synchronization phenomena. In [19], a novel stream encryption scheme with avalanche effect (SESAE) was introduced. Using the scheme and an ideal pseudorandom number generator to generate a 2^d-word key stream, one can encrypt a plaintext such that by using any key stream generated from a different seed to decrypt the ciphertext, the decrypted plaintext will become an avalanche-like text which has $(2^d - 1)/2^d$ consecutive one's with a high probability.

Based on one theorem proposed by Banerjee and Grebogi, this paper introduces a chaos robustness criterion for a kind of 2-dimensional piecewise smooth maps (2DPSMs) and constructs a 2DPSM with robust chaos feature. Combing the chaos generalized synchronization (GS) theorem with the 2DPSM, this paper proposes a 6-dimensional chaotic generalized synchronization system (6DCGSS) and designs a 2^{16}-word chaotic pseudorandom number generator (CPRNG). At last, using the CPRNG and the SESAE encrypts an RGB image Panda and shows the performance of the CPRNG.

The rest of this paper is organized as follows. Section 2 proposes the chaos robustness criterion for the 2DPSMs and constructs a novel 2DPSM with robust chaos feature. Section 3 introduces the definition and theorem for GS and presents a novel 6DCGSS. Section 4 designs a 2^{16}-word CPRNG and makes the statistic tests for the CPRNG. Section 5 makes an image encryption experiment with avalanche effect. Section 6 performs security analysis on the proposed image encryption scheme. Finally, some concluding remarks are presented in Section 7.

2. The 2-Dimensional Piecewise Robust Chaotic Map

2.1. The Robust Chaos of Normal Form. In [22], Nusse and Yorke have proved that, using some coordinate transformations, any 2-dimensional piecewise smooth map (2DPSM) can be reduced to the normal form in some small neighborhood of the fixed point of the 2DPSM. The normal form is defined as follows:

$$\begin{pmatrix} x(k+1) \\ y(k+1) \end{pmatrix} = \begin{cases} \begin{pmatrix} \tau_L & 1 \\ -\delta_L & 0 \end{pmatrix} \begin{pmatrix} x(k) \\ y(k) \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & \text{if } x \le 0 \\ \begin{pmatrix} \tau_R & 1 \\ -\delta_R & 0 \end{pmatrix} \begin{pmatrix} x(k) \\ y(k) \end{pmatrix} + \mu \begin{pmatrix} 1 \\ 0 \end{pmatrix}, & \text{if } x > 0, \end{cases} \quad (1)$$

where μ is a parameter and $\tau_{L,R}$ and $\delta_{L,R}$ are the traces and determinants of the corresponding matrices of the linearized map in the two subregions R_L and R_R given by

$$\begin{aligned} R_L &= \left\{(x, y) \in R^2,\ x \le 0,\ y \in R\right\}, \\ R_R &= \left\{(x, y) \in R^2,\ x > 0,\ y \in R\right\}. \end{aligned} \quad (2)$$

Banerjee et al. have proposed the robust chaos theorem on the normal form as follows [8, 10].

Theorem 1 (see [8, 10]). *If*

$$\begin{aligned} &0 < \delta_L < 1, \\ &0 < \delta_R < 1, \end{aligned} \quad (3)$$

$$\begin{aligned} &\tau_L > 1 + \delta_L, \\ &\tau_R < -(1 + \delta_R), \end{aligned} \quad (4)$$

$$\begin{aligned} &\delta_L \tau_R \lambda_{1L} - \delta_R \lambda_{1L} \lambda_{2L} + \delta_R \lambda_{2L} - \delta_L \tau_R + \delta_L \tau_L - \delta_L^2 \\ &\quad - \lambda_{2L} \delta_L > 0, \end{aligned} \quad (5)$$

where λ_{1L} and λ_{2L} are the eigenvalues of coefficient matrix, then the 2DPSM has a bifurcation from no attractor to a chaotic attractor. The chaotic attractor for $\mu > 0$ is robust.

Formulas (3)–(5) give the criteria of the chaotic attractor appearing in 2DPSM (1). However, it will be difficult to determine the robust chaos regions for the system parameters.

Based on Theorem 1, this study proposes the following theorem which provides parameters inequalities to determine easily the robust chaos regions for the system parameters.

Theorem 2. *Let $\mu > 0$, $\gamma > 0$. Denote*

$$\tau_R = -(1 + \delta_R) - \gamma. \quad (6)$$

If the following inequalities hold,

$$\begin{aligned} &0 < \delta_L < 1, \\ &0 < \delta_R < 1, \end{aligned} \quad (7)$$

$$\tau_L > 1 + \delta_L, \quad (8)$$

$$\tau_L < \frac{(\gamma + 1 - \delta_L)}{(\gamma + \delta_R)}, \quad (9)$$

then conditions (3)–(5) hold. That is, 2DPSM (1) has a chaotic attractor.

Proof. First, inequalities (6)–(8) are equivalent to conditions (3)-(4). Second, we show that inequality (9) implies that condition (5) holds.

The eigenvalues of coefficient matrix are shown as follows:

$$\begin{aligned}\lambda_{1L} &= \frac{\tau_L + \sqrt{\tau_L^2 - 4\delta_L}}{2},\\ \lambda_{2L} &= \frac{\tau_L - \sqrt{\tau_L^2 - 4\delta_L}}{2}.\end{aligned} \qquad (10)$$

Let $A = \sqrt{\tau_L^2 - 4\delta_L}$; then

$$(\tau_L + A)(\tau_L - A) = \tau_L^2 - A^2 = 4\delta_L. \qquad (11)$$

Substituting (10) into (5) gives

$$\begin{aligned}B &= \delta_L\tau_R\lambda_{1L} - \delta_R\lambda_{1L}\lambda_{2L} + \delta_R\lambda_{2L} - \delta_L\tau_R + \delta_L\tau_L - \delta_L^2\\ &\quad - \lambda_{2L}\delta_L = \delta_L\tau_R\cdot\frac{\tau_L + A}{2} - \delta_R\cdot\frac{\tau_L + A}{2}\cdot\frac{\tau_L - A}{2}\\ &\quad + \delta_R\cdot\frac{\tau_L - A}{2} - \delta_L\tau_R + \tau_L\delta_L - \delta_L^2 - \delta_L\cdot\frac{\tau_L - A}{2}\\ &= \delta_L\tau_R\cdot\frac{\tau_L + A}{2} - \delta_R\delta_L + \delta_R\cdot\frac{\tau_L - A}{2} - \delta_L\tau_R\\ &\quad + \tau_L\delta_L - \delta_L^2 - \delta_L\cdot\frac{\tau_L - A}{2} = \frac{\tau_L\delta_L\tau_R}{2} - \delta_R\delta_L\\ &\quad + \frac{\tau_L\delta_R}{2} - \delta_L\tau_R + \tau_L\delta_L - \delta_L^2 - \frac{\tau_L\delta_L}{2} + \frac{A}{2}(\delta_L\tau_R\\ &\quad - \delta_R + \delta_L) = \frac{1}{2}\left[\tau_L\delta_L\tau_R - 2\delta_L\delta_R + \tau_L\delta_R - 2\delta_L\tau_R\right.\\ &\quad \left. + \tau_L\delta_L - 2\delta_L^2 + A(\delta_L\tau_R - \delta_R + \delta_L)\right].\end{aligned} \qquad (12)$$

Denote

$$\begin{aligned}C &= A(\delta_L\tau_R - \delta_R + \delta_L)\\ &= \sqrt{\tau_L^2 - 4\delta_L}(\delta_L\tau_R - \delta_R + \delta_L)\\ &= \sqrt{\tau_L^2 - 4\delta_L}(\delta_L(\tau_R + 1) - \delta_R)\\ &= -\sqrt{\tau_L^2 - 4\delta_L}(\delta_L(\delta_R + \gamma) + \delta_R)\\ &> -\tau_L(\delta_L(\delta_R + \gamma) + \delta_R) = \tau_L(\delta_L\tau_R - \delta_R + \delta_L).\end{aligned} \qquad (13)$$

Substituting (13) into (12) gives

$$\begin{aligned}B &> \frac{1}{2}\left[\tau_L\delta_L\tau_R - 2\delta_L\delta_R + \tau_L\delta_R - 2\delta_L\tau_R + \tau_L\delta_L - 2\delta_L^2\right.\\ &\quad \left. + \tau_L(\delta_L\tau_R - \delta_R + \delta_L)\right] = \frac{1}{2}\left[2\tau_L\delta_L\tau_R - 2\delta_L\delta_R\right.\\ &\quad \left. - 2\delta_L\tau_R + 2\tau_L\delta_L - 2\delta_L^2\right] = \delta_L\left[\tau_L\tau_R - \delta_R - \tau_R + \tau_L\right.\\ &\quad \left. - \delta_L\right] = \delta_L\left[\tau_L(\tau_R + 1) - (\tau_R + \delta_R) - \delta_L\right]\\ &= \delta_L\left[-\tau_L(\delta_R + \gamma) + (\gamma + 1) - \delta_L\right] = \delta_L\left[(\gamma + 1)\right.\\ &\quad \left. - \gamma\tau_L - \tau_L\delta_R - \delta_L\right] > 0\end{aligned} \qquad (14)$$

because inequality (9) holds. In summary, this completes the proof. □

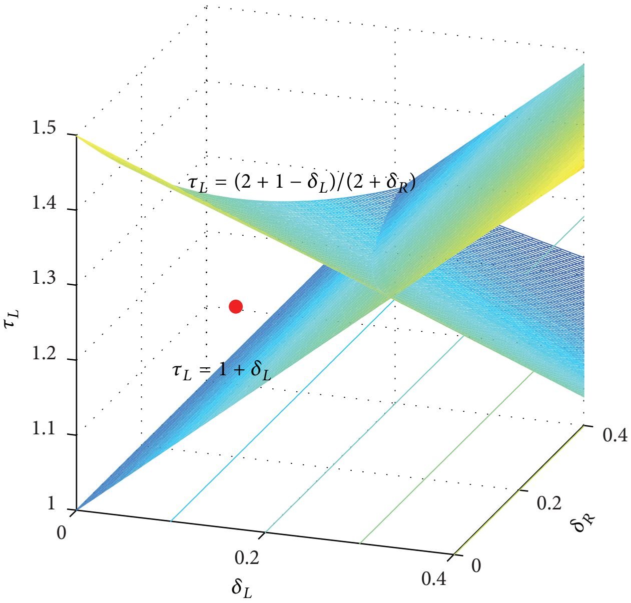


FIGURE 1: The robust chaos regions of parameters $\{\delta_L, \delta_R, \tau_L\}$ for normal form (1) with $\gamma = 2$.

