Hindawi Publishing Corporation
Mathematical Problems in Engineering
Volume 2016, Article ID 8973583, 11 pages
http://dx.doi.org/10.1155/2016/8973583

Research Article

The Design and Its Application in Secure Communication and Image Encryption of a New Lorenz-Like System with Varying Parameter

Lilian Huang, Donghai Shi, and Jie Gao

Harbin Engineering University, Harbin, Heilongjiang 150001, China

Correspondence should be addressed to Lilian Huang; lilian_huang@163.com

Received 9 October 2015; Revised 8 December 2015; Accepted 24 February 2016

Academic Editor: Herve G. E. Kadji

A new Lorenz-like chaotic system with varying parameter is proposed by adding a state feedback function. The structure of the new designed system is simple and has more complex dynamic behaviors. The chaos behavior of the new system is studied by theoretical analysis and numerical simulation. And the bifurcation diagram shows a chaos-cycle-chaos evolution when the new parameter changes. Then a new synchronization scheme by a single state variable drive is given based on the new system and a chaotic parameter modulation digital secure communication system is also constructed. The results of simulation demonstrate that the new proposed system could be well applied in secure communication. Otherwise, based on the new system, the encryption and decryption of image could be achieved also.

1. Introduction

With the development of the mobile, PC, cloud computing, the Internet of things, and wearable devices, the data-intensive science such as big data [1] has become the main topic of the technological reform. The most prominent features of the big data are enormous volume of data, wide variety of data types, lower value density, and faster processing. But the big data has both advantages and disadvantages. It brings great convenience to individuals and enterprises; at the same time the data security is an urgent problem to be solved. From the view of information security, the traditional cryptography and secure communication model can be cracked easily, so that great security risks exist in the information system in every country. Therefore it is very urgent to improve the information security technology for the country and the enterprise in which the big data is main stream.

Due to the characteristic of the long-term unpredictability and extreme sensitivity to initial values, the chaos system has been researched deeply in the secure communications and the cryptography. Since Pecora and Carroll [2] first proposed the master-slave synchronization method in 1990, many synchronization types were presented, such as complete synchronization [3], lag synchronization [4], generalized synchronization [5], modified projective synchronization [6], modified function projective synchronization [7], phase synchronization [8], and dislocation synchronization [9]. Now more and more people paid their attention to chaotic secure communication, and the research mainly focuses on two aspects: one is to find a safer secure communication scheme, such as chaotic masking [10, 11], chaotic modulation [12], chaos shift keying [13], and chaos spreading spectrum [14] and the other is to research chaotic systems with a better encryption performance, such as fractional-order chaotic systems [15, 16], time-delay chaotic systems [17], complex chaotic system [18], and multiscroll chaotic systems [19]. Kiani-B et al. [20] applied the fractional-order Kalman filter in secure communications system. Mei [21] proposed a new secure communication scheme based on uncertain time-delay chaos system. Mahmoud et al. [22] researched the projective synchronization for complex hyperchaotic system and achieved secure communications with four-order complex Lorenz system. In addition, other secure communication schemes based on fractional-order [23], time-delay [24], and

multiscroll [25] chaotic systems have been proposed also. In the field of cryptography, compared with the traditional password, the generated mechanisms for chaos passwords are different and have real-time, so it has a greater advantage in terms of image encryption and video and other multimedia data encryption, and therefore the research on chaos image encryption has attracted more and more people [26–28]. The quality of the chaotic password is closely related to the chaos systems. For the low-dimensional chaotic system, because of its simple form, small key space, and low chaos sequence complexity, its security is not high enough. So many scholars focus on the hyperchaotic systems and fractional-order chaotic systems. Zhu and Sun [29] analyzed the security of the hyperchaos image encryption (HIE) algorithm, improved hyperchaos image encryption (IHIE) algorithm, and proposed the enhanced hyperchaos image encryption algorithms. Zhao et al. [30] gave an image encryption scheme based on an improper fractional-order chaotic system.

So the more complicated structure of the chaotic systems, the better performance of the secure communications and cryptography. However, these complicated chaotic systems are usually not easy to design synchronous controller, which decreases the communication efficiency. Therefore it is necessary to seek a new chaotic system with simple structure and complex behaviors.

In this paper, we propose a new Lorenz-like system with varying parameter by adding a state feedback factor in Lorenz-like system [31]. By theoretical analysis and numerical simulation, the structure of the new system is simple and easy to construct. At the same time, it has more complicated behaviors. This paper is divided into three parts as follows. Firstly, the new Lorenz-like chaotic system with varying parameter is designed based on the Lorenz-like system and analyzes its chaos characteristics theoretically. Secondly, a synchronization scheme driven by a single state variable is achieved based on the new proposed system, and the chaotic parameter modulation digital secure communications system is constructed. Finally, the designed variable parameter chaotic system is applied to image encryption and a three-chaotic-image encryption algorithm is proposed.

2. The Lorenz-Like System with Varying Parameter

2.1. The New Chaotic System. The Lorenz-like system is given by [31]

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= bx - xz, \\ \dot{z} &= xy - cz, \end{aligned} \tag{1}$$

where a and c are real constants and b is a bifurcation parameter. Compared with the traditional Lorenz system, y is not in the second equation. If we replace parameter b with a function of x, such as

$$b = \begin{cases} d_1 + d_2, & |x| \geq \theta \\ d_1 - d_2, & |x| < \theta \end{cases} \quad d_1, d_2, \theta \in R, \tag{2}$$

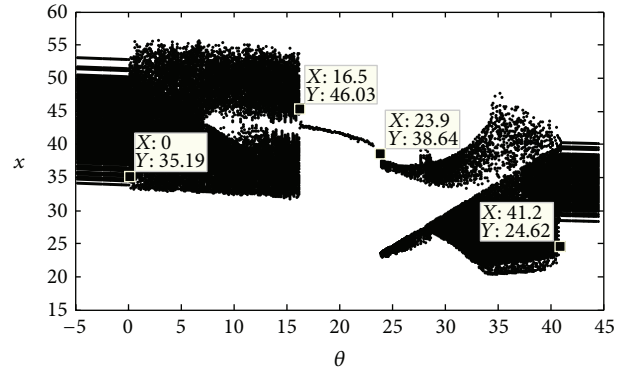

Figure 1: Bifurcation diagram of chaotic system (3) with the change of θ.

then a new system is generated and can be written as

$$\begin{aligned} \dot{x} &= a(y - x), \\ \dot{y} &= bx - xz, \\ \dot{z} &= xy - cz, \\ b &= d_1 + d_2 \operatorname{sgn}(|x| - \theta), \end{aligned} \tag{3}$$

where a, c, d_1, d_2, and θ are real constants, b is a state feedback control function, and θ is the threshold. From (2), we can know that b switches between $d_1 + d_2$ and $d_1 - d_2$ under the control of x; then the Lorenz-like system (3) shows the bifurcation under the control of state variable x.

When choosing $a = 20$, $c = 8$, $d_1 = 70$, and $d_2 = 15$, we can get a bifurcation diagram (Figure 1) of chaotic system (3) with the change of θ. For convenience, the Lorenz-like system when $b = 85$ is denoted as A chaotic system and when $b = 55$ as B chaotic system. From Figure 1, we can get that when $\theta < 0, b = 85$, the new Lorenz-like system is equivalent to the A chaotic system, while when $\theta > 41.2, b = 55$; it is equivalent to the B chaotic system. When $0 < \theta < 41.2$, b switches between 85 and 55 under the control of the state variable x; in other words, the new Lorenz-like system automatically switches between A and B chaotic systems (Figure 2). And when $16.5 < \theta < 23.9$, system appears periodic oscillation obviously.

