Adaptive synchronization of a switching system and its applications to secure communications

Weiguo Xia and Jinde Cao

Citation: Chaos: An Interdisciplinary Journal of Nonlinear Science **18**, 023128 (2008); doi: 10.1063/1.2937017
View online: http://dx.doi.org/10.1063/1.2937017
View Table of Contents: http://scitation.aip.org/content/aip/journal/chaos/18/2?ver=pdfcov
Published by the AIP Publishing

Adaptive synchronization of a switching system and its applications to secure communications

Weiguo Xia and Jinde Cao[a)]
Department of Mathematics, Southeast University, Nanjing 210096, China

(Received 31 January 2008; accepted 6 May 2008; published online 27 June 2008)

This paper studies the adaptive synchronization of a switching system with unknown parameters which switches between the Rössler system and a unified chaotic system. Using the Lyapunov stability theory and adaptive control method, the receiver system will achieve synchronization with the drive system and the unknown parameters would be estimated by the receiver. Then the proposed switching system is used for secure communications based on the communication schemes including chaotic masking, chaotic modulation, and chaotic shift key strategies. Since the system switches between two chaotic systems and the parameters are almost unknown, it is more difficult for the intruder to extract the useful message from the transmission channel. In addition, two new schemes in which the chaotic signal used to mask (or modulate) the transmitted signal switches between two components of a chaotic system are also presented. Finally, some simulation results are given to show the effectiveness of the proposed communication schemes. © *2008 American Institute of Physics*. [DOI: 10.1063/1.2937017]

In recent years, switched systems have been widely investigated due to their potential applications in secure communication, aircraft control, switching power converters, and many other fields. In this paper, we discuss the adaptive synchronization of a switching chaotic system which switches between two chaotic systems by utilizing the Lyapunov stability theory and adaptive control method. Several communication strategies are then presented based on the synchronization of the switching system. Moreover, another two new schemes in which the signal used to modulate the transmitted signal switches between two components of a chaotic system are also presented. As the parameters are almost unknown and the signal switches as time varies, it is more difficult for the intruder to detect the useful message from the transmission channel. Finally, the proposed schemes are validated through numerical simulations.

I. INTRODUCTION

In 1963, the first attractor, named for its discoverer Lorenz, arose from a mathematical model of the atmosphere.[1] In 1979, Rössler presented another chaotic attractor from chemical kinetics.[2] After that, many other chaotic attractors were discovered. In 2002, Lü and Chen proposed a unified chaotic system which unifies the Lorenz system, the Chen system, and the Lü system together.[3–6]

Since Pecora and Carrol[7] found the chaos synchronization in the laboratory in 1990, chaos synchronization have been intensively studied,[8–19] due to their great potential applications in many different areas such as secure communication, biological systems, information science, chemical reaction, etc. Secure communication utilizing the synchronization of chaos has become an interesting issue in recent years. In the existing literatures, many communication schemes have been proposed including chaotic masking,[11,20] chaotic modulation,[10,11,13,21,22] and chaotic shift key.[9,11,23] In Ref. 20, the chaotic masking scheme was developed. In this scheme, using two synchronized chaotic systems, the message is masked by a chaotic signal, and the receiver can recover the message by subtracting the masking signal. In Ref. 22, the authors proposed another communication scheme known as chaotic modulation. In this scheme, the transmitter is switching among different trajectories of the same chaotic attractor. Then the message modulated into the phase space of the chaotic attractor can be recovered by the synchronized receiver. In Ref. 23, the chaotic shift key scheme which was designed to transmit a digital signal was discussed. It can be considered as a special case of chaotic modulation. In Ref. 24, the author gave a detailed history of chaotic secure communication system, and then presented a new scheme based on impulsive synchronization.

In recent years, increasing interest has been devoted to the study of adaptive synchronization and its application to secure communication.[9–11,21,25] In Ref. 9, Feki designed an observer-based response system to synchronize with a drive system with unknown parameters, and then applied this to secure communication. In Ref. 10, Wu investigated the adaptive synchronization of a unified chaotic system and then proposed a new communication scheme by modulating the emitted signal into the parameter. In Ref. 11, Yu *et al.* proposed several new schemes including chaotic masking, chaotic modulation, and chaotic shift key based on the adaptive control method.

Recently, switched systems have been widely investigated since their numerous applications in control of mechanical systems, the automotive industry, and so on. In Ref. 26, Liberzon *et al.* proposed three basic problems regarding the stability and design of switched systems. In Ref. 27,

[a)]Electronic addresses: jdcao@seu.edu.cn; jdcaoseu@gmail.com.

Huang *et al.* discussed the robust stability of switched Hopfield neural networks. Most previous works[9–11] studied communication schemes based on the chaos synchronization between the drive and response system. However, in this paper we consider a switching system which switches between a unified chaotic system and the Rössler system as a transmitter and then introduce several communication schemes based on the adaptive synchronization of the switching system. In addition, only one component of a chaotic system was used to mask (or modulate) the plaintext message in Ref. 11. In this paper, we will discuss two new schemes based on the switch method in which a chaotic signal used to mask (or modulate) the message switches between two components of a chaotic system.

The synchronization problem of a switching chaotic system is discussed in the paper, and then this switching chaotic system is used for secure communication. Since the chaotic signal used to modulate the transmitted message switches between two chaotic systems, it is more difficult for the intruder to detect useful information from the channel. In addition, two new schemes in which the chaotic signal used to mask (or modulate) the transmitted signal switches between two components of a chaotic system are proposed. In this case, the intruder can not easily find which component is used as a carrier. The rest of the paper is organized as follows: In Sec. II, the switching chaotic system is introduced. In Sec. III, adaptive synchronization of the system with unknown parameters is given. In Sec. IV, several communication schemes are presented based on adaptive synchronization and the switch scheme. Simulation examples are given to show the effectiveness of the proposed schemes in Sec V. Finally, the conclusion is drawn in Sec. VI.