Remark 3. Compared with inequalities (3)–(5), inequalities (6)–(9) more easily determine the robust chaos regions for the system parameters.

For any given nonnegative real numbers γ, one can determine the chaos regions on parameters $\{\delta_L, \delta_R, \tau_L\}$ from inequalities (6)–(9). For example, choosing $\gamma = 2$, the robust chaos regions of 2DPSM are shown in Figure 1. The position of the red dot in Figure 1 is located in the robust chaos region surrounding the two planes.

2.2. A Novel 2DPSM. Let $\gamma = 1$, $\mu = 0.9$, $\delta_L = 0.09$, $\tau_L = 1.5$, $\delta_R = 0.2$, and $\tau_R = -2.2$; then system (1) becomes

$$\begin{pmatrix} x(k+1)\\ y(k+1)\end{pmatrix} = \begin{cases}\begin{pmatrix}1.5 & 1\\ -0.09 & 0\end{pmatrix}\begin{pmatrix}x(k)\\ y(k)\end{pmatrix} + 0.9\begin{pmatrix}1\\ 0\end{pmatrix}, & \text{if } x \le 0\\ \begin{pmatrix}-2.2 & 1\\ -0.2 & 0\end{pmatrix}\begin{pmatrix}x(k)\\ y(k)\end{pmatrix} + 0.9\begin{pmatrix}1\\ 0\end{pmatrix}, & \text{if } x > 0.\end{cases} \qquad (15)$$

The parameters satisfy the conditions given in Theorem 2:

$$\begin{aligned}&\mu > 0,\\ &\gamma > 0,\\ &0 < \delta_L < 1,\\ &0 < \delta_R < 1,\end{aligned}$$

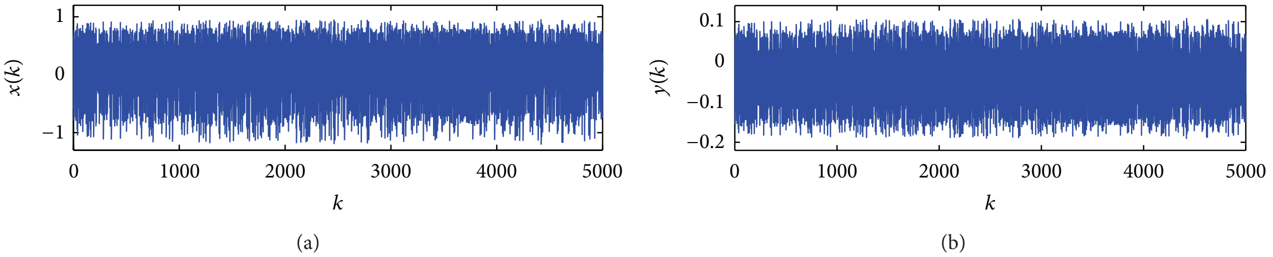


Figure 2: The evolution of state variables: (a) $k-x(k)$ and (b) $k-y(k)$. Here $1 \le k \le 5000$.

$$\tau_L > 1+\delta_L,$$
$$\tau_L < \frac{(\gamma+1-\delta_L)}{(\gamma+\delta_R)}. \tag{16}$$

Therefore system (15) has a chaotic attractor. Select the following initial conditions:

$$x_0 = 0.3,$$
$$y_0 = 0.01. \tag{17}$$

Then, the evolution of state variables $k-x(k)$ and $k-y(k)$ is shown in Figures 2(a)-2(b). Extensive numerical simulations show that the dynamic behaviors of the chaotic map demonstrate chaotic attractor features as the theory expects.

3. A Novel 6DCGSS

3.1. Definition and Theorem on GS. First let us remember the definition and theorem for GS.

Definition 4 (see [23]). Consider two systems

$$\mathbf{X}(k+1) = F(\mathbf{X}(k)), \tag{18}$$
$$\mathbf{Y}(k+1) = G(\mathbf{Y}(k), \mathbf{X}_m(k)), \tag{19}$$

where

$$\begin{aligned}
&\mathbf{X}(k) = (x_1(k), \ldots, x_n(k))^T, \\
&\mathbf{X}_m(k) = (x_1(k), \ldots, x_m(k))^T, \\
&\mathbf{Y}(k) = (y_1(k), \ldots, y_m(k))^T, \quad m \le n, \\
&F(\mathbf{X}(k)) = (f_1(\mathbf{X}(k)), \ldots, f_n(\mathbf{X}(k)))^T, \\
&G(\mathbf{Y}(k), \mathbf{X}_m(k)) \\
&\quad = (g_1(\mathbf{Y}(k), \mathbf{X}_m(k)), \ldots, g_m(\mathbf{Y}(k), \mathbf{X}_m(k)))^T.
\end{aligned} \tag{20}$$

If there exists a transformation $H : \mathbb{R}^m \to \mathbb{R}^m$, where

$$H(\mathbf{X}_m(k)) = (h_1(\mathbf{X}_m(k)), \ldots, h_m(\mathbf{X}_m(k)))^T, \tag{21}$$

and an open subset $B = B_X \times B_Y \subset \mathbb{R}^n \times \mathbb{R}^m$ such that all trajectories of (18) and (19) with initial conditions $(\mathbf{X}(0), \mathbf{Y}(0)) \in B$ satisfy

$$\lim_{k\to+\infty} \|H(\mathbf{X}_m(k)) - \mathbf{Y}(k)\| = 0, \tag{22}$$

then the systems in (18) and (19) are said to be in GS with respect to the transformation $H(\mathbf{X}_m(k))$. System (18) is called the driving system; system (19) is said to be the driven system.

In order to construct the new discrete chaotic system (DCS) with the generalized chaos synchronization (GCS) property, we present the following theorem.

Theorem 5 (see [23]). *Let $\mathbf{X}$, $\mathbf{X}_m$, $\mathbf{Y}$, $F(\mathbf{X})$, and $G(\mathbf{Y}, \mathbf{X}_m)$ be defined by (20).*

Suppose that

$$H(\mathbf{X}_m) = (y_1, y_2, \ldots, y_m)^T \tag{23}$$

is an invertible transformation. If two systems (18) and (19) are in GS via the transformation $H(\mathbf{X}_m)$, then the function $G(\mathbf{Y}, \mathbf{X}_m)$ given in (19) will have the following form:

$$G(\mathbf{Y}, \mathbf{X}_m) = H(F_m(\mathbf{X})) - q(\mathbf{X}_m, \mathbf{Y}), \tag{24}$$

where

$$F_m(\mathbf{X}) = (f_1(\mathbf{X}), f_2(\mathbf{X}), \ldots, f_m(\mathbf{X}))^T \tag{25}$$

and the function

$$\begin{aligned}
&q(\mathbf{X}_m, \mathbf{Y}) \\
&\quad = (q_1(\mathbf{X}_m, \mathbf{Y}), q_2(\mathbf{X}_m, \mathbf{Y}), \ldots, q_m(\mathbf{X}_m, \mathbf{Y}))^T
\end{aligned} \tag{26}$$

guarantees that the zero solution of the following error equation is asymptotically stable:

$$\begin{aligned}
\mathbf{e}(k+1) &= H(\mathbf{X}_m(k+1)) - (\mathbf{Y}(k+1)) \\
&= q(\mathbf{X}_m, \mathbf{Y}).
\end{aligned} \tag{27}$$

3.2. A Novel 6DCGSS. Firstly, we propose a novel 3-dimensional chaotic system based on 2DPSM (15) and a trigonometric function:

$$\begin{pmatrix} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1) \end{pmatrix} = \begin{cases} \begin{pmatrix} 1.5x_1(k) + x_2(k) + 0.9 \\ -0.09x_1(k) \\ \sin(x_1(k) + x_2(k)) - \cos(x_3(k)) \end{pmatrix}, & \text{if } x_1(k) \le 0 \\ \begin{pmatrix} -2.2x_1(k) + x_2(k) + 0.9 \\ -0.2x_1(k) \\ \sin(x_1(k) + x_2(k)) - \cos(x_3(k)) \end{pmatrix}, & \text{if } x_1(k) > 0. \end{cases} \quad (28)$$

2DPSM (15) is chaotic map, and trigonometric functions are bounded function. Hence system (28) is chaotic.