As shown in Figure 2, the blue part denotes A chaotic system and the red part B chaotic system. With the change of parameter, the nonlinear dynamical behaviors change significantly. When $\theta = 10$ or $\theta = 30$, a strange attractor appears in Figures 2(b) and 2(d). In Figure 3, the three-dimensional phase diagram of chaotic system (3) is given with $\theta = 10, 20, 30$, and 37.

2.2. Chaotic Characters

2.2.1. Symmetry and Invariance. For system (3), let $(x, y, z) \rightarrow (-x, -y, z)$; the system equation remains the same. Then the system is symmetrical about the z-axis, and the symmetry is not associated with the system parameters. If we let $x(0) = 0$, $y(0) = 0$, and $z(0)$ be any value, the system equation can transform into $\dot{z} = -cz$; that

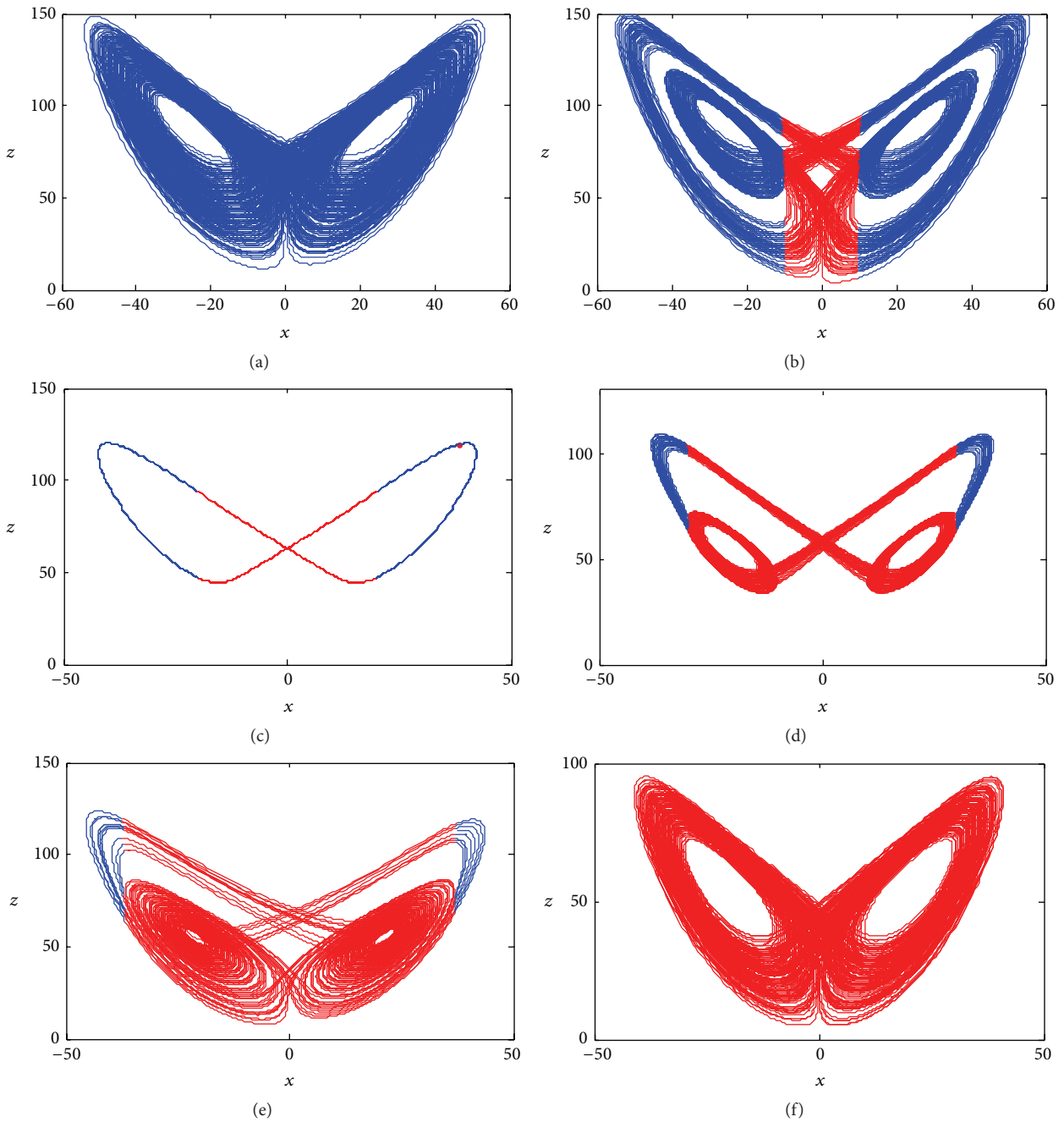

FIGURE 2: x-z plane phase diagram of chaotic system (3) (a) $\theta = -1$; (b) $\theta = 10$; (c) $\theta = 20$; (d) $\theta = 30$; (e) $\theta = 37$; and (f) $\theta = 50$.

is, the system will move on z-axis and will be stable at the origin.

2.2.2. Dissipation and the Existence of Attractor. For system (3),

$$\nabla \cdot f = \frac{\partial \dot{x}}{\partial x} + \frac{\partial \dot{y}}{\partial y} + \frac{\partial \dot{z}}{\partial z} = -a - c < 0. \tag{4}$$

So, we can conclude that the system is dissipative and converges by exponential $dV/dt = e^{-(a+c)t}$; that is, the volume element with the initial volume $V(0)$ converges to $V(0)e^{-(a+c)t}$ at time t. When $t \to \infty$, each small volume that contains the system trajectories converges to zero at an exponential rate of $-(a + c)t$. All the trajectories of the system will eventually be limited to a subset of zero volume, and this limit subset is called attractor.

2.2.3. The Existence and Stability of Equilibrium Point. For system (3), the equilibrium points are

$$\begin{gathered} O(0, 0, 0), \\ P^{+}\left(\sqrt{cb}, \sqrt{cb}, b\right), \\ P^{-}\left(-\sqrt{cb}, -\sqrt{cb}, b\right). \end{gathered} \tag{5}$$