II. THE SWITCHING SYSTEM

In Ref. 6, Lü *et al.* proposed a unified chaotic system

$$\dot{x} = (25\alpha + 10)(y - x), \quad \dot{y} = (28 - 35\alpha)x - xz + (29\alpha - 1)y, \quad \dot{z} = xy - \frac{\alpha + 8}{3}z, \tag{1}$$

where $\alpha \in [0,1]$. When $\alpha \in [0,0.8)$, system (1) belongs to the Lorenz chaotic system. When $\alpha = 0.8$, system (1) belongs to the Lü chaotic system. When $\alpha \in (0.8,1]$, system (1) is the Chen chaotic system. Based on this, Yu *et al.* introduced a modified chaotic system in Ref. 11,

$$\dot{x} = (25\alpha + a)(y - x), \quad \dot{y} = (b - 35\alpha)x - xz + (29\alpha - c)y, \quad \dot{z} = xy - \frac{\alpha + f}{3}z, \tag{2}$$

where $\alpha \in [0,1]$. When the parameters are taken as $(a,b,c,f) = (10,28,1,8)$, it is system (1). In Ref. 2, Rössler discussed another chaotic system

$$\dot{x} = -y - z, \quad \dot{y} = x + my, \quad \dot{z} = n + z(x - l). \tag{3}$$

Typical values of the parameters are $(m,n,l) = (0.2,0.2,5.7)$. In this paper, we propose a switching chaotic system

$$\begin{aligned} \dot{x} &= g(t)\{[25\beta(t) + a](y - x)\} + [1 - g(t)][-y - z], \\ \dot{y} &= g(t)\{[b - 35\beta(t)]x - xz + [29\beta(t) - c]y\} + [1 - g(t)][x + my], \\ \dot{z} &= g(t)\left[xy - \frac{\beta(t) + f}{3}z\right] + [1 - g(t)][n + z(x - l)], \end{aligned} \tag{4}$$

where a, b, c, f, m, n, and l are constant parameters, $\beta(t) \in [0,1]$, and $g(t)$ is a step function with respect to time t defined by

$$g(t) = \begin{cases} 1, & 2k\omega \leqslant t < (2k+1)\omega, \\ 0, & (2k+1)\omega \leqslant t < (2k+2)\omega, \ k = 0,1,2,\ldots, \end{cases} \tag{5}$$

where ω is a positive constant. When $2k\omega \leqslant t < (2k+1)\omega$, $k = 0,1,2,\ldots$, system (4) is the unified system (2). When $(2k+1)\omega \leqslant t < (2k+2)\omega$, $k = 0,1,2,\ldots$, system (4) is the Rössler system (3). As time t varies, system (4) switches between systems (2) and (3). The switching system exhibits more abundant chaotic behaviors as the switch scheme and more parameters are introduced. Moreover, one can find that the switching system is still chaotic when the parameters are not taken the typical values.

III. ADAPTIVE SYNCHRONIZATION OF THE SWITCHING SYSTEM

In this section, based on Lyapunov stability theory and adaptive control approach adaptive synchronization of the switching chaotic system is discussed.

Consider the following two chaotic switching systems with unknown parameters. Drive system with subscript d and response system with subscript r are described by

$$\begin{aligned} \dot{x}_d &= g(t)\{[25\beta(t) + a](y_d - x_d)\} + [1 - g(t)][-y_d - z_d], \\ \dot{y}_d &= g(t)\{[b - 35\beta(t)]x_d - x_d z_d + [29\beta(t) - c]y_d\} + [1 - g(t)][x_d + my_d], \\ \dot{z}_d &= g(t)\left[x_d y_d - \frac{\beta(t) + f}{3}z_d\right] + [1 - g(t)][n + z_d(x_d - l)], \end{aligned} \tag{6}$$

and

$$\begin{aligned} \dot{x}_r &= g(t)\{[25\beta(t) + \hat{a}(t)](y_r - x_r)\} + g(t)u_1 + [1 - g(t)][-y_r - z_r] + [1 - g(t)]u_1', \\ \dot{y}_r &= g(t)\{[\hat{b}(t) - 35\beta(t)]x_r - x_r z_r + [29\beta(t) - \hat{c}(t)]y_r\} + g(t)u_2 + [1 - g(t)][x_r + \hat{m}(t)y_r] + [1 - g(t)]u_2', \\ \dot{z}_r &= g(t)\left[x_r y_r - \frac{\beta(t) + \hat{f}(t)}{3}z_r\right] + g(t)u_3 + [1 - g(t)]\{\hat{n}(t) + z_r[x_r - \hat{l}(t)]\} + [1 - g(t)]u_3', \end{aligned} \tag{7}$$

where a, b, c, f, m, n, and l are unknown constant parameters to the response system, $\beta(t) \in [0,1]$, $g(t)$ is a function defined by Eq. (5), $\hat{a}(t)$, $\hat{b}(t)$, $\hat{c}(t)$, $\hat{f}(t)$, $\hat{m}(t)$, $\hat{n}(t)$, and $\hat{l}(t)$ are

functions with respect to time t, and u_1, u_2, u_3, u_1', u_2', and u_3' are the controllers. Subtracting system (6) from Eq. (7), then the error dynamical system can be written as

$$\dot{e}_1 = g(t)\{[25\beta(t)+a](e_2-e_1)+[\hat{a}(t)-a]\ (y_r-x_r)]\}+g(t)u_1 + [1-g(t)][-e_2-e_3]+[1-g(t)]u_1',$$

$$\dot{e}_2 = g(t)\{[b-35\beta(t)]e_1+[\hat{b}(t)-b]x_r+[29\beta(t)-c]e_2 - [\hat{c}(t)-c]y_r+e_1e_3-z_re_1-x_re_3\}+g(t)u_2 + [1-g(t)]\{e_1+[\hat{m}(t)-m]y_r+me_2\}+[1-g(t)]u_2', \quad (8)$$

$$\dot{e}_3 = g(t)\left[-\frac{\beta(t)+f}{3}e_3-\frac{\hat{f}(t)-f}{3}z_r-e_1e_2+y_re_1+x_re_2\right] + g(t)u_3+[1-g(t)]\{\hat{n}(t)-n+z_re_1+x_re_3-e_1e_3 - [\hat{l}(t)-l]z_r-le_3\}+[1-g(t)]u_3',$$