Secondly, let the driving part of the 6DCGSS have the following form with system (28):

$$\mathbf{X}(k+1) = \begin{cases} x_1(k+1) \\ x_2(k+1) \\ x_3(k+1). \end{cases} \quad (29)$$

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

$$H(\mathbf{X}) = A\mathbf{X} \overset{\Delta}{=} (h_1(\mathbf{X}), h_2(\mathbf{X}), h_3(\mathbf{X})), \quad (30)$$

where

$$A = \begin{pmatrix} -3 & 7 & 4 \\ 6 & -2 & -2 \\ 5 & 0 & 6 \end{pmatrix} \quad (31)$$

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

$$\mathbf{Y}(k+1) = \mathbf{AX}(k+1) - \frac{1}{9}(\mathbf{AX}(k) - \mathbf{Y}(k)). \quad (32)$$

From (32), it follows that $q(\mathbf{X}, \mathbf{Y})$ can be represented by $\mathbf{e}(k)/9$. It guarantees that the zero solution of the error equation (27) is asymptotically stable. From Theorem 5, systems (29) and (32) are GS with respect to the transformation $\mathbf{H} = A$ for any initial value $(\mathbf{X}(0), \mathbf{Y}(0)) \in \mathbb{R}^3 \times \mathbb{R}^3$. Since H is invertible, system (32) is also chaotic.

3.3. Numerical Simulations. Select the following initial conditions:

$$\mathbf{X}(0) = (0.3, 0.01, 0.2)^T, \quad (33)$$

$$\mathbf{Y}(0) = A\mathbf{X}(0) + 1. \quad (34)$$

The chaotic orbits of the state variables $\{x_1, x_2, x_3\}$ for the first 5000 iterations are shown in Figures 3(a)–3(d). The evolution of state variables $k - x_1(k)$, $k - x_2(k)$, and $k - x_3(k)$ is shown in Figures 4(a)–4(c).

The chaotic orbits of the state variables $\{y_1, y_2, y_3\}$ for the first 5000 iterations are shown in Figures 5(a)–5(d). The evolution of state variables $k - y_1(k)$, $k - y_2(k)$, and $k - y_3(k)$ is shown in Figures 6(a)–6(c). The dynamic behaviors of the chaotic map demonstrate chaotic attractor characteristics.

Figures 7(a)–7(c) show that although the initial condition (34) has a perturbation, $\mathbf{X}(k)$ and $\mathbf{Y}(k)$ are rapidly conversing into generalized synchronization as Theorem 5 predicts.

4. Bit String CPRNG and Pseudorandomness Tests

4.1. Chaotic Pseudorandom Number Generator. Denote

$$\mathbf{X}_i = \{x_i(k) \mid k = 1, 2, \ldots, N\},$$
$$\mathbf{Y}_i = \{y_i(k) \mid k = 1, 2, \ldots, N\}, \quad (35)$$

where $i = 1, 2, 3$ and x_i's and y_i's are generated by (29) and (32). Introduce a transformation $T_1 : \mathbb{R} \to \{0, 1, \ldots, 2^{16} - 1\}$ which transforms the chaotic streams of systems (35) into key streams:

$$\mathbf{P} = T_1(\mathbf{S}) = \operatorname{mod}\left(\operatorname{round}\left(L\frac{\mathbf{S} - \min(\mathbf{S})}{\max(\mathbf{S}) - \min(\mathbf{S})}, 2^{16}\right)\right). \quad (36)$$

Here

$$\mathbf{S} = \mathbf{X}_2 + \mathbf{X}_3 - \mathbf{Y}_1 - \mathbf{Y}_2 + \mathbf{Y}_3, \quad (37)$$

where $L = 10^{15}$.

Now we can design a CPRNG based on the transformations (36)-(37) and GS systems (29) and (32). The seeds of the CPRNG are the initial conditions of the GS systems, which can be chosen via random number generators. Therefore the output key streams of the CPRNG can be obtained via (36), GS systems (29) and (32).

4.2. Pseudorandomness Tests. The FIPS 140-2 test consists of four subtests: Monobit Test, Poker Test, Runs Test, and Long Runs Test. Each test needs a single stream of 20,000 one and zero bits from the key stream 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 1. The Long Runs 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 Porker Test correspond to significant $\alpha = 10^{-4}$ for the normal cumulative distribution and the χ^2 distribution, respectively, and the required intervals of the Runs Tests correspond approximately to the significant $\alpha = 1.6 \times 10^{-7}$ for the normal cumulative distribution [24, 25]. If we select the significant $\alpha = 10^{-4}$ of all tests,

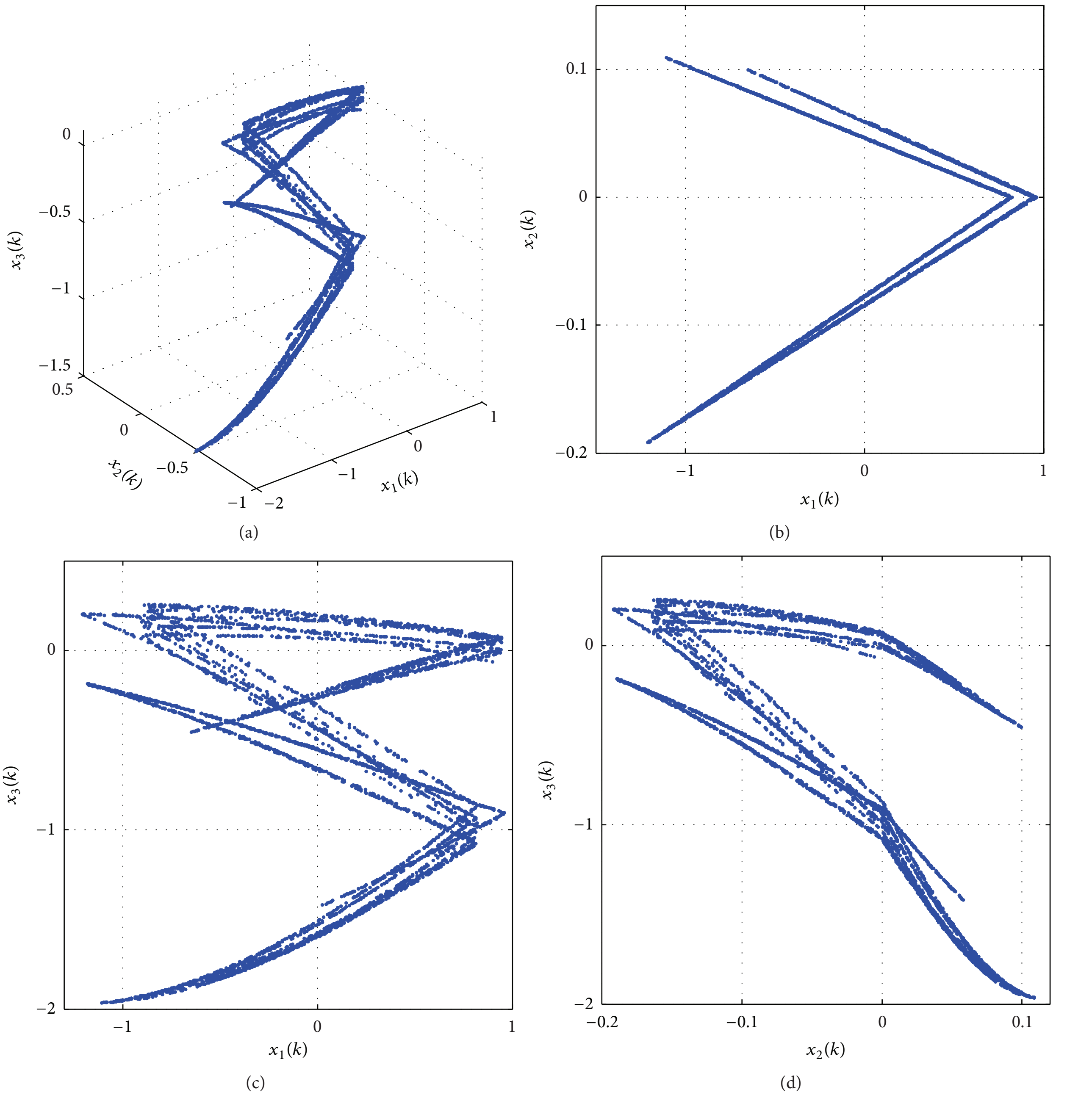


Figure 3: Chaotic trajectories of variables: (a) $x_1(k)-x_2(k)-x_3(k)$, (b) $x_1(k)-x_2(k)$, (c) $x_1(k)-x_3(k)$, and (d) $x_2(k)-x_3(k)$. Here $1 \le k \le 5000$.

the corresponding accepted intervals are listed in the third column in Table 1.

According to Golomb's three postulates on the randomness [26], the ideal values of the first three tests should be those listed in the 4th column in Table 1.

In order to test the pseudorandomness of the CPRNG, we transform the 16-bit stream defined by (36) to the $\{0,1\}$ bit stream as follows.