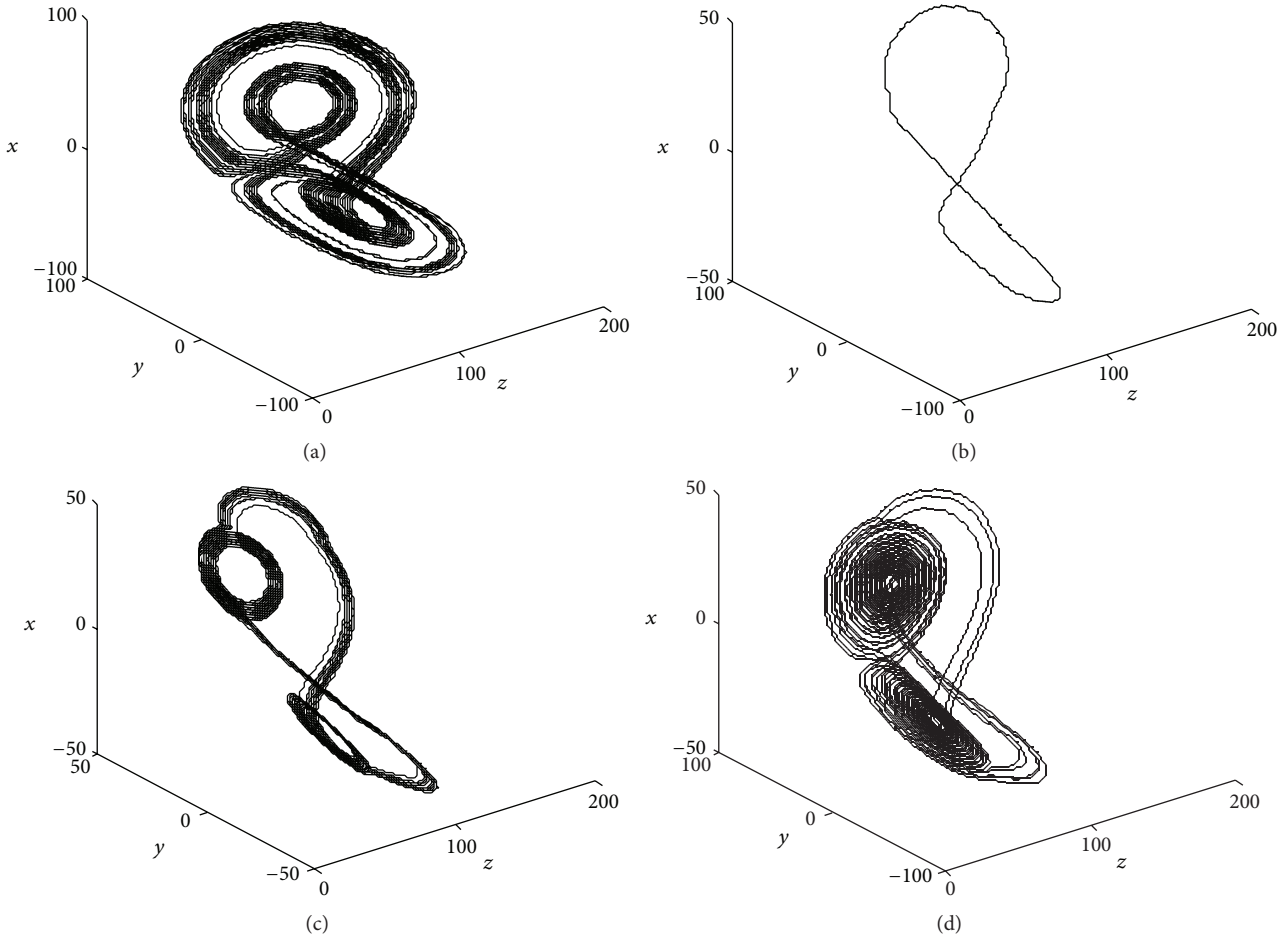

Figure 3: Three-dimensional phase diagram of chaotic system (3): (a) $\theta = 10$; (b) $\theta = 20$; (c) $\theta = 30$; and (d) $\theta = 37$.

It is easy to know that O is the shared equilibrium point for both A system and B system. When choosing $a = 20$, $c = 8$, $d_1 = 70$, and $d_2 = 15$, the other two equilibrium points of A system are $P_A^+(26.0768, 26.0768, 85)$ and $P_A^-(-26.0768, -26.0768, 85)$, and the other two equilibrium points of B system are $P_B^+(20.9762, 20.9762, 55)$ and $P_B^-(-20.9762, -20.9762, 55)$. The distribution of equilibrium points in the phase space can be seen in Table 1, in which D_{-1}, D_0, and D_{+1} denote three areas separated by θ as follows:

$$\begin{aligned} D_{+1} &= \{(x, y, z) \mid x > \theta\}, \\ D_0 &= \{(x, y, z) \mid -\theta \le x \le \theta\}, \\ D_{-1} &= \{(x, y, z) \mid x < -\theta\}. \end{aligned} \tag{6}$$

For A chaotic system, the corresponding eigenvalues for each equilibrium point can be calculated as follows:

$$\begin{aligned} &\lambda_1^O = -52.4264 \quad \lambda_1^{P_A^+} = \lambda_1^{P_A^-} = -30.1071, \\ &\lambda_2^O = +32.4264 \quad \lambda_2^{P_A^+} = \lambda_2^{P_A^-} = 1.0536 + j30.0388, \\ &\lambda_3^O = -8 \qquad\quad \lambda_3^{P_A^+} = \lambda_3^{P_A^-} = 1.0536 - j30.0388. \end{aligned} \tag{7}$$

Table 1: The distribution of equilibrium points in the phase space.

The scope of θ	Region		
	$D_{-1}{}^{\ddagger}$	$D_0{}^{\dagger}$	$D_{+1}{}^{\ddagger}$
$\theta \le 0$		$P_A^{-\ddagger}\ O^{\ddagger}\ P_A^{+\ddagger}$	
$0 < \theta < 20.9762$	$P_A^{-\ddagger}\ P_B^{-\ddagger}$	$O^{\dagger}$	$P_B^{+\ddagger}\ P_A^{+\ddagger}$
$20.9762 \le \theta \le 26.0768$	$P_A^{-\ddagger}$	$P_B^{-\dagger}\ O^{\dagger}\ P_B^{+\dagger}$	$P_A^{+\ddagger}$
$\theta > 26.0768$		$P_A^{-\dagger}\ P_B^{-\dagger}\ O^{\dagger}\ P_B^{+\dagger}\ P_A^{+\dagger}$	
$\theta \gg 26.0768$		$P_B^{-\dagger}\ O^{\dagger}\ P_B^{+\dagger}$	

Note: † represents D_0 and ‡ represents D_{-1} and D_{+1}.

Obviously, O is a saddle point, and P_A^+, P_A^- are saddle-focus equilibrium points. And all these three equilibrium points are unstable, which leads the orbits of system stretch in phase space. Under the interactive stretching and contractions, the chaotic motion is generated. In the same way, we also can draw a similar conclusion that B chaotic system also has three unstable equilibrium points and the chaotic condition is satisfied.

From Table 1, it is easy to know that the system has three equilibrium points when $\theta \le 0$ and it is equal to A chaotic

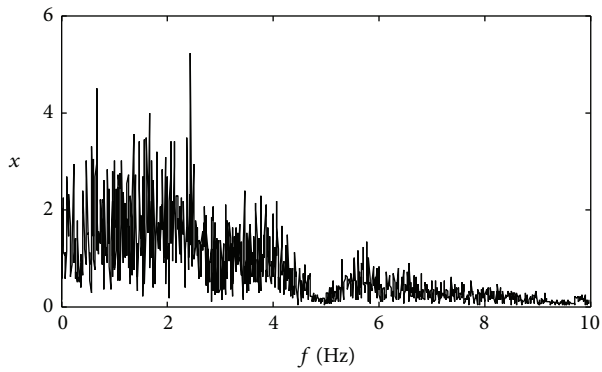

Figure 4: The spectrum of Lorenz-like system with varying parameter when $\theta = 4$.