where $e_1=x_r-x_d$, $e_2=y_r-y_d$, and $e_3=z_r-z_d$. Choose the controllers and adaptive laws as

$$u_i=-k_ie_i,\quad u_1'=-k_1'e_1+e_3^2,\quad u_2'=-k_2'e_2,\quad u_3'=-k_3'e_3,$$

$$\dot{k}_i=g(t)e_i^2,\quad \dot{k}_i'=[1-g(t)]e_i^2,$$

$$\dot{\hat{a}}=-g(t)(y_r-x_r)e_1,\quad \dot{\hat{b}}=-g(t)x_re_2,\quad \dot{\hat{c}}=g(t)y_re_2, \quad (9)$$

$$\dot{\hat{f}}=g(t)\frac{z_r}{3}e_3,\quad \dot{\hat{m}}=-[1-g(t)]y_re_2,\quad \dot{\hat{n}}=-[1-g(t)]e_3,$$

$$\dot{\hat{l}}=[1-g(t)]z_re_3,$$

where $i=1,2,3$.

Choose a Lyapunov function candidate as follows:

$$V[e(t)]=\tfrac{1}{2}[e_1^2+e_2^2+e_3^2+(k_1-p_1)^2+(k_2-p_2)^2+(k_3-p_3)^2 + (k_1'-p_4)^2+(k_2'-p_5)^2+(k_3'-p_6)^2+(\hat{a}-a)^2 + (\hat{b}-b)^2+(\hat{c}-c)^2+(\hat{f}-f)^2+(\hat{m}-m)^2+(\hat{n}-n)^2 + (\hat{l}-l)^2], \quad (10)$$

where p_1, p_2, p_3, p_4, p_5, and p_6 are positive constants. Differentiating V along the solution of Eqs. (8) and (9), we have

$$\begin{aligned}
\dot{V}[e(t)] &= e_1\dot{e}_1+e_2\dot{e}_2+e_3\dot{e}_3+(k_1-p_1)\dot{k}_1+(k_2-p_2)\dot{k}_2+(k_3-p_3)\dot{k}_3+(k_1'-p_4)\dot{k}_1'+(k_2'-p_5)\dot{k}_2'+(k_3'-p_6)\dot{k}_3' \\
&\quad +(\hat{a}-a)\dot{\hat{a}}+(\hat{b}-b)\dot{\hat{b}}+(\hat{c}-c)\dot{\hat{c}}+(\hat{f}-f)\dot{\hat{f}}+(\hat{m}-m)\dot{\hat{m}}+(\hat{n}-n)\dot{\hat{n}}+(\hat{l}-l)\dot{\hat{l}} \\
&= g(t)\Big\{-[25\beta(t)+a]e_1^2+[25\beta(t)+a]e_1e_2+[\hat{a}(t)-a](y_r-x_r)e_1+[b-35\beta(t)]e_1e_2+[\hat{b}(t)-b]x_re_2 \\
&\quad +[29\beta(t)-c]e_2^2-[\hat{c}(t)-c]y_re_2+e_1e_2e_3-z_re_1e_2-x_re_2e_3-\frac{\beta(t)+f}{3}e_3^2-\frac{\hat{f}(t)-f}{3}z_re_3-e_1e_2e_3+y_re_1e_3+x_re_2e_3 \\
&\quad -k_1e_1^2-k_2e_2^2-k_3e_3^2\Big\}+[1-g(t)]\{-e_1e_2-e_1e_3+e_1e_2+[\hat{m}(t)-m]y_re_2+me_2^2+[\hat{n}(t)-n]e_3+z_re_1e_3+x_re_3^2 \\
&\quad -e_1e_3^2-[\hat{l}(t)-l]z_re_3-le_3^2-k_1'e_1^2+e_1e_3^2-k_2'e_2^2-k_3'e_3^2\}+g(t)[(k_1-p_1)e_1^2+(k_2-p_2)e_2^2+(k_3-p_3)e_3^2] \\
&\quad +[1-g(t)][(k_1'-p_4)e_1^2+(k_2'-p_5)e_2^2+(k_3'-p_6)e_3^2]+(\hat{a}-a)\dot{\hat{a}}+(\hat{b}-b)\dot{\hat{b}}+(\hat{c}-c)^2+(\hat{f}-f)^2 \\
&\quad +(\hat{m}-m)^2+(\hat{n}-n)^2+(\hat{l}-l)^2 \\
&= g(t)\Big\{-[25\beta(t)+a]e_1^2+[a+b-10\beta(t)-z_r]e_1e_2+[29\beta(t)-c]e_2^2-\frac{\beta(t)+f}{3}e_3^2+y_re_1e_3-p_1e_1^2-p_2e_2^2-p_3e_3^2\Big\} \\
&\quad +[1-g(t)]\{(z_r-l)e_1e_3+me_2^2+(x_r-l)e_3^2-p_4e_1^2-p_5e_2^2-p_6e_3^2\} \\
&\leqslant g(t)\left\{\left[-25\beta(t)-a+\frac{[a+b-10\beta(t)-z_r]^2}{2}+\frac{y_r^2}{2}-p_1\right]e_1^2+\left[29\beta(t)-c+\frac{1}{2}-p_2\right]e_2^2\right. \\
&\quad \left.+\left[-\frac{\beta(t)+f}{3}+\frac{1}{2}-p_3\right]e_3^2\right\}+[1-g(t)]\left\{\left[\frac{1}{2}-p_4\right]e_1^2+[m-p_5]e_2^2+\left[x_r-l+\frac{[z_r-l]^2}{2}-p_6\right]e_3^2\right\}. \quad (11)
\end{aligned}$$