Construct a transform $T_2 : \{0,1,\ldots,2^{16}-1\} \to \{0,1\}$ which is defined by

$$T_2 = T_{22} \circ T_{21} \tag{38}$$

s.t. for all $\mathbf{y} \in \{0,1,\ldots,2^{16}-1\}^N$:

$$T_{21}(\mathbf{y}) = \text{dec2bin}(\mathbf{y}). \tag{39}$$

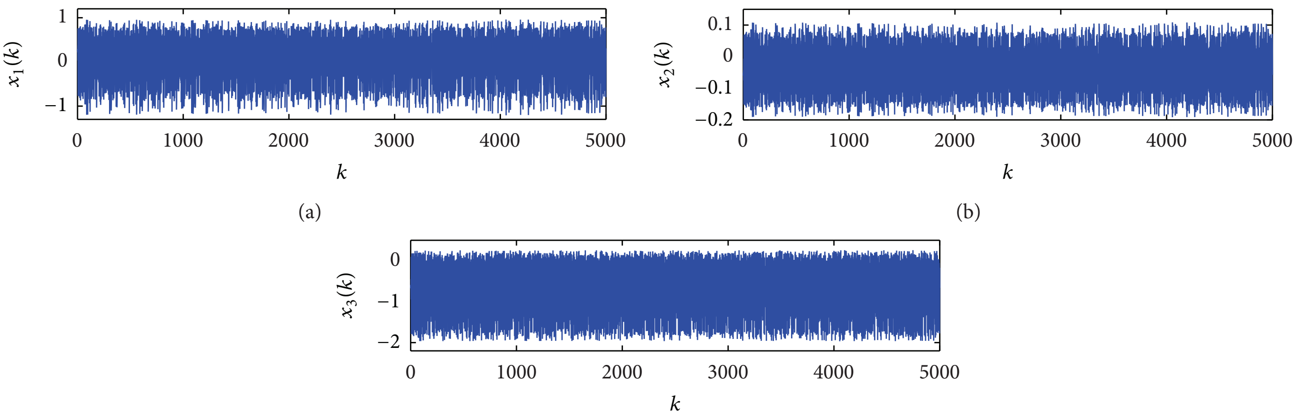
Let $\mathbf{z} = \text{dec2bin}(\mathbf{Y})$; then

$$T_{22}(\mathbf{z}) = \mathbf{z}(:), \tag{40}$$

where dec2bin and $\mathbf{z}(:)$ are both Matlab commands. Then the transformation $T : \mathbb{R} \to \{0,1\}$ is defined via

$$T = T_2 \circ T_1. \tag{41}$$

The FIPS 140-2 test is used to check 1,000 key streams randomly generated by CPRNG with random perturbing of the



(a)

(b)

(c)

FIGURE 4: The evolution of state variables: (a) $k - x_1(k)$, (b) $k - x_2(k)$, and (c) $k - x_3(k)$. Here $1 \le k \le 5000$.

TABLE 1: The required intervals of the FIPS 140-2 Monobit Test, Porker Tests, Runs Test. Here, MT, PT, and LT represent the Monobit Test, the Porker Test, and the Long Runs Test, respectively. k represents the length of the run of a tested sequence. χ^2 DT represents χ^2 distribution.

Test	FIPS 140-2	$\alpha = 10^{-4}$	Golomb's
item	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	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

initial conditions $\mathbf{X}(0)$, $\mathbf{Y}(0)$, the parameters $\{\tau_L, \delta_L, \delta_R, \mu, \gamma\}$, and the parameters of matrix $A = (\alpha_{i,j})$ in the range $|\epsilon| \in [10^{-16}, 10^{-1}]$, respectively.

All sequences pass the FIPS 140-2 test, and there are 12 sequences failing to pass the G FIPS 140-2 test. The statistic test results are listed in the 3rd column in Table 2, in which the statistic results are described by mean values ± standard deviation (Mean ± SD). In [27], a new CPRNG1 was proposed. The test results show that there are 2 sequences failing to pass the FIPS 140-2 test, and there are 23 sequences failing to pass the G FIPS 140-2 test. The statistic test results are listed in the 4th column in Table 2.

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: as shown in Algorithm 1.

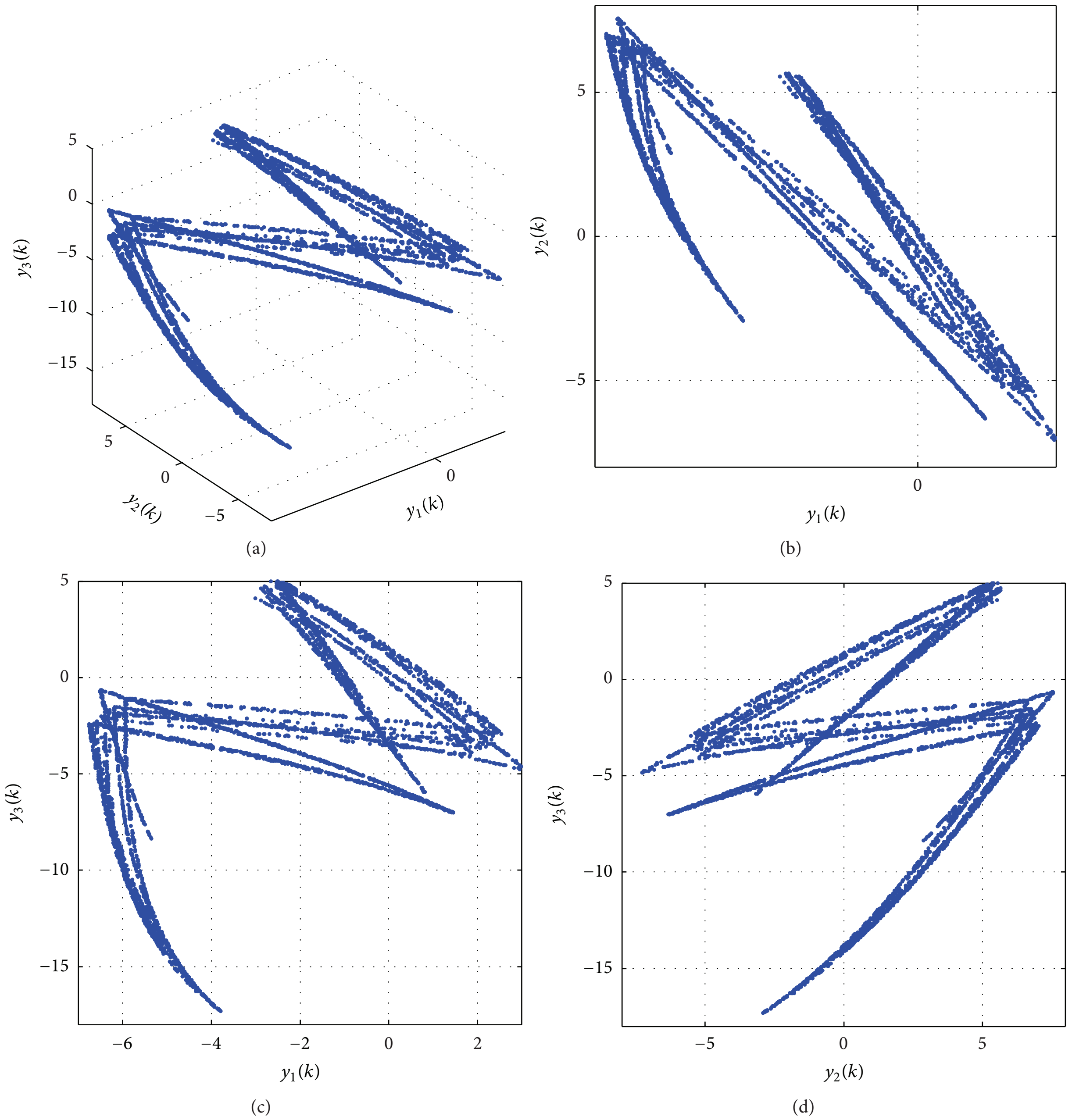
Here, "randi([0 254], 1, 255)" generates a vector of uniformly distributed random integers $\{0, 1, \ldots, 254\}$ of dimension 255; "mod" means taking modulus after division; "zeros(1, N)" is a zero row vector of dimension N.

```
N=20000;
K=randi([0 254],1,255);
S=[0:255-1];j=0;
for i=1:255
         j=mod(j+S(i)+K(i),255);
              Sk=S(j+1);
                 S(j+1)=S(i);
                      S(i)=Sk;
end
        C=zeros(1,N); j=0;i=0; k=1;
for l=1:N/8
           i=mod(i+1,255);
              j=mod(j+S(i+1),255);
                 Sk=S(j+1);
                    S(j+1)=S(i+1);
                       S(i+1)=Sk;
  C(l)=S(mod(S(j+1)+S(i+1),255)+1);
end
  C=(dec2bin(C))';
      C=C(:);
         C=bin2dec(C);
```

ALGORITHM 1

Consequently, the RC4 algorithm PRNG is designed. Now, the FIPS 140-2 test is used to test the 1,000 key streams randomly generated by RC4 algorithm. Results show that 1000 sequences all passed the FIPS 140-2 test criteria and there are 18 sequences failing to pass the G FIPS 140-2 test. The statistic test results are listed in the 5th column in Table 2.