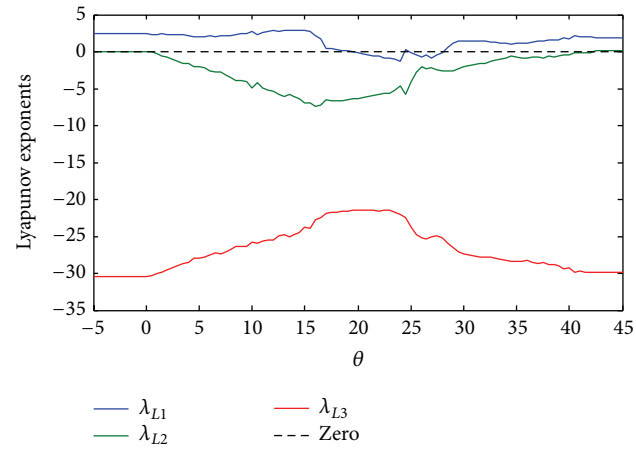

Figure 5: Lyapunov exponents curves of chaotic system (3) with the change of θ.

Table 2: Lyapunov exponents and Lyapunov dimension.

θ	Lyapunov exponents			Lyapunov dimension (D_L)
	λ_{L1}	λ_{L2}	λ_{L3}	
$\theta \le 0$ (A system)	2.5110	−0.0029	−30.4572	2.0824
$\theta = 4$	2.2269	−1.6438	−28.5472	2.0204
$\theta \gg 26.0678$ (B system)	2.0533	0.0242	−30.0060	2.0684

system. The system also can be treated approximately such that it has three equilibrium points when $\theta \gg 26.0768$ and the system is equal to B chaotic system. But in addition to these two cases, the system has five equilibrium points. Of all the five points, O influences the trajectory in the whole region, while P_B^+ and P_B^- influence the trajectory in D_0, and P_A^+ and P_A^- influence the trajectory in D_{-1} and D_{+1}. With the increase of θ, D_0 gradually extends and $D_{\pm 1}$ is reduced; that is, the influence of P_B^+ and P_B^- gradually increases while P_A^+ and P_A^- are reduced until they nearly disappear. So the system shows a complex dynamic chaos-cycle-chaos when the new parameter θ changes.

2.2.4. Spectrum. In Figure 4, we can see that spectrum of the system is continuous, which shows that the new designed system has the chaotic characteristics.

2.2.5. Lyapunov Exponents and Lyapunov Dimension. Lyapunov exponent measures the exponential rates of divergence or convergence of nearby trajectories in phase space. A three-order nonlinear system has three Lyapunov exponents $(\lambda_{L1}, \lambda_{L2}, \lambda_{L3})$. All the Lyapunov exponents are listed in Table 2, and the curves with the change of θ are also given as in Figure 5. Obviously λ_{L2} of A and B systems is close to zero, while λ_{L2} (when $\theta = 4$) is a negative number for the reason of θ; this implies that a new chaotic attractor occurred in the new system.

For a n-order system, the Lyapunov dimension can be calculated as follows:

$$D_L = j + \frac{\lambda_{L1} + \lambda_{L2} + \cdots + \lambda_{Lj}}{\left|\lambda_{L(j+1)}\right|}, \tag{8}$$

where $\lambda_{L1} > \lambda_{L2} > \cdots > \lambda_{Ln}$ and $\lambda_{L1} + \lambda_{L2} + \cdots + \lambda_{Lj} > 0$ while $\lambda_{L1} + \lambda_{L2} + \cdots + \lambda_{L(j+1)} < 0$.

From the results in Table 2, we can get that all the Lyapunov dimensions are fractions and $2 < D_L < 3$. Thus, it is another evidence of chaos. In addition, both Lyapunov exponents' curves and bifurcation diagram can show the effect of parameter, so the same conclusion can be obtained from Figure 5 as Figure 1.

2.2.6. A Brief Summary. This section shows a new Lorenz-like system (3) with varying parameter; several conclusions can be gotten as follows: (i) b is a constant in Lorenz-like system (1) while it switches between $d_1 + d_2$ and $d_1 - d_2$ in system (3), so the new system's structure has a slight difference with the Lorenz-like system (1) and it equals system (1) when $\theta \le 0$ or $\theta \gg 26.0678$; (ii) new chaotic behaviors occur when θ change (see Figures 1, 2, and 3); (iii) the equilibrium points are not fixed for the reason of θ as Table 1 shows; and (iv) the Lyapunov exponent λ_{L2} is apparently different (see Table 2 and Figure 5). All the conclusions imply that the new proposed system has more complicated behaviors with respect to the Lorenz-like system (1).

3. The Application in Secure Communication for the New Lorenz-Like System

3.1. Synchronization Design for Single Variable Drive. For a better description of the synchronization scheme, here we use notation (x_1, x_2, x_3) in place of (x, y, z) in (3); then the master system is

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1), \\ \dot{x}_2 &= b_x x_1 - x_1 x_3, \\ \dot{x}_3 &= -c x_3 + x_1 x_2, \\ b_x &= d_1 + d_2 \operatorname{sgn}(|x_1| - \theta), \quad \theta \in R. \end{aligned} \tag{9}$$

And the slave system is

$$\begin{aligned}\dot{y}_1 &= a\left(y_2 - y_1\right),\\ \dot{y}_2 &= b_y y_1 - y_1 y_3 + u_1,\\ \dot{y}_3 &= -cy_3 + y_1 y_2 + u_2,\\ b_y &= d_1 + d_2 \operatorname{sgn}\left(\left|y_1\right| - \theta\right), \quad \theta \in R.\end{aligned} \tag{10}$$

So the controller is designed as follows:

$$\begin{aligned}u_1 &= -b_y y_1 + b_x x_1 + a x_1 + y_1 y_3 - x_1 y_3 - a y_1,\\ u_2 &= -y_1 y_2 + x_1 y_2.\end{aligned} \tag{11}$$

The designed controller only contains one state variable x_1 of the master system; thus it has simple structure and is driven by single variable. So it is easy to be achieved.

Let the error system be

$$\begin{aligned}e_1 &= y_1 - x_1,\\ e_2 &= y_2 - x_2,\\ e_3 &= y_3 - x_3.\end{aligned} \tag{12}$$

Then, the error dynamics equation is

$$\begin{aligned}\dot{e}_1 &= a\left(e_2 - e_1\right),\\ \dot{e}_2 &= -x_1 e_3 - a e_1,\\ \dot{e}_3 &= -ce_3 + x_1 e_2.\end{aligned} \tag{13}$$

Select the Lyapunov function as $(e) = (1/2)e_1^2 + (1/2)e_2^2 + (1/2)e_3^2$; then take the derivative of $V(e)$, so

$$\begin{aligned}\dot{V}(e) &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3\\ &= e_1 a\left(e_2 - e_1\right) + e_2\left(-xe_3 - ae_1\right)\\ &\quad + e_3\left(-ce_3 + xe_2\right)\\ &= -ae_1^2 + ae_1e_2 - x_1e_2e_3 - ae_1e_2 - ce_3^2 + x_1e_2e_3\\ &= -ae_1^2 - ce_3^2.\end{aligned} \tag{14}$$

When $e = (e_1, e_2, e_3)^{\mathrm{T}} = (0,0,0)^{\mathrm{T}}$, $V(e) = 0$, and when $e \neq (0,0,0)^{\mathrm{T}}$, $V(e) > 0$ and $\dot{V}(e) < 0$. According to the Lyapunov stability theorem, $e_1 \to 0$, $e_2 \to 0$, and $e_3 \to 0$ when $t \to \infty$; that is, the synchronization between master and slave system has been achieved.