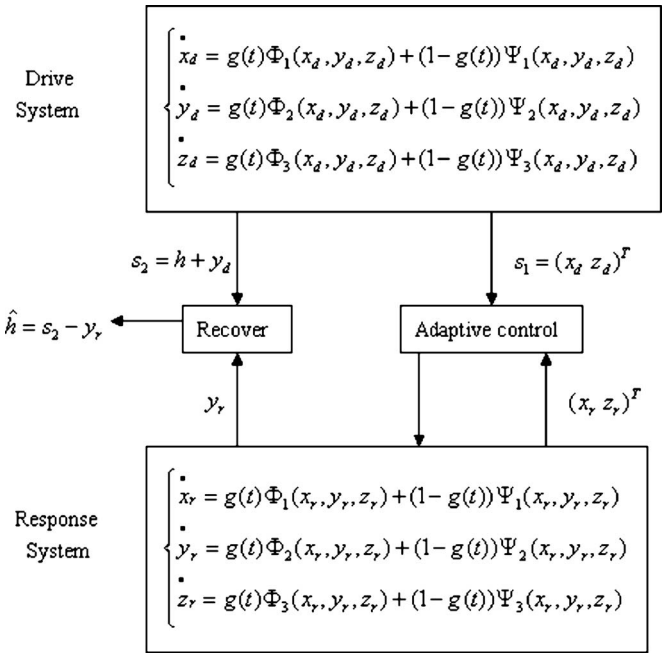

FIG. 1. Chaotic masking scheme, where $(\dot{x}\ \dot{y}\ \dot{z})^T=\Phi(x,y,z)=(\Phi_1\ \Phi_2\ \Phi_3)^T$ denotes the unified system (2) and $(\dot{x}\ \dot{y}\ \dot{z})^T=\Psi(x,y,z)=(\Psi_1\ \Psi_2\ \Psi_3)^T$ denotes the Rössler system (3).

Note that $\beta(t)$, $x_r(t)$, $y_r(t)$, and $z_r(t)$ are bounded. Let $p_1=\max\{-25\beta(t)-a+[a+b-10\beta(t)-z_r]^2/2+y_r^2/2\}+1$, $p_2=30\frac{1}{2}-c$, $p_3=-f/3+3/2$, $p_4=3/2$, $p_5=m+1$, and $p_6=\max\{x_r-l+[z_r-l]^2/2\}+1$. Then one obtains

$$\dot{V}[e(t)] \leqslant g(t)(-e_1^2-e_2^2-e_3^2)+[1-g(t)](-e_1^2-e_2^2-e_3^2) = -e_1^2-e_2^2-e_3^2. \tag{12}$$

From Eq. (12), one knows that the receiver system (7) synchronizes with the drive system (6).

IV. NEW COMMUNICATION SCHEMES BASED ON THE SWITCH METHOD

A. Applications of the switching system to secure communications

In this subsection, the applications of the switching system to secure communications are discussed based on the adaptive synchronization.

1. Chaotic masking

Yu *et al.* proposed a new communication scheme based on the chaotic masking scheme.[11] In this paper, the method is adopted here. The plaintext message $h(t)$ is masked by the chaotic signal y_d, and only x_d and z_d are used to drive the response system. It should be noted that the signal y_d is a component switches between two different chaotic systems. Under some restricted conditions of the parameters the drive and response system will achieve synchronization. If we denote by $s_2(t)=y_d+h(t)$ the transmitted chaotic signal, then $h(t)$ can be recovered by $\hat{h}(t)=s_2(t)-y_r$, since $y_r\to y_d$ as $t\to\infty$. The chaotic masking scheme is illustrated in Fig. 1, where $(\dot{x}\ \dot{y}\ \dot{z})^T=\Phi(x,y,z)=(\Phi_1\ \Phi_2\ \Phi_3)^T$ and $(\dot{x}\ \dot{y}\ \dot{z})^T=\Psi(x,y,z)=(\Psi_1\ \Psi_2\ \Psi_3)^T$ denote the unified system (2) and the Rössler system (3), respectively.

The equations for the drive system and the response system are

$$\begin{aligned}
\dot{x}_d &= g(t)\{[25\beta(t)+a](y_d-x_d)\}+[1-g(t)][-y_d-z_d],\\
\dot{y}_d &= g(t)\{[b-35\beta(t)]x_d-x_dz_d+[29\beta(t)-c]y_d\}\\
&\quad +[1-g(t)][x_d+my_d],\\
\dot{z}_d &= g(t)\left[x_dy_d-\frac{\beta(t)+f}{3}z_d\right]+[1-g(t)][n+z_d(x_d-l)],
\end{aligned} \tag{13}$$

and

$$\begin{aligned}
\dot{x}_r &= g(t)\{[25\beta(t)+a](y_r-x_r)\}\\
&\quad +g(t)u_1+[1-g(t)][-y_r-z_r]+[1-g(t)]u_1',\\
\dot{y}_r &= g(t)\{[b-35\beta(t)]x_r-x_rz_r+[29\beta(t)-c]y_r\}+g(t)u_2\\
&\quad +[1-g(t)][x_r+my_r]+[1-g(t)]u_2',\\
\dot{z}_r &= g(t)\left[x_ry_r-\frac{\beta(t)+\hat{f}(t)}{3}z_r\right]+g(t)u_3\\
&\quad +[1-g(t)]\{\hat{n}(t)+z_r[x_r-\hat{l}(t)]\}+[1-g(t)]u_3',
\end{aligned} \tag{14}$$

where f, n, and l are unknown parameters to the receiver, a, b, c, and m are known constant parameters, and other notations are the same as the above section. The proposed control is similar to the one in Eqs. (9) with the fact that now, the variable y_d will not be used to control, since it is variable used to mask, and as a consequence, $u_2=0$ and $u_2'=0$. Thus the controllers and adaptive laws are designated by

$$\begin{aligned}
&u_i=-k_ie_i,\quad u_2=0,\quad u_1'=-k_1'e_1+e_3^2,\quad u_2'=0,\\
&u_3'=-k_3'e_3,\quad \dot{k}_i=g(t)e_i^2,\quad \dot{k}_i'=[1-g(t)]e_i^2,\\
&\hat{f}=g(t)\frac{z_r}{3}e_3,\quad \hat{n}=-[1-g(t)]e_3,\quad \dot{\hat{l}}=[1-g(t)]z_re_3,
\end{aligned} \tag{15}$$

where $i=1,3$. Equation (15) is independent of y_d, since only x_d and z_d are transmitted by the drive system.