ZUC is a stream cipher that forms the heart of the third-generation partnership project (3 GPP) confidentiality algorithm 128-EEA3 and the 3GPP integrity algorithm 128-EIA3. Now, the FIPS 140-2 test suit is used to test the 1,000 key streams randomly generated by the ZUC algorithm program (see Appendix A in [28]). Results show that the 1000 sequences all passed the FIPS 140-2 test criteria, and there are 21 sequences failing to pass the G FIPS 140-2 test criteria. The statistic test results are listed in the 6th column in Table 2.



(a)

(b)

(c)

(d)

FIGURE 5: 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) $y_2(k)-y_3(k)$. Here $1 \le k \le 5000$.

Observing the statistical properties of the pseudorandomness of the sequences generated via the new CPRNG, RC4 algorithm, and the ZUC algorithm, we can find that the three algorithms do not have significant differences. And compared with CPRNG1, the new CPRNG has better randomness performance.

4.3. Key Space. The key set parameters of CPRNG include the initial conditions $\mathbf{X}(0)$, $\mathbf{Y}(0)$, the parameters set $\{\tau_L, \delta_L, \delta_R, \mu, \gamma\}$, and the matrix $A = (\alpha_{i,j})$. It can be proved that if the perturbation matrix $\Delta = (\delta_{i,j})$ satisfies

$$\left|\delta_{i,j}\right| < 0.98217 \tag{42}$$

the matrix $A + \Delta$ is still invertible. Therefore the CPRNG has $3 + 3 + 5 + 9$ key parameters denoted by

$$\mathbf{K}_s = \{k_1, k_2, \dots, k_{20}\}. \tag{43}$$

Let the key set be perturbed by

$$\mathbf{K}_s(\Delta) = \mathbf{K}_s + [\delta_1, \delta_2, \dots, \delta_{20}], \tag{44}$$

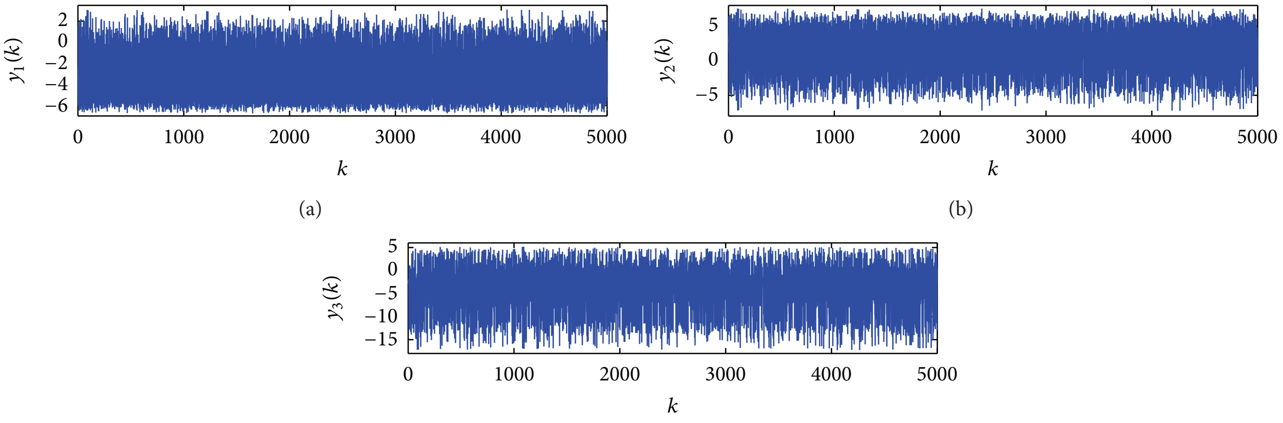
where

$$10^{-16} \le \left|\delta_i\right| \le 10^{-1}, \quad i = 1, \dots, 20. \tag{45}$$

The Matlab platform uses double precision decimal computations. That means that each computed decimal number

Table 2: The tested Mean ± SD of the FIPS 140-2 tested values of 1,000 key streams generated by the new CPRNG, CPRNG1 [27], the RC4, and ZUC CPRNG. Here, MT, PT, and LT represent Monobit Test, Poker Test, and Long Runs Test. SD represents the standard diviation.

Test item	Bits	CPRNG	CPRNG1	RC4	ZUC
		Mean ± SD	Mean ± SD	Mean ± SD	Mean ± SD
MT	0	10000 ± 71.328	10009 ± 73.288	10001 ± 71.472	9998.4 ± 71.843
	1	9999.4 ± 71.328	9991.2 ± 73.280	9999.2 ± 71.278	10002 ± 71.843
PT	—	15.040 ± 5.6514	15.208 ± 5.5133	15.022 ± 5.4730	15.043 ± 5.5491
LT	0	13.587 ± 1.8830	13.874 ± 1.8710	14.004 ± 2.0635	13.488 ± 1.829
	1	13.558 ± 1.7747	13.699 ± 2.0661	13.596 ± 1.8759	13.595 ± 1.9305
k	Bits	Run Test	Run Test	Run Test	Run Test
1	0	2499.6 ± 46.302	2496.4 ± 46.026	2501.1 ± 49.008	2501.9 ± 45.735
	1	2498.8 ± 45.166	2499.5 ± 47.159	2500.9 ± 46.437	2502.7 ± 46.121
2	0	1249.9 ± 31.556	1250.2 ± 32.381	1251.2 ± 31.473	1252.1 ± 32.606
	1	1250.5 ± 32.686	1247.6 ± 32.23	1249.8 ± 32.095	1249.5 ± 32.221
3	0	624.36 ± 22.817	623.05 ± 22.889	624.67 ± 22.545	624.09 ± 22.648
	1	625.75 ± 23.483	624.86 ± 23.33	625.35 ± 23.071	624.64 ± 23.455
4	0	312.86 ± 16.369	312.34 ± 16.687	312.50 ± 16.961	312.56 ± 16.748
	1	312.49 ± 16.970	312.21 ± 16.986	312.04 ± 16.874	312.72 ± 16.506
5	0	156.70 ± 12.068	156.21 ± 12.303	156.00 ± 12.713	155.65 ± 12.097
	1	155.74 ± 12.134	155.711 ± 11.773	155.94 ± 12.245	156.66 ± 12.369
6+	0	156.03 ± 12.079	157.94 ± 11.808	156.21 ± 12.331	155.75 ± 11.719
	1	156.10 ± 11.785	156.27 ± 12.441	156.29 ± 12.372	155.82 ± 11.497



(a)

(b)

(c)

Figure 6: The evolution of state variables: (a) $k - y_1(k)$, (b) $k - y_2(k)$, and (c) $k - y_3(k)$. Here $1 \le k \le 5000$.

has 16 bits' accuracy. Therefore for each perturbed key parameter $k_i + \delta_i$ (please see formula (44)), $|\delta_i| \in [10^{-16}, 10^{-1}]$; that is, δ_i has a representation:

$$\delta_i = 0.0a_2a_3 \cdots a_{16}, \tag{46}$$

where

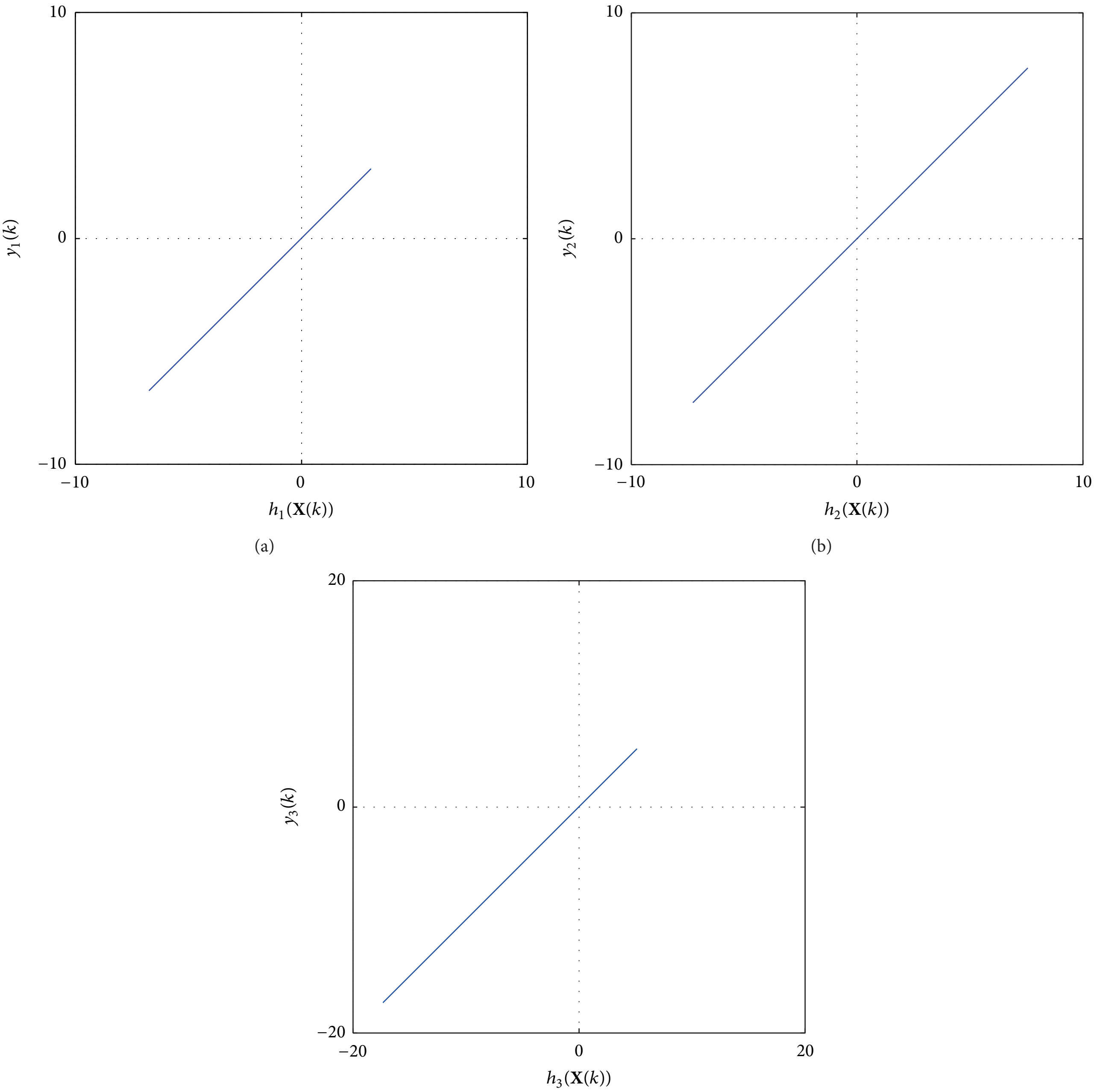
$$a_i \in [0, 1, \ldots, 9]. \tag{47}$$

Therefore, there are larger 10^{15} possible key values. According to the permutation and combination theory, our 20 keys have a key space which is larger than $10^{20\times 15} > 2^{996}$.

4.4. The Correlation of Key Stream. Now we compare the difference between the key stream $S = T(\mathbf{S})$ with 20000-code length generated by key set (43) with the key streams S_p's generated by perturbed key set (44), respectively.

The comparing results are shown in the 3rd column in Table 3. Observe that the average percent of different codes is 50.029%. It is very close to the ideal different value of 50%. Here SV represents statistic values, DC represents different codes, and CC represents correlation coefficients between the key stream and the perturbed key streams.

Let us compare 1000 different codes with length 20000 and the correlation coefficients of the key streams S_p's, S_{1p}'s, S_r's, and S_z's generated via our CPRNG, the CPRNG1 [27],



(a)

(b)

(c)

Figure 7: 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) $h_3(\mathbf{X}(k)) - y_3(k)$. Here $1 \leq k \leq 5000$.

Table 3: The statistic data for the percentages of the codes of the key streams variations between S and S_p's, S_1 and S_{1p}'s, S_{r0} and S_r's, and S_{z0} and S_z's.

Item	SV	S_p's	S_{1p}'s	S_r's	S_z's
DC	Min	48.995%	48.625%	48.765%	48.845%
	Mean	50.029%	49.995%	49.987%	50.014%
	Max	50.950%	51.020%	51.230%	51.120%
CC	Min	0.0000030	0.0000007	0.0000018	0.0000022
	Mean	0.0055411	0.0054141	0.0057124	0.0055848
	Max	0.0201125	0.027542	0.0246616	0.0230973

Table 4: The statistic data for the percentages of the codes of the key streams variations between S and S_m's, S_1 and S_m's, S_{r0} and S_m's, and S_{z0} and S_m's.

Item	SV	S	S_1	S_{r0}	S_{z0}
DC	Min	48.920%	48.955%	48.855%	49.050%
	Mean	49.989%	50.016%	49.980%	50.005%
	Max	51.265%	51.110%	50.900%	51.050%
CC	Min	0.0000054	0.0000049	0.0000077	0.0000010
	Mean	0.0056671	0.0055194	0.0058262	0.0056874
	Max	0.0252603	0.0222300	0.0228920	0.0209927

RC4 algorithm PRNG, and ZUC algorithm PRNG, respectively. The comparing results are shown in Table 3. Compare the unperturbed key streams S, S_1 [27], S_{r0}, and S_{z0} of each PRNG with the 1000 key streams S_m's generated by the Matlab function randi([0 1], 1, 20000). The comparing results are shown in Table 4.

The results suggest that the key streams generated via the perturbed keys of our CPRNG are almost completely independent.

5. A SESAE Experiment on CPRNG

Based on the 2^{16}-word CPRNG defined by (36) and the stream encryption scheme with avalanche effect (SESAE) [19], this subsection investigates an image encryption example. And the secret key is changed for each plaintext.

First, let us remember the definition of SESAE.

Definition 6 (see [19]). Let $P = \{p_1, p_2, \ldots, p_n\}$ be a binary key stream with d-bit segments generated by a pseudorandom number generator (PRNG), let $M = \{m_1, m_2, \ldots, m_n\}$ be a binary plaintext steam, and let $C = \{c_1, c_2, \ldots, c_n\}$ be a ciphertext stream. Then the stream encryption scheme with avalanche effect (SESAE) is described as follows.

(1) The ciphertext $C = E(M, P)$ is determined by

$$c_i = \begin{cases} p_i, & \text{if } m_i = 0 \\ \sim p_i, & \text{if } m_i = 1, \end{cases} \tag{48}$$

where $\sim p_i$ is defined as the bit string obtained by replacing all "1"s in p_i with "0"s and all "0"s in p_i with "1"s.

(2) The corresponding decrypted plaintext $M = E^{-1}(C, P)$ is determined by

$$m_i = \begin{cases} 0, & \text{if } p_i = c_i \\ 1, & \text{if } p_i \neq c_i. \end{cases} \tag{49}$$

Definition 7 (see [19]). A PRNG, S, which generates binary d-bit key streams, is called an ideal PRNG, if S has the following properties:

(1) The period of any key stream generated by the PRNG is larger than 2^d. Its seed space and key space are larger than 2^{512}.

(2) In one period of pseudorandom key streams generated by the PRNG, the distribution of different d-bit segments in the key stream is homogenous. That is, if the period $p = n \times 2^d$, then the number of each different d-bit segment is equal to n. If the period p is not an integer multiple of 2^d, then the difference between the numbers of different d-bit segments is at most one.

(3) The two key streams $\mathscr{P}_1$, $\mathscr{P}_2$ generated by any two different seeds have $(2^d - 1)/2^d \times 100\%$ different d-bit segments.

Now let us consider a SESAE experiment on CPRNG, encrypting and decrypting an RGB image "Panda" with 128× 128 pixels as shown in Figure 8(a).

(1) A sender transforms the image Panda to a binary plaintext steam $M = \{m_1, m_2, \ldots, m_n\}$, where $n = 128 \times 128 \times 3 \times 8$.

(2) The sender uses CPRNG (36) with initial conditions (33) and (34) to generate a 2^{16}-word key stream with length $n + 1000$. And then drop the first 1000 iterative values to obtain a key stream:

$$P = \{p_1, p_2, \ldots, p_n\}. \tag{50}$$

(3) The sender uses formula (48) to encrypt the plaintext steam M, obtaining a ciphertext $C = E(M, P)$.

(4) The receiver uses formula (49) to decrypt the ciphertext and obtain a decrypted plaintext image $M = E^{-1}(C, P)$ without errors (see Figure 8(b)).

(5) Randomly disturb initial conditions (33) and (34), the parameters, and matrix (31), for 1000 times in the range $|\epsilon| \in [10^{-16}, 10^{-1}]$, to obtain key streams (dropping the first 1000 iterative values):

$$P_i, \quad i = 1, 2, \ldots, 1000. \tag{51}$$

(6) Use $\{P_1, \ldots, P_{1000}\}$ to decrypt the ciphertext and obtain decrypted plaintext, respectively:

$$\overline{M}_i = E^{-1}(C, P_i), \quad i = 1, \ldots, 1000. \tag{52}$$

(7) Change $\overline{M}_i$ to RGB images.