Figure 6 gives the synchronization error curves between the master system and slave system with $a = 20$, $c = 8$, $d_1 = 70$, $d_2 = 15$, and $\theta = 4$; the initial value $(x(0), y(0), z(0)) = (-10.5, -7, 8)$, $(x_1(0), y_1(0), z_1(0)) = (0, 10, 6)$. From Figure 6, the master system traces the slave system to achieve synchronization quickly. The advantage of this chaotic synchronization system is that the controller is simple and only one signal is to be transmitted to complete the synchronization between the drive system and response system, which improves communication efficiency and conserves resources.

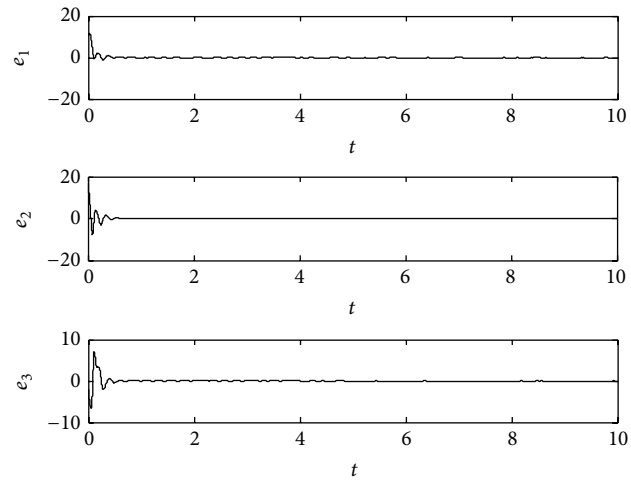

Figure 6: Synchronization error curve between master and slave systems when $\theta = 4$.

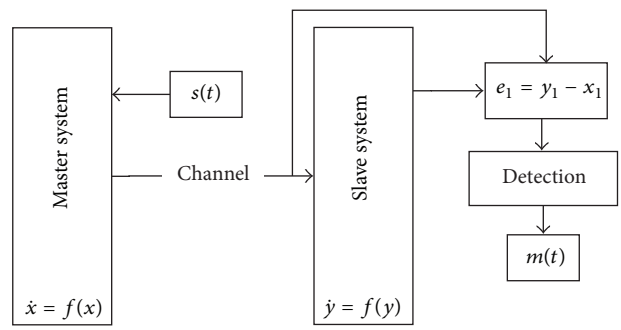

Figure 7: The schematic of digital secure communications.

3.2. Chaos Parameter Modulation Digital Secure Communications System. Based on the synchronization scheme designed in the previous section, a chaotic parameter modulation digital secure communication system is given in Figure 7.

The transmitter system is

$$\begin{aligned}\dot{x}_1 &= 20\left(x_2 - x_1\right),\\ \dot{x}_2 &= b_x x_1 - x_1 x_3,\\ \dot{x}_3 &= -8x_3 + x_1 x_2,\\ b_x &= 70 + 15 \operatorname{sgn}\left(\left|x_1\right| - (4 + 2s(t))\right).\end{aligned} \tag{15}$$

The receiver system is

$$\begin{aligned}\dot{y}_1 &= 20\left(y_2 - y_1\right),\\ \dot{y}_2 &= \left(b_y + 20\right)x_1 - x_1 y_3 - a y_1,\\ \dot{y}_3 &= -8y_3 + x_1 y_2,\\ b_y &= 70 + 15 \operatorname{sgn}\left(\left|x_1\right| - 4\right),\end{aligned} \tag{16}$$

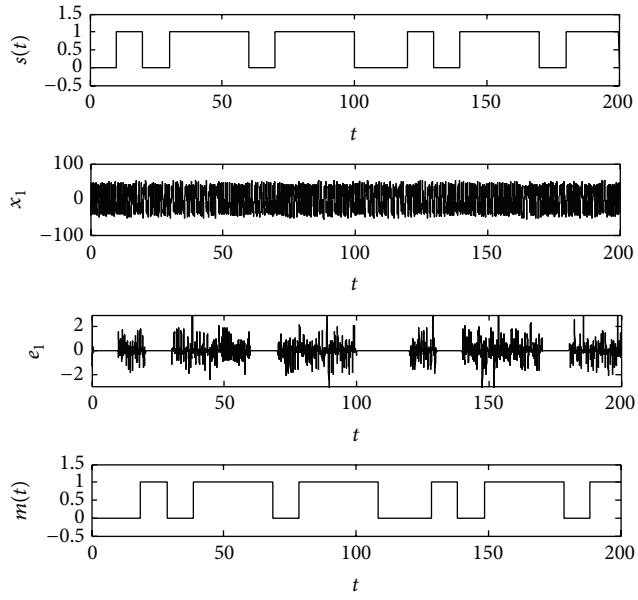

Figure 8: Chaotic parameter modulation digital secure communication.

where $s(t)$ is a digital signal to be transmitted. In order to encrypt $s(t)$, we select $\theta = 4$ to represent "0" and $\theta = 6$ to represent "1"; that is,

$$\theta = 4 + 2\left(s\left(t\right)\right) = \begin{cases} 4, & s\left(t\right) = 0 \\ 6, & s\left(t\right) = 1. \end{cases} \tag{17}$$

In this case, the topology of the phase diagram is similar, so it is difficult to crack encrypted signal and extract useful information by phase space reconstruction.

Based on the theory above, we simulate the digital secure communication system as in Figure 8. The digital signal $s(t)$ "0101110111001011101" will be transmitted and sent per symbol interval, that is, 10 seconds, where x_1 is not only the encrypted signal but also the driven signal. The synchronization between the master system and slave system only can be reached when $\theta = 4$, and there is a large error between the response system and the drive system when $\theta = 6$ just as e_1 in Figure 8. Finally the decrypted signal $m(t)$ can be gotten from e_1 after detection, and compared with $s(t)$, there is a nearly 10-second delay.

4. Image Encryption Algorithm Based on Lorenz-Like System with Varying Parameter

4.1. A Three-Order Image Encryption Algorithm. Based on system (3), a three-order image encryption algorithm is given and the diagram of the image encryption and decryption is shown in Figure 9.

The chaotic image encryption is to disrupt the original image (plaintext) by chaotic sequence. The process of the algorithm is as follows: first, set the initial value of the system as the key; then iterate system (3) for 5000 times to make it fully chaotic. Later, continue to iterate system (3) to obtain $x(n)$, $y(n)$, and $z(n)$. Then the chaotic sequences key$x(n)$, key$y(n)$, and key$z(n)$ can be gotten as below:

$$\begin{aligned} &\text{key}x\left(n\right) \\ &\quad = \bmod\left(\left(\left|x\left(n\right)\right| - \text{floor}\left(\left|x\left(n\right)\right|\right)\right) \times 10^{14}, 256\right), \\ &\text{key}y\left(n\right) \\ &\quad = \bmod\left(\left(\left|y\left(n\right)\right| - \text{floor}\left(\left|y\left(n\right)\right|\right)\right) \times 10^{14}, 256\right), \\ &\text{key}z\left(n\right) \\ &\quad = \bmod\left(\left(\left|z\left(n\right)\right| - \text{floor}\left(\left|z\left(n\right)\right|\right)\right) \times 10^{14}, 256\right), \end{aligned} \tag{18}$$

where "floor" is the MATLAB function and floor(A) rounds the element A to the nearest integers less than or equal to A.