Choose a Lyapunov function candidate as follows:

$$\begin{aligned}
V[e(t)] &= \tfrac{1}{2}[e_1^2+e_2^2+e_3^2+(k_1-p_1)^2+(k_3-p_3)^2+(k_1'-p_4)^2\\
&\quad +(k_3'-p_6)^2+(\hat{f}-f)^2+(\hat{n}-n)^2+(\hat{l}-l)^2],
\end{aligned} \tag{16}$$

where p_1, p_3, p_4, and p_6 are positive constants. Then the derivative of V with respect to time along the solution of Eqs. (13)–(15) is

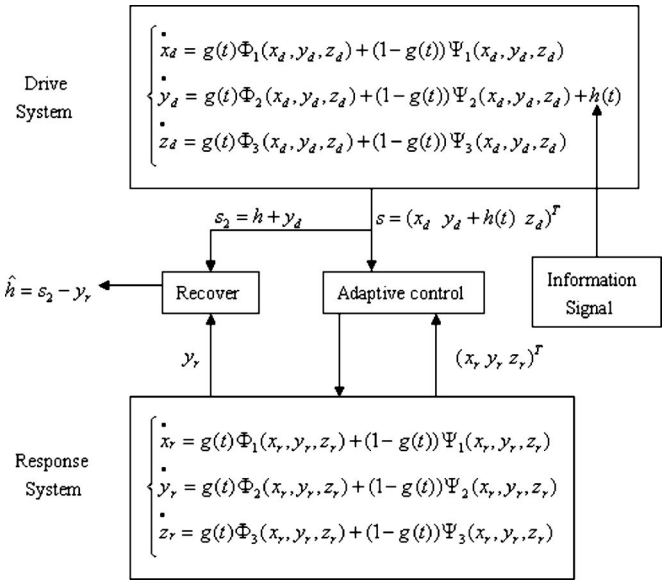

FIG. 2. Chaotic modulation scheme, where $(\dot{x}\ \dot{y}\ \dot{z})^T=\Phi(x,y,z)=(\Phi_1\ \Phi_2\ \Phi_3)^T$ denotes the unified system (2) and $(\dot{x}\ \dot{y}\ \dot{z})^T=\Psi(x,y,z)=(\Psi_1\ \Psi_2\ \Psi_3)^T$ denotes the Rössler system (3).

$$\dot{V}[e(t)] \leqslant g(t)\Bigg(\Bigg\{-25\beta(t)-a+\rho\frac{[a+b-10\beta(t)-z_r]^2}{2}+\frac{y_r^2}{2}-p_1\Bigg\}e_1^2+\Bigg[29\beta(t)-c+\frac{1}{2\rho}\Bigg]e_2^2+\Bigg[-\frac{\beta(t)+f}{3}+\frac{1}{2}-p_3\Bigg]e_3^2\Bigg)+[1-g(t)]\Bigg(\Bigg[\frac{1}{2}-p_4\Bigg]e_1^2+me_2^2+\Bigg\{x_r-l+\frac{[z_r-l]^2}{2}-p_6\Bigg\}e_3^2\Bigg). \tag{17}$$

Choosing $c>29\geqslant\max|29\beta(t)|$, $m<0$, sufficient large positive constants ρ, and appropriate p_i, one can obtain

$$\dot{V}[e(t)] \leqslant -e_1^2-\varepsilon e_2^2-e_3^2, \tag{18}$$

where ε is a positive constant. From Eq. (18) one knows that the receiver system (14) synchronizes with the drive system (13). Thus, we can recover the plaintext message by $\hat{h}(t)=h(t)+y_d-y_r$. In practice, c must be chosen to guarantee the switching system chaotic. In this paper one often chooses $0<c\leqslant 7$ and $0\leqslant\beta(t)<c/29$.

2. Chaotic modulation

In this subsection, we discuss the application of the switching system based on the chaotic modulation scheme proposed in Ref. 11. The modulation scheme is illustrated in Fig. 2. In this case, the plaintext message $h(t)$ is modulated into the component y_d of the switching system and the transmitted signal is $[x_d\ y_d+h(t)\ z_d]^T$. If the receiver system synchronizes with the drive system, then the plaintext message $h(t)$ can be recovered by $\hat{h}(t)=s_2(t)-y_r$, where $s_2(t)=y_d+h(t)$. As the chaotic signal used to modulate the plaintext is a component switching between two different chaotic systems, it is more difficult for the attacker to detect the useful message from the channel.

The equations for the drive system and response systems are

$$\begin{aligned}
\dot{x}_d &= g(t)\{[25\beta(t)+a](y_d-x_d)\}+[1-g(t)][-y_d-z_d],\\
\dot{y}_d &= g(t)\{[b-35\beta(t)]x_d-x_dz_d+[29\beta(t)-c]y_d\}\\
&\quad+[1-g(t)][x_d+my_d]+h(t),\\
\dot{z}_d &= g(t)\left[x_dy_d-\frac{\beta(t)+f}{3}z_d\right]+[1-g(t)][n+z_d(x_d-l)],
\end{aligned} \tag{19}$$

and

$$\begin{aligned}
\dot{x}_r &= g(t)\{[25\beta(t)+a](y_r-x_r)\}+g(t)u_1\\
&\quad+[1-g(t)][-y_r-z_r]+[1-g(t)]u_1',\\
\dot{y}_r &= g(t)\{[b-35\beta(t)]x_r-x_rz_r+[29\beta(t)-c]y_r\}\\
&\quad+g(t)u_2+(1-g(t))[x_r+my_r]+[1-g(t)]u_2',\\
\dot{z}_r &= g(t)\left[x_ry_r-\frac{\beta(t)+\hat{f}(t)}{3}z_r\right]+g(t)u_3\\
&\quad+[1-g(t)]\{\hat{n}(t)+z_r[x_r-\hat{l}(t)]\}+[1-g(t)]u_3',
\end{aligned} \tag{20}$$

where f, n, and l are unknown parameters to the receiver, a, b, c, and m are known constant parameters, and other notations are the same as the above section. Subtracting Eq. (19) from Eq. (20), then the error dynamical system can be written as