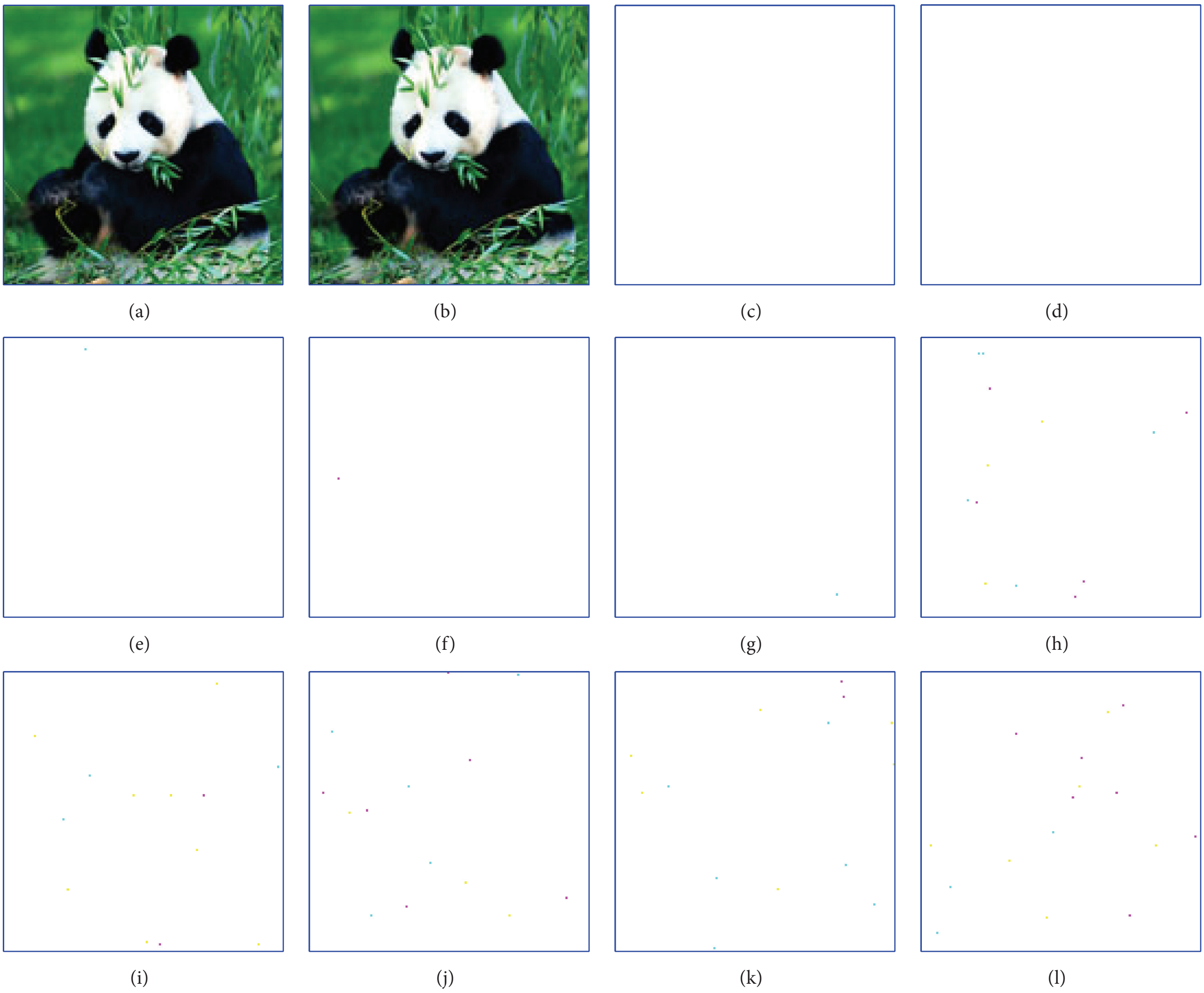


Figure 8: (a) Original image beach. (b) Decrypted image without error. Ten decrypted images via key streams generated with slightly perturbed initial conditions and system parameters in the range $[10^{-16}, 10^{-1}]$: (c) $I_{0,1}$, (d) $I_{0,2}$, (e) $I_{1,1}$, (f) $I_{1,2}$, (g) $I_{1,3}$, (h) $I_{13,6}$, (i) $I_{13,7}$, (j) $I_{14,1}$, (k) $I_{14,2}$, and (l) $I_{16,1}$.

In order to increase the security of the SESAE, we now propose one-time-pad scheme as follows: Let $K_s \subset R^n$ be the seed space (i.e., perturbed initial conditions (33) and (34)). Sender Alice and receiver Bob share a secret function $f : K_s \to K_s$. In the simplest case, f can be chosen as an invertible matrix. Before each communication, Alice selects randomly an element $k \in K_s$ and sends it to Bob. Then, they can use f as the seed for one-time encryption.

6. Security Analysis

A good encryption scheme should be able to resist all kinds of known attacks, such as statistical attack and differential attack. This study has performed some security analyses on the proposed image encryption scheme, including key space analysis, key sensitivity analysis, and correlation analysis. They have demonstrated the security of the SESAE.

6.1. Key Space Analysis. The size of the key space is the total number of different keys that can be used in the encryption. The Matlab platform uses double precision decimal computations. That means that each computed decimal number has 16 bits' accuracy.

Therefore, the size of the key space for our 20 keys is larger than $10^{15\times20} > 2^{996}$. The key space is large enough to make brute-force attacks infeasible.

6.2. Key Sensitivity Analysis. After changing $\overline{M_i}$ to RGB images, all images become almost pure white images. There are total of 393216 $\{0, 1\}$ codes in each decrypted image. Among the decrypted images, the minimum number of 0s in the decrypted images is 0 and the maximum one is 16. Let $I_{i,j}$ denote the jth image having number "i" of 0 codes.

The first five decrypted images with minimum zero codes and the last five images with maximum zero codes (denoted

Table 5: The statistical data of the first 10 images with minimum "0"s codes and the last 10 decrypted images with maximum "0"s codes.

Images	N_1	N_2	Percentage	Images	N_1	N_2	Percentage
$I_{0,1}$	0	0	100	$I_{13,1}$	13	13	99.9966
$I_{0,2}$	0	0	100	$I_{13,2}$	13	13	99.9966
$I_{1,1}$	1	1	99.9997	$I_{13,3}$	13	13	99.9966
$I_{1,2}$	1	1	99.9997	$I_{13,4}$	13	13	99.9966
$I_{1,3}$	1	1	99.9997	$I_{13,5}$	13	13	99.9966
$I_{1,4}$	1	1	99.9997	$I_{13,6}$	13	13	99.9966
$I_{1,5}$	1	1	99.9997	$I_{13,7}$	13	13	99.9966
$I_{1,6}$	1	1	99.9997	$I_{14,1}$	14	14	99.9964
$I_{1,7}$	1	1	99.9997	$I_{14,2}$	14	14	99.9964
$I_{1,8}$	1	1	99.9997	$I_{16,1}$	16	16	99.9959

Table 6: Differences between the original keystream S_0 and the keystreams $S_{i,j}$, measured by norm $\|S_0 - S_{i,j}\|$.

	$\|S_0 - S_{i,j}\|(\times 10^{-1})$				
	$S_{3,1}$	$S_{4,1}$	$S_{4,2}$	$S_{4,3}$	$S_{4,4}$
S_0	0.25520	0.28385	0.24254	0.27552	0.24290
	$S_{24,1}$	$S_{24,2}$	$S_{25,1}$	$S_{25,2}$	$S_{27,1}$
S_0	0.5253	0.30803	0.28799	0.23376	0.29791

by $I_{0,1}$, $I_{0,2}$, $I_{1,1}$, $I_{1,2}$, $I_{1,3}$, $I_{13,6}$, $I_{13,7}$, $I_{14,1}$, $I_{14,2}$, and $I_{16,1}$, resp.) are shown in Figures 8(c)–8(l), respectively.

Table 5 lists the statistical data of the first 10 decrypted images with minimum "0"s codes and the last 10 decrypted images with maximum "0"s codes. Here N_1 and N_2 represent the number of "0"s and the number of the color pixels with brightness less than 255, respectively. Percentage represents the percentage of "1" codes in the decrypted image.

Observe that the percentages of the numbers of "1" codes are in the range [99.9959%, 100%], which is very close to the ideal value $(2^{16} - 1)/2^{16} \times 100\% \approx 99.9984\%$ [19].

In summary, the simulation shows that using the image encrypting algorithm to encrypt RGB images is able to generate encrypted images with significant avalanche effects and be sensitive with respect to the secret key.

6.3. Correlation Analysis. Table 6 lists some statistic data of the norms between the original key stream S_0 and the key stream $S_{i,j}$ used in the ten decrypted images shown in Figures 8(c)–8(l), respectively.

The comparison results show that in the norms between the original image and the corresponding decrypted images there are no significant correlations.

7. Conclusions

The main results of this paper are summarized as follows:

(1) It proposes a chaos robustness criterion theorem which provides parameter inequalities to determine easily the robust chaos parameters regions for the 2DPSM. And a novel 2DPSM is designed to illustrate the theorem.

(2) It constructs a 6-dimensional chaotic GS system (6DCGSS), based on the 2DPSM and the GS theorem. Using the 6DCGSS, we design a 2^{16}-word CPRNG. The key space of the CPRNG is larger than 2^{996}, which is large enough against brute-force attacks.

(3) It compares the testing results by the FIPS 140-2 test suit/generalized FIPS 140-2 test suit for 1000 key streams consisting of 20,000 bits generated by the CPRNG, the RC4 algorithm, and the ZUC algorithm, respectively. The numerical results show that the three algorithms do not have significant differences. And compared with CPRNG1, the new CPRNG has better randomness performance.

(4) It shows an image encryption example by using the CPRNG and SESAE. The simulation results suggest that the decrypted ciphertext will become a monotone white text if a key stream is used with different seeds generated by CPRNG to decrypt the ciphertext. The results show that the encrypted image has significant avalanche effect.

Furthermore, to prevent opponents' attacks, we propose "one-time-pad" scheme. In summary, chaotic map criterion Theorem 2 and generalized synchronization Theorem 5 make us able to design CPRNGs with large key space, which have function similar to one-time-pad scheme.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

This project is jointly supported by the National Natural Science Foundation of China (Grant nos. 61074192, 61170037).

References

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

[2] H.-X. Wang, C. He, and K. Ding, "Robust public watermarking based on chaotic map," *Journal of Software*, vol. 15, no. 8, pp. 1245–1251, 2004.

[3] X. Shi and Z. Wang, "Robust chaos synchronization of four-dimensional energy resource system via adaptive feedback control," *Nonlinear Dynamics*, vol. 60, no. 4, pp. 631–637, 2010.

[4] X. L. Yang, G. Yang, and W. Zhu, "Encryption system based on virtual optical and spatiotemporal chaos," *Computer Engineering and Applications*, vol. 50, no. 1, pp. 68–73, 2014.