Through the above process in (18), we get the chaotic sequences key$x(n)$, key$y(n)$, and key$z(n)$ which range between 0 and 255. Original image matrix (plaintext) is P and the ciphertext matrices are C_1, C_2, and C_3, which are obtained after three-order encryption, respectively, where C_3 is the final ciphertext image matrix. The encryption formula is as follows:

$$\begin{aligned} C_1\left(n\right) &= P\left(n\right) \oplus \text{key}x\left(n\right), \\ C_2\left(n\right) &= C_1\left(n\right) \oplus \text{key}y\left(n\right), \\ C_3\left(n\right) &= C_2\left(n\right) \oplus \text{key}z\left(n\right). \end{aligned} \tag{19}$$

"$\oplus$" in (19) means "XOR", and the same is in (20). Just as Figure 9, the decryption process is the opposite of the encryption process. First, we should set the correct key; then for system (3), the decryption process is the same with the encryption to obtain the same chaotic sequences to decrypt correctly. Decryption formula is as follows:

$$\begin{aligned} C_2\left(n\right) &= C_3\left(n\right) \oplus \text{key}z\left(n\right), \\ C_1\left(n\right) &= C_2\left(n\right) \oplus \text{key}y\left(n\right), \\ P\left(n\right) &= C_1\left(n\right) \oplus \text{key}x\left(n\right). \end{aligned} \tag{20}$$

4.2. Simulation and Analysis. In this section, an image encryption experiment was given and a 512 × 512 color image "Lena" is chosen as the plaintext. In simulation, the step is selected as 0.01, and $a = 20$, $c = 8$, $d_1 = 70$, $d_2 = 15$, and $\theta = 4$. The encryption key is initial value $(x(0), y(0), z(0)) = (0.2, 0.7, 1.6)$. Based on the above algorithm, the image encryption system is designed to achieve the Lena encryption. The simulation results shown in Figure 10, and several tests have been carried out to demonstrate the effectiveness and efficiency of the proposed encryption algorithm.

4.2.1. Key Space Analysis. Key space size is the total number of different keys which can be used in an encryption process; it should be large enough to preclude the eavesdropping by brute-force attack. A single precision floating point format number has 2^{32} kinds of possibilities; then the key space

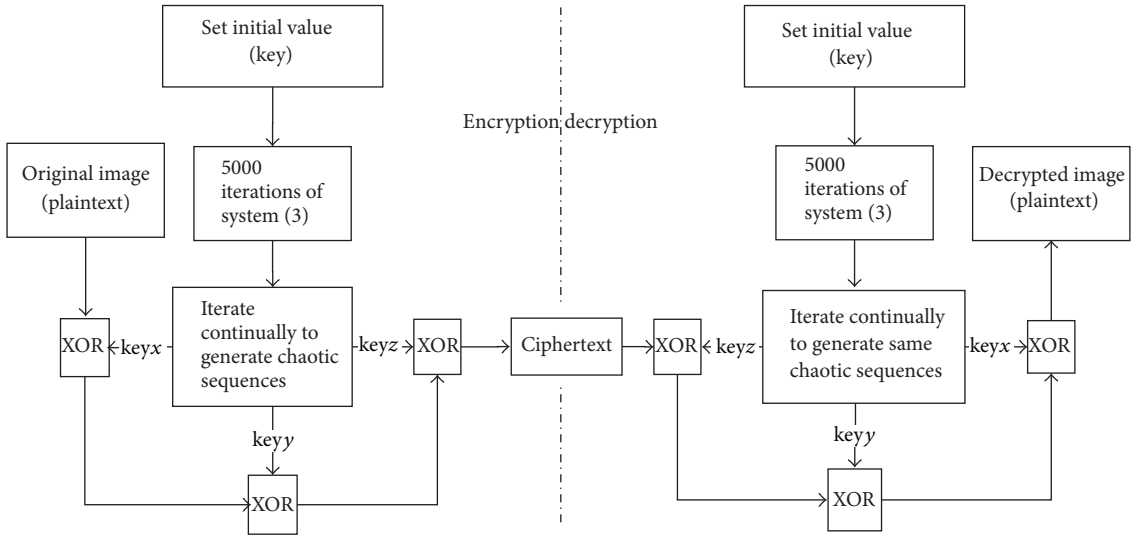

Figure 9: The diagram of image encryption and decryption.

(a) (b) (c) (d)

Figure 10: The simulation results of image encryption and decryption. (a) Original image (plaintext); (b) encrypted image (ciphertext); (c) decrypted image (plaintext); and (d) illegal decrypted image.

in this paper will be up to 2^{96}. Otherwise, if the system parameters are chosen as keys, it will get much larger key space, which greatly increases the security of the system.

4.2.2. Histogram Analysis. From the histogram of a digital image, the distribution of the pixel values can be gotten; if the encrypted image is well encrypted, the histogram will be uniform, so the histogram attack can be prevented effectively. Figure 11 gives the histograms of both original image and encrypted image; it is obvious that the histograms of red, green, and blue for original image are steep and not flat enough; the histograms for encrypted image are all uniform and quite different from that of the original image when using the proposed algorithm.

4.2.3. Key Sensitivity Analysis. A good cryptosystem must be highly sensitive at small changes in secret key in encryption and decryption process, so a full test contains two aspects: (i) slightly different keys to encrypt the same image are used and the difference between the corresponding encrypted images is computed; (ii) for an encrypted image only one correct key can decrypt it, so decrypt the encrypted image by an incorrect key which is similar to the correct one and observe whether it can be correctly decrypted.

Table 3 gives some special cases to evaluate the sensitivity in encryption process, and the encrypted images were also shown in Figure 12; the difference ratio is really high, which means a good key sensitivity in encryption process. The test result in decryption process also can be seen in Figure 12; Figure 12(f) is the correct decrypted image; Figure 12(g) is the incorrect one with only a slight change 10^{-14} for the key's first value.

4.2.4. Correlation Coefficients and Efficiency Analysis. A good image encryption algorithm should have two characteristics: (i) high security, which is partly analyzed in key space and key sensitivity, will be analyzed by correlation coefficients complementally in this section; (ii) high efficiency, which means low time consumption in encryption and decryption process, will be analyzed in this section also.