$$\begin{aligned}
\dot{e}_1 &= g(t)\{[25\beta(t)+a](e_2-e_1)\}-g(t)k_1e_1\\
&\quad+[1-g(t)][-e_2-e_3]+[1-g(t)](-k_1'e_1+e_3^2),\\
\dot{e}_2 &= g(t)\{[b-35\beta(t)]e_1+[\hat{b}(t)-b]x_r+[29\beta(t)-c]e_2\\
&\quad-[\hat{c}(t)-c]y_r+e_1e_3-z_re_1-x_re_3\}-g(t)e_2\\
&\quad+[1-g(t)]\{e_1+[\hat{m}(t)-m]y_r+me_2\}-[1-g(t)]e_2,\\
\dot{e}_3 &= g(t)\left[-\frac{\beta(t)+f}{3}e_3-\frac{\hat{f}(t)-f}{3}z_r-e_1e_2+y_re_1+x_re_2\right]\\
&\quad-g(t)k_3e_3+[1-g(t)]\{\hat{n}(t)-n+z_re_1+x_re_3\\
&\quad-e_1e_3-[\hat{l}(t)-l]z_r-le_3\}-[1-g(t)]k_3'e_3,
\end{aligned} \tag{21}$$

where $e_1=x_r-x_d$, $e_2=y_r-y_d$, and $e_3=z_r-z_d$. Noting that the transmitted signal is $[x_d\ y_d+h(t)\ z_d]^T$, we choose the controllers and adaptive laws similar to the one in Eqs. (9),

$$\begin{aligned}
&u_i=-k_ie_i,\quad u_2=u_2'=-[y_r-(y_d+h(t))],\quad u_1'=-k_1'e_1+e_3^2,\\
&u_3'=-k_3'e_3,\quad \dot{k}_i=g(t)e_i^2,\quad \dot{k}_i'=[1-g(t)]e_i^2,\\
&\dot{\hat{f}}=g(t)\frac{z_r}{3}e_3,\quad \dot{\hat{n}}=-[1-g(t)]e_3,\quad \dot{\hat{l}}=[1-g(t)]z_re_3,
\end{aligned} \tag{22}$$

where $i=1,3$.

Choose a Lyapunov function candidate as follows:

$$V[e(t)] = \tfrac{1}{2}[e_1^2 + e_2^2 + e_3^2 + (k_1 - p_1)^2 + (k_3 - p_3)^2 + (k_1' - p_4)^2 + (k_3' - p_6)^2 + (\hat{f} - f)^2 + (\hat{n} - n)^2 + (\hat{l} - l)^2], \quad (23)$$

where p_1, p_3, p_4, and p_6 are positive constants. Differentiating V along the solution of Eqs. (21) and (22), similar to Eq. (11), one has

$$\dot{V}[e(t)] \leqslant g(t)\left(\left\{-25\beta(t) - a + \rho\frac{[a + b - 10\beta(t) - z_r]^2}{2} + \frac{y_r^2}{2} - p_1\right\}e_1^2 + \left[29\beta(t) - c + \frac{1}{2\rho} - 1\right]e_2^2 + \left[-\frac{\beta(t) + f}{3} + \frac{1}{2} - p_3\right]e_3^2\right) + [1 - g(t)]\left\{\left[\frac{1}{2} - p_4\right]e_1^2 + (m - 1)e_2^2 + \left[x_r - l + \frac{[z_r - l]^2}{2} - p_6\right]e_3^2\right\}. \quad (24)$$

Choosing $c + 1 > 29 \geqslant \max|29\beta(t)|$, $m < 1$, sufficient large positive constants ρ, and appropriate p_i, one obtains

$$\dot{V}[e(t)] \leqslant -e_1^2 - \varepsilon e_2^2 - e_3^2, \quad (25)$$

where ε is a positive constant. From Eq. (25) one knows that the response system (20) synchronizes with the drive system (19). As discussed in the above subsection, c must be chosen to guarantee the switching system chaotic. Here we often choose $-1 < c \leqslant 7$ and $0 \leqslant \beta(t) < (c+1)/29$.

3. Chaotic shift key

The unknown constant parameters of the drive system can be correctly estimated by the receiver system based on the adaptive synchronization method. In previous works,[9,11] the authors pointed out that the receiver system can also estimate slow varying variables, such that $\dot{\theta} \approx 0$ (θ is a system parameter) or piecewise constant such that $\dot{\theta} = 0$ everywhere except at some discrete instants of time. Therefore, if a digital information signal is modulated into some parameter (or parameters), the response system can estimate these variations and hence recover the information signal. Here, we introduce the switch scheme into the communication scheme. In this situation, a binary signal is modulated into different parameters as time varies. The equations for the drive system are

$$\dot{x}_d = g(t)\{[25\beta(t) + a](y_d - x_d)\} + [1 - g(t)][-y_d - z_d],$$

$$\dot{y}_d = g(t)\{[b - 35\beta(t)]x_d - x_d z_d + [29\beta(t) - g(t)h(t)]y_d\} + [1 - g(t)]\{x_d + [1 - g(t)]h(t)y_d\}, \quad (26)$$

$$\dot{z}_d = g(t)\left[x_d y_d - \frac{\beta(t) + f}{3}z_d\right] + [1 - g(t)][n + z_d(x_d - l)],$$

and the response system is

$$\dot{x}_r = g(t)\{[25\beta(t) + \hat{a}(t)](y_r - x_r)\} + g(t)u_1 + [1 - g(t))[-y_r - z_r] + [1 - g(t)]u_1',$$

$$\dot{y}_r = g(t)\{[\hat{b}(t) - 35\beta(t)]x_r - x_r z_r + [29\beta(t) - \hat{c}(t)]y_r\} + g(t)u_2 + [1 - g(t)][x_r + \hat{m}(t)y_r] + [1 - g(t)]u_2', \quad (27)$$

$$\dot{z}_r = g(t)\left[x_r y_r - \frac{\beta(t) + \hat{f}(t)}{3}z_r\right] + g(t)u_3 + [1 - g(t)]\{\hat{n}(t) + z_r[x_r - \hat{l}(t)]\} + [1 - g(t)]u_3',$$

where $g(t)$ is a step function defined by Eq. (5), and $h(t)$ is a binary signal. The signal is modulated into system parameter c or m as time varies. With the controllers and adaptive laws designated by Eq. (9), the parameters in the response system will converge to those in the drive system based on adaptive synchronization discussed in Sec. III. Thus the signal can be recovered by $\hat{h}(t) = g(t)\hat{c}(t) + [1 - g(t)]\hat{m}(t)$.