[5] M. I. Feigin, "Doubling of the oscillation period with C-bifurcations in piecewise continuous systems," *Journal of Applied Mathematics and Mechanics*, vol. 34, pp. 861–869, 1970.

[6] M. I. Feigin, "On the generation of sets of subharmonic modes in a piecewise continuous system," *Journal of Applied Mathematics and Mechanics*, vol. 38, pp. 810–818, 1974.

[7] M. I. Feigin, "On the structure of C-bifurcation boundaries of piecewise-continuous systems," *Journal of Applied Mathematics and Mechanics*, vol. 42, no. 5, pp. 885–895, 1978.

[8] S. Banerjee and C. Grebogi, "Border collision bifurcations in two-dimensional piecewise smooth maps," *Physical Review E*, vol. 59, no. 4, pp. 4052–4061, 1999.

[9] M. di Bernardo, C. J. Budd, A. R. Champneys, and P. Kowalczyk, *Piecewise-Smooth Dynamical Systems: Theory and Applications*, Springer, London, UK, 2008.

[10] S. Banerjee, J. A. Yorke, and C. Grebogi, "Robust chaos," *Physical Review Letters*, vol. 80, no. 14, pp. 3049–3052, 1998.

[11] R. Matthews, "On the derivation of a chaotic encryption algorithm," *Cryptologia*, vol. 13, no. 1, pp. 29–42, 1989.

[12] J. Fridrich, "Image encryption based on chaotic maps," in *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics, Computational Cybernetics and Simulation*, vol. 2, pp. 1105–1110, Orlando, Fla, USA, October 1997.

[13] M. Salleh, S. Ibrahim, and I. F. Isnin, "Enhanced chaotic image encryption algorithm based on Baker's map," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '03)*, vol. 2, pp. II508–II511, Bangkok, Thailand, May 2003.

[14] H. S. Kwok and W. K. S. Tang, "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons & Fractals*, vol. 32, no. 4, pp. 1518–1529, 2007.

[15] N. Singh and A. Sinha, "Optical image encryption using Hartley transform and logistic map," *Optics Communications*, vol. 282, no. 6, pp. 1104–1109, 2009.

[16] C.-K. Chen, C.-L. Lin, C.-T. Chiang, and S.-L. Lin, "Personalized information encryption using ECG signals with chaotic functions," *Information Sciences*, vol. 193, pp. 125–140, 2012.

[17] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, "A novel image encryption algorithm based on chaotic maps and GF(2^8) exponent transformation," *Nonlinear Dynamics*, vol. 72, no. 1-2, pp. 399–406, 2013.

[18] C. K. Volos, I. M. Kyprianidis, and I. N. Stouboulos, "Image encryption process based on chaotic synchronization phenomena," *Signal Processing*, vol. 93, no. 5, pp. 1328–1340, 2013.

[19] L. Min and G. Chen, "A novel stream encryption scheme with avalanche effect," *The European Physical Journal B*, vol. 86, article 459, 2013.

[20] N. Hazarika and M. Saikia, "A novel partial image encryption using chaotic logistic map," in *Proceedings of the 1st International Conference on Signal Processing and Integrated Networks (SPIN '14)*, pp. 231–236, Noida, India, February 2014.

[21] J. Yang, Y. Chen, and F. Zhu, "Singular reduced-order observer-based synchronization for uncertain chaotic systems subject to channel disturbance and chaos-based secure communication," *Applied Mathematics and Computation*, vol. 229, pp. 227–238, 2014.

[22] H. E. Nusse and J. A. Yorke, "Border-collision bifurcations including 'period two to period three' for piecewise smooth systems," *Physica D*, vol. 57, no. 1-2, pp. 39–57, 1992.

[23] H. Y. Zang, L. Q. 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.

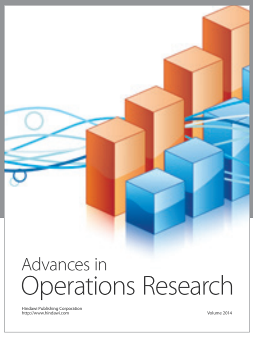
[24] L. Q. Min, H. J. Hao, and L. J. Zhang, "Study on the statistical test for string pseudorandom number generators," in *Advances in Brain Inspired Cognitive Systems*, vol. 7888, pp. 278–287, Springer, Berlin, Germany, 2013.

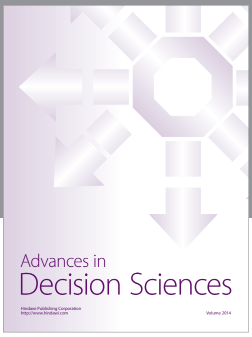
[25] L. Q. Min, T. Y. Chen, and H. Y. Zang, "Analysis of FIPS 140-2 test and chaos-based pseudorandom number generator," *Chaotic Modeling and Simulation*, vol. 2, pp. 273–280, 2013.

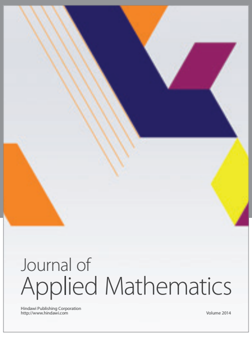
[26] S. Golomb, *Shift Register Sequences*, Aegean Park Press, Walnut Creek, Calif, USA, 1981.

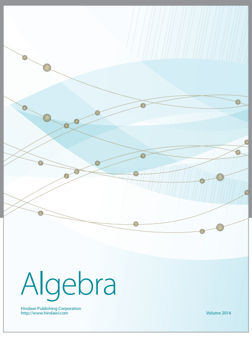
[27] L. Min, X. Lan, L. Hao, and X. Yang, "A 6 dimensional chaotic generalized synchronization system and design of pseudorandom number generator with application in image encryption," in *Proceedings of the 10th International Conference on Computational Intelligence and Security (CIS '14)*, pp. 356–362,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

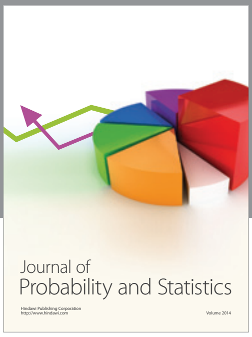
[28] ETSI/SAGE Specification, *Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3*, Document 2: ZUC Specification; Version: 1.5, 2011.


Advances in
Operations Research

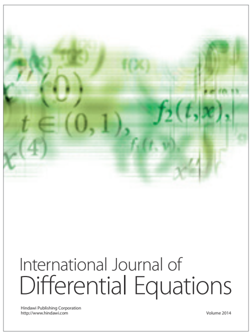

Advances in
Decision Sciences


Journal of
Applied Mathematics

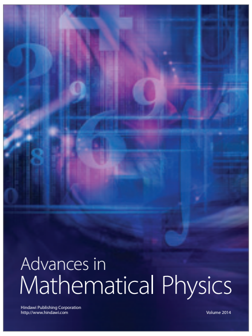

Algebra

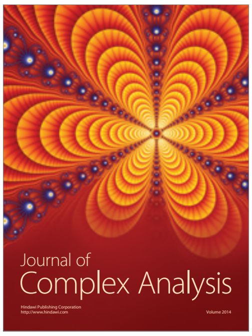

Journal of
Probability and Statistics

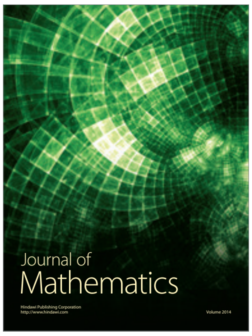
The Scientific
World Journal

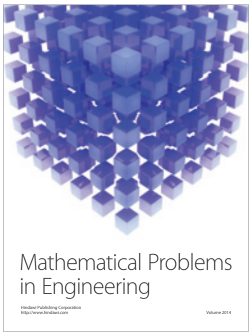

International Journal of
Differential Equations

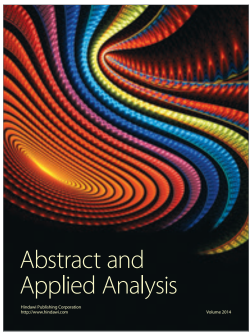
International Journal of
Combinatorics

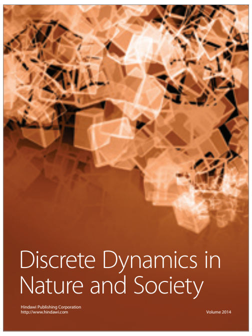

Advances in
Mathematical Physics

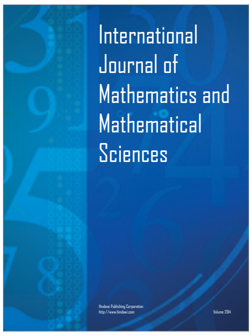

Journal of
Complex Analysis


Journal of
Mathematics


Mathematical Problems
in Engineering

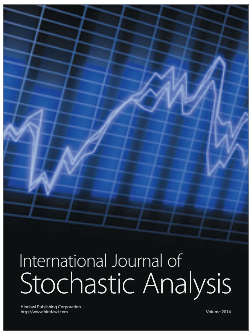

Abstract and
Applied Analysis


Discrete Dynamics in
Nature and Society


International
Journal of
Mathematics and
Mathematical
Sciences

Journal of
Discrete Mathematics

Journal of
Function Spaces


International Journal of
Stochastic Analysis

Journal of
Optimization