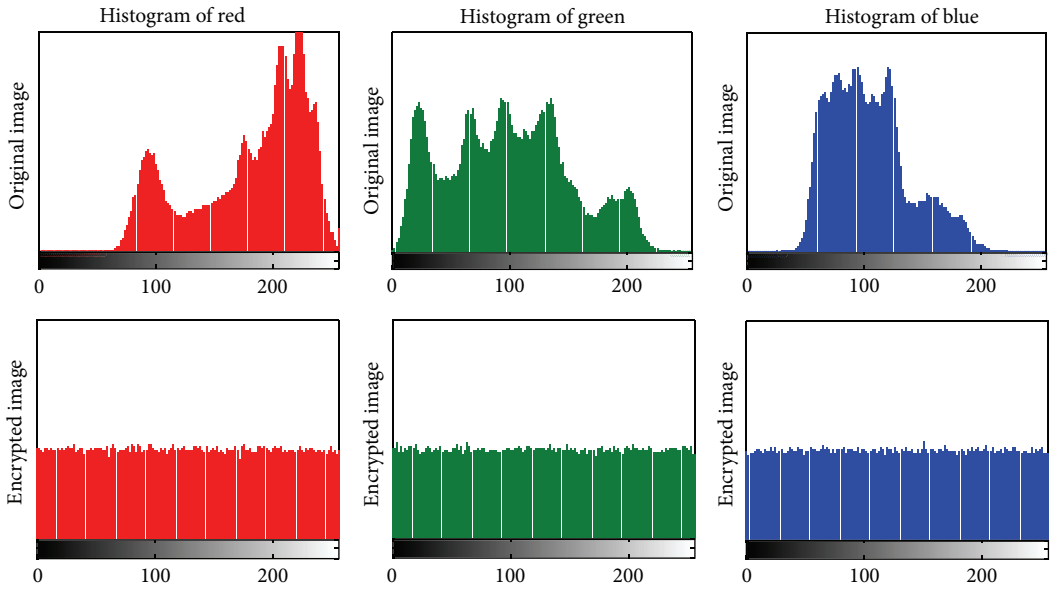

Figure 11: Histogram of original image and encrypted image.

Table 3: Differences between encrypted images produced by slightly different keys.

Encryption keys (I) Figure 12(b)			Encryption keys (II)				Difference ratio between (I) and (II) (%)
$x(0)$	$y(0)$	$z(0)$	$x(0)$	$y(0)$	$z(0)$		
2.5	−3.7	9.3	$2.5 + 1 \times 10^{-14}$	−3.7	9.3	Figure 12(c)	99.61
			2.5	$-3.7 + 1 \times 10^{-14}$	9.3	Figure 12(d)	99.60
			2.5	−3.7	$9.3 + 1 \times 10^{-14}$	Figure 12(e)	99.60

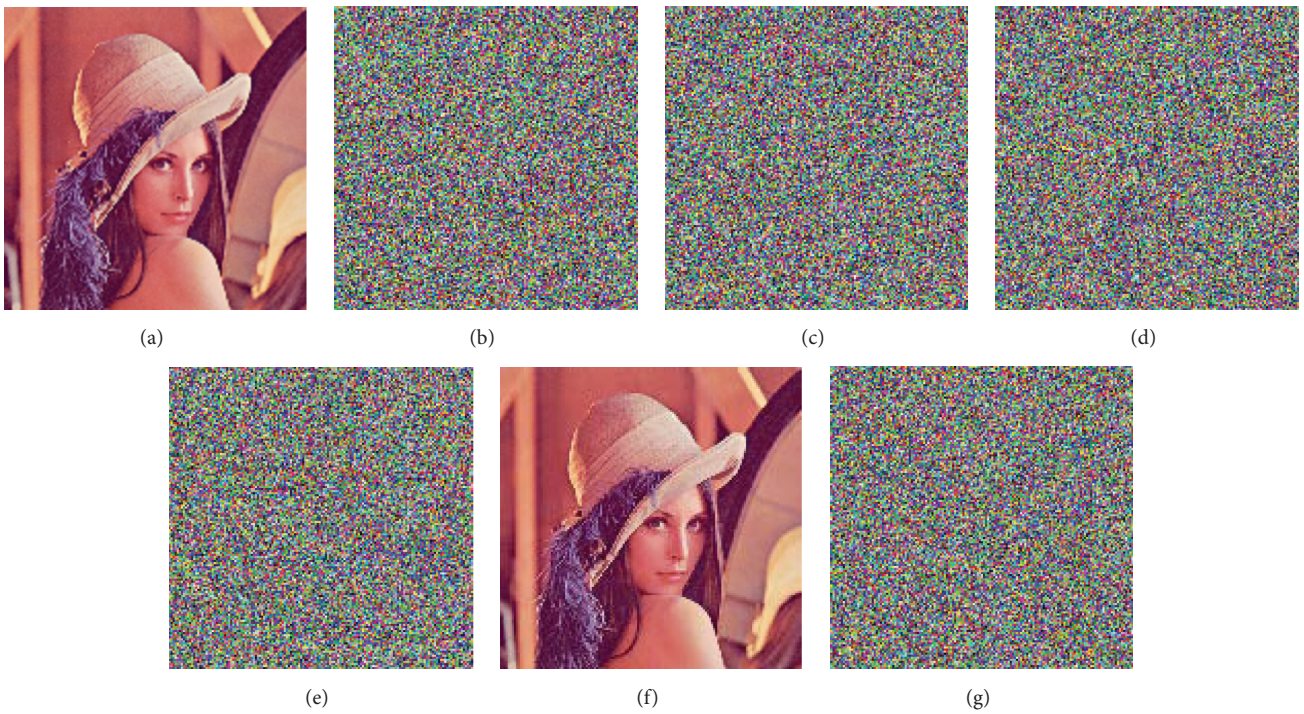

Figure 12: Key sensitivity test. (a) Original image (plaintext); (b), (c), (d), (e) the encrypted images with different keys as Table 3; (f) decrypt (b) with key (2.5, −3.7, 9.3); and (g) decrypt (b) with key ($2.5–1 \times 10^{-14}$, −3.7, 9.3).

Table 4: Correlation coefficients and cost comparisons.

Chaotic systems used	Correlation coefficients						Cost (s)
	Original image (plaintext)			Encrypted image (ciphertext)			
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal	
Proposed system	0.9788	0.9677	0.9752	0.0086	0.0307	−0.0326	10.9689
Reference [29]	0.9788	0.9677	0.9752	0.0167	−0.0004	0.0371	13.9933
Reference [30]	0.9788	0.9677	0.9752	−0.0750	−0.1078	0.0036	14.0401

The correlation coefficient of an image can be measured as follows:

$$C_r = \frac{N\sum_{i=0}^{N} x_i y_i - \left(\sum_{i=0}^{N} x_i\right)\left(\sum_{i=0}^{N} y_i\right)}{\sqrt{\left(N\sum_{i=0}^{N} x_i^2 - \left(\sum_{i=0}^{N} x_i\right)^2\right)\left(N\sum_{i=0}^{N} y_i^2 - \left(\sum_{i=0}^{N} y_i\right)^2\right)}}, \quad (21)$$

where N is the number of pair of pixels and x and y are values of two adjacent pixels in grey scale. The correlation coefficients are calculated out based on 3000 random pixels, and all correlation coefficients of plaintext are greater than 0.96 while those of ciphertext are all near "zero," which implies a good information hiding for plaintext.

Recently many chaotic systems with complex structure were found or applied to image encryption, such as systems in [29, 30]. Here we realize image encryption with different chaotic systems under the same simulation environment; then comparisons with the proposed algorithm were done and the results of correlation coefficients and cost are listed in Table 4. Compared with algorithms based on other chaotic systems in [29, 30], we can know that the correlation coefficients of ciphertext are nearly, but the time consumption is less for the proposed system. This comparison demonstrates that the proposed image encryption algorithm based on the new Lorenz-like system shows a good performance as well as algorithms based on other systems, and the efficiency is high for the reason of its simple structure.