Remark: In addition, the signal information can be divided into several parts, and each part is modulated into a system parameter, respectively. Thus one can easily recover the signal by combining the corresponding parameters in the receiver system together. For example, the binary signal can be modulated into the parameters c and m, and the corresponding drive system is

$$\dot{x}_d = g(t)\{[25\beta(t) + a](y_d - x_d)\} + [1 - g(t)][-y_d - z_d],$$

$$\dot{y}_d = g(t)\left\{[b - 35\beta(t)]x_d - x_d z_d + \left[29\beta(t) - \frac{h(t)}{2}\right]y_d\right\} + [1 - g(t)]\left[x_d + \frac{h(t)}{2}y_d\right], \quad (28)$$

$$\dot{z}_d = g(t)\left[x_d y_d - \frac{\beta(t) + f}{3}z_d\right] + [1 - g(t)][n + z_d(x_d - l)].$$

The response system is Eq. (7). One would demodulate the message by $\hat{h}(t) = \hat{c}(t) + \hat{m}(t)$. In fact, the parameters c, f, m, n, and l all could be used to modulate the signal. Thus one can choose several parameters from them randomly to modulate the signal. It is very difficult for the attacker to ascertain which parameter (or parameters) is used to modulate the transmitted signal. The wide choice range enhances the security of this communication scheme.

B. Other communication schemes

In this subsection, we use the unified system (2) instead of the switching system (4) as a transmitter. It is noted, in Ref. 11, that the chaotic signal used to mask (or modulate) the information signal is only one component of the chaotic system. Here, we show two new methods to mask (or modulate) the information signal in which the chaotic signal used to mask (or modulate) could switch between two components of the unified system. These methods could also be introduced into other chaotic systems when they serve as transmitters in secure communication.

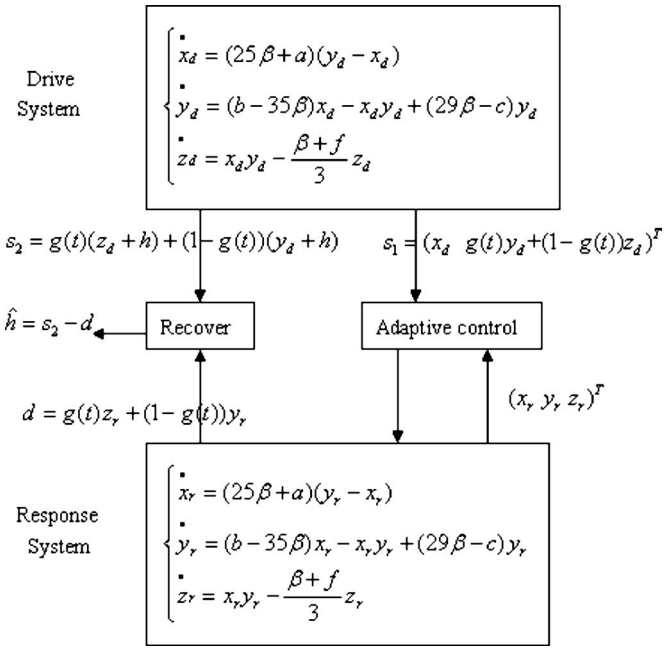

FIG. 3. Switch masking scheme.

1. A switch scheme based on chaotic masking

In this scheme, the chaotic signal used to mask the plaintext message $h(t)$ switches between two components y_d and z_d of a chaotic system. When $2k\omega \leqslant t < (2k+1)\omega$, $k=0,1,2,\ldots, g(t)=1$, z_d is added into the plaintext message $h(t)$ for masking the signal, and x_d and y_d are used to drive the response system. When $(2k+1)\omega \leqslant t < (2k+2)\omega$, $k=0,1,2,\ldots, g(t)=0$, y_d is used to mask $h(t)$, and x_d and z_d are enough to drive the response system. If we use the transmitted signal $s_2(t)=g(t)[z_d+h(t)]+[1-g(t)][y_d+h(t)]$, then the plaintext signal $h(t)$ can be recovered by $\hat{h}(t)=s_2(t)-\{g(t)z_r+[1-g(t)]y_r\}$, as the response system will synchronize with the drive system. The switch masking scheme is depicted in Fig. 3.

The drive system and response system are defined below, respectively,

$$\dot{x}_d = [25\beta(t) + a](y_d - x_d),$$

$$\dot{y}_d = [b - 35\beta(t)]x_d - x_d z_d + [29\beta(t) - c]y_d, \tag{29}$$

$$\dot{z}_d = x_d y_d - \frac{\beta(t) + f}{3} z_d,$$

and

$$\dot{x}_r = [25\beta(t) + a](y_r - x_r) + u_1,$$

$$\dot{y}_r = [b - 35\beta(t)]x_r - x_r z_r + [29\beta(t) - c]y_r + g(t)u_2, \tag{30}$$

$$\dot{z}_r = x_r y_r - \frac{\beta(t) + f}{3} z_r + [1 - g(t)]u_3,$$

where a, b, c, and f are known constant parameters, and other notations are defined as in Sec. III. The controllers are designated by

$$u_i = -k_i e_i, \quad \dot{k}_1 = e_1^2, \quad \dot{k}_2 = g(t)e_2^2, \quad \dot{k}_3 = [1 - g(t)]e_3^2, \tag{31}$$

where $i=1,2,3$. Subtracting system (29) from Eq. (30), one has

$$\dot{e}_1 = [25\beta(t) + a](e_2 - e_1) + u_1,$$

$$\dot{e}_2 = [b - 35\beta(t)]e_1 + [29\beta(t) - c]e_2 + e_1 e_3 - z_r e_1 - x_r e_3 + g(t)u_2, \tag{32}$$

$$\dot{e}_3 = -\frac{\beta(t) + f}{3} e_3 - e_1 e_2 + y_r e_1 + x_r e_2 + [1 - g(t)]u_3,$$

where $e_1=x_r-x_d$, $e_2=y_r-y_d$, and $e_3=z_r-z_d$.