5. Conclusion

A new Lorenz-like system with varying parameter is proposed by adding a state feedback function in this paper. Firstly, we analyze the influence of the threshold θ to the chaotic behavior of the new system and found that the system shows a chaos-cycle-chaos evolution when θ changes. Then we analyze the new system's chaotic characteristics. After that a new synchronization scheme using a single state variable drive based on the new system is designed. Finally, a chaotic parameter modulation digital secure communication system and image encryption based on the new system proposed is designed. The simulation results show that the new system has a good performance in application. Otherwise, according to the new system designed, we can modify many other systems to get more chaotic systems which have simple structure and complex dynamics. This will enrich the amount of chaotic signal sources, simplify designing, and improve the security of communication and image encryption.

Competing Interests

The authors declare that they have no competing interests.

Acknowledgments

This research is funded by the National Natural Science Foundation of China (nos. 61203004 and 61306142) and the Natural Science Foundation of Heilongjiang Province (Grant no. F201220).

References

[1] W. Feng, "The opportunities and challenges of information security in big data era," *China Venture Capital*, vol. 34, pp. 49–53, 2013.

[2] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Review Letters*, vol. 64, no. 8, pp. 821–824, 1990.

[3] J. Q. Lu and J. D. Cao, "Adaptive complete synchronization of two identical or different chaotic (hyperchaotic) systems with fully unknown parameters," *Chaos*, vol. 15, no. 4, Article ID 043901, 10 pages, 2005.

[4] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths, "From phase to lag synchronization in coupled chaotic oscillators," *Physical Review Letters*, vol. 78, no. 22, pp. 4193–4196, 1997.

[5] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel, "Generalized synchronization of chaos in directionally coupled chaotic systems," *Physical Review E*, vol. 51, no. 2, pp. 980–994, 1995.

[6] G.-H. Li, "Modified projective synchronization of chaotic system," *Chaos, Solitons and Fractals*, vol. 32, no. 5, pp. 1786–1790, 2007.

[7] K. S. Sudheer and M. Sabir, "Adaptive modified function projective synchronization between hyperchaotic Lorenz system and hyperchaotic LU system with uncertain parameters," *Physics Letters A*, vol. 373, no. 41, pp. 3743–3748, 2009.

[8] B. Blasius, A. Huppert, and L. Stone, "Complex dynamics and phase synchronization in spatially extended ecological systems," *Nature*, vol. 399, no. 6734, pp. 354–359, 1999.

[9] L.-L. Huang, S.-S. Shi, and J. Zhang, "Dislocation synchronization of the different complex value chaotic systems based on single adaptive sliding mode controller," *Mathematical Problems in Engineering*, vol. 2015, Article ID 240586, 8 pages, 2015.

[10] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz-based chaotic circuits with applications to communications," *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, vol. 40, no. 10, pp. 626–633, 1993.

[11] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via

chaotic synchronization," *International Journal of Bifurcation and Chaos*, vol. 2, no. 3, pp. 709–713, 1992.

[12] T. Yang and L. O. Chua, "Secure communication via chaotic parameter modulation," *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 43, no. 9, pp. 817–819, 1996.

[13] G. Kolumban, M. P. Kennedy, G. Kis, and Z. Jako, "FM-DCSK: a novel method for chaotic communications," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '98)*, pp. 477–480, Monterey, Calif, USA, June 1998.

[14] M. Itoh, "Spread spectrum communication via chaos," *International Journal of Bifurcation and Chaos*, vol. 9, no. 1, pp. 155–213, 1999.

[15] C. Li and G. Chen, "Chaos in the fractional order Chen system and its control," *Chaos, Solitons and Fractals*, vol. 22, no. 3, pp. 549–554, 2004.

[16] D. Chen, C. Liu, C. Wu, Y. Liu, X. Ma, and Y. You, "A new fractional-order chaotic system and its synchronization with circuit simulation," *Circuits, Systems, and Signal Processing*, vol. 31, no. 5, pp. 1599–1613, 2012.

[17] J. Tang, "Synchronization of different fractional order time-delay chaotic systems using active control," *Mathematical Problems in Engineering*, vol. 2014, Article ID 262151, 11 pages, 2014.

[18] P. Liu and S. Liu, "Anti-synchronization between different chaotic complex systems," *Physica Scripta*, vol. 83, no. 6, Article ID 065006, 9 pages, 2011.

[19] C.-X. Zhang and S.-M. Yu, "Design and implementation of a novel multi-scroll chaotic system," *Chinese Physics B*, vol. 18, no. 1, pp. 119–129, 2009.

[20] A. Kiani-B, K. Fallahi, N. Pariz, and H. Leung, "A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 3, pp. 863–879, 2009.

[21] R. Mei, "Secure communication scheme using uncertain delayed chaotic system synchronization based on disturbance observers," in *Proceedings of the International Workshop on Chaos-Fractals Theories and Applications (IWCFTA '09)*, pp. 177–181, IEEE, Shenyang, China, November 2009.

[22] G. M. Mahmoud, E. E. Mahmoud, and A. A. Arafa, "On projective synchronization of hyperchaotic complex nonlinear systems based on passive theory for secure communications," *Physica Scripta*, vol. 87, no. 5, Article ID 055002, 10 pages, 2013.

[23] H.-F. Cao and R.-X. Zhang, "Parameter modulation digital communication and its circuit implementation using fractional-order chaotic system via a single driving variable," *Acta Physica Sinica*, vol. 61, no. 2, pp. 123–130, 2012.

[24] M. J. Wang and X. Y. Wang, "A secure communication scheme based on parameter identification of first order time-delay chaotic system," *Acta Physica Sinica*, vol. 58, no. 3, pp. 1467–1472, 2009.

[25] L. Gámez-Guzmán, C. Cruz-Hernández, R. M. López-Gutiérrez, and E. E. García-Guerrero, "Synchronization of Chua's circuits with multi-scroll attractors: application to communication," *Communications in Nonlinear Science and Numerical Simulation*, vol. 14, no. 6, pp. 2765–2775, 2009.

[26] S. Li and X. Zheng, "Cryptanalysis of a chaotic image encryption method," in *Proceedings of the IEEE International Symposium on Circuits and Systems (ISCAS '02)*, vol. 2, pp. 708–711, Phoenix-Scottsdale, Ariz, USA, May 2002.

[27] A. Kanso and M. Ghebleh, "A novel image encryption algorithm based on a 3D chaotic map," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 7, pp. 2943–2959, 2012.

[28] L. Y. Zhang, X. B. Hu, Y. S. Liu, K.-W. Wong, and J. Gan, "A chaotic image encryption scheme owning temp-value feedback," *Communications in Nonlinear Science and Numerical Simulation*, vol. 19, no. 10, pp. 3653–3659, 2014.

[29] C.-X. Zhu and K.-H. Sun, "Cryptanalysis and improvement of a class of hyperchaos based image encryption algorithms," *Acta Physica Sinica*, vol. 61, no. 12, p. 120503, 2012.

[30] J. F. Zhao, S. H. Wang, Y. X. Chang, and X. F. Li, "A novel image encryption scheme based on an improper fractional-order chaotic system," *Nonlinear Dynamics*, vol. 80, no. 4, pp. 1721–1729, 2015.

[31] L. L. Huang, X. Y. Wang, and G. H. Sun, "Design and circuit simulation of the new Lorenz chaotic system," in *Proceedings of the 3rd International Symposium on Systems and Control in Aeronautics and Astronautics (ISSCAA '10)*, pp. 1443–1447, Harbin, China, June 2010.