Choose the following Lyapunov function candidate:

$$V[e(t)] = \tfrac{1}{2}[e_1^2 + e_2^2 + e_3^2 + (k_1 - p)^2 + k_2^2 + k_3^2], \tag{33}$$

where p is a positive constant. Differentiating V along the solution of Eqs. (31) and (32), similarly to the above process, one has

$$\dot{V}[e(t)] \leqslant \left\{ -25\beta(t) - a + \rho_1 \frac{[a + b - 10\beta(t) - z_r]^2}{2} + \frac{\rho_2 y_r^2}{2} - p \right\} e_1^2 + \left[29\beta(t) - c + \frac{1}{2\rho_1} \right] e_2^2 + \left[-\frac{\beta(t) + f}{3} + \frac{1}{2\rho_2} \right] e_3^2. \tag{34}$$

Choosing $c > 29 \geqslant \max|29\beta(t)|$, $f > 1 \geqslant \max|\beta(t)|$, sufficient large positive constants ρ_i, and appropriate p, one obtains

$$\dot{V}[e(t)] \leqslant -e_1^2 - \varepsilon_1 e_2^2 - \varepsilon_2 e_3^2, \tag{35}$$

where ε_1 and ε_2 are positive constants. From Eq. (35) one knows that the response system (30) synchronizes with the drive system (29). Thus, we can recover the plaintext message by $\hat{h}(t)=s_2(t)-\{g(t)z_r+[1-g(t)]y_r\}$. As discussed in the above subsection, c must be chosen to guarantee the system chaotic. Here we often choose $0 < c \leqslant 2$ and $0 \leqslant \beta(t) < c/29$.

2. A switch scheme based on chaotic modulation

In this subsection, the switch method is introduced into the chaotic modulation scheme. The equations for the drive system and response system are

$$\dot{x}_d = [25\beta(t) + a](y_d - x_d),$$

$$\dot{y}_d = [b - 35\beta(t)]x_d - x_d z_d + [29\beta(t) - c]y_d + g(t)h(t), \tag{36}$$

$$\dot{z}_d = x_d y_d - \frac{\beta(t) + f}{3} z_d + [1 - g(t)]h(t),$$

and

$$\dot{x}_r = [25\beta(t) + a](y_r - x_r) + u_1,$$

$$\dot{y}_r = [b - 35\beta(t)]x_r - x_r z_r + [29\beta(t) - c]y_r + g(t)u_2, \tag{37}$$

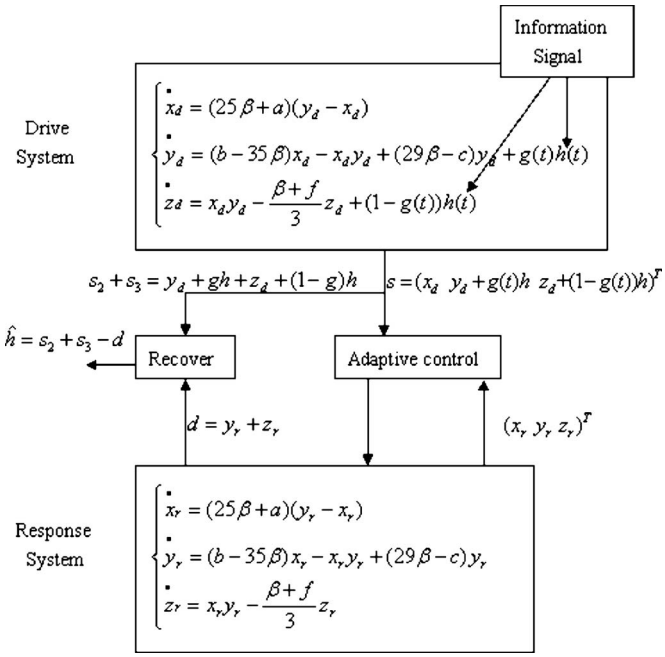

FIG. 4. Switch modulation scheme.

$$\dot{z}_r = x_r y_r - \frac{\beta(t)+f}{3} z_r + [1-g(t)]u_3,$$

where a, b, c, and f are known constant parameters, and other notations are defined as in Sec. III. The controllers are designated by

$$u_1 = -k_1 e_1, \quad \dot{k}_1 = e_1^2, \quad u_2 = -[y_r - y_d - h(t)],$$
$$u_3 = -[z_r - z_d - h(t)]. \tag{38}$$

The plaintext message $h(t)$ is modulated into the chaotic signal y_d when $2k\omega \leqslant t < (2k+1)\omega$, $k=0,1,2,\ldots$ as $g(t)=1$. While $(2k+1)\omega \leqslant t < (2k+2)\omega$, $k=0,1,2,\ldots$, the message $h(t)$ is modulated into z_d as $g(t)=0$. Thus the message $h(t)$ is modulated into a signal which switches between two components of the unified system. The transmitted signal is $s = \{x_d \ y_d + g(t)h(t) \ z_d + [1-g(t)]h(t)\}^T$. As the response system will synchronize with the drive system, the message $h(t)$ can be recovered by $\hat{h}(t) = s_2(t) + s_3(t) - y_r - z_r$, where $s_2 = y_d + g(t)h(t)$ and $s_3 = z_d + [1-g(t)]h(t)$. The switch modulation scheme is illustrated in Fig. 4. Subtracting system (36) from Eq. (37) yields the following error dynamical system:

$$\dot{e}_1 = [25\beta(t) + a](e_2 - e_1) + u_1,$$
$$\dot{e}_2 = [b - 35\beta(t)]e_1 + [29\beta(t) - c]e_2 + e_1 e_3 - z_r e_1 - x_r e_3 - g(t)e_2, \tag{39}$$
$$\dot{e}_3 = -\frac{\beta(t)+f}{3} e_3 - e_1 e_2 + y_r e_1 + x_r e_2 - [1-g(t)]e_3,$$

where $e_1 = x_r - x_d$, $e_2 = y_r - y_d$, and $e_3 = z_r - z_d$.

Choose a Lyapunov function candidate as follows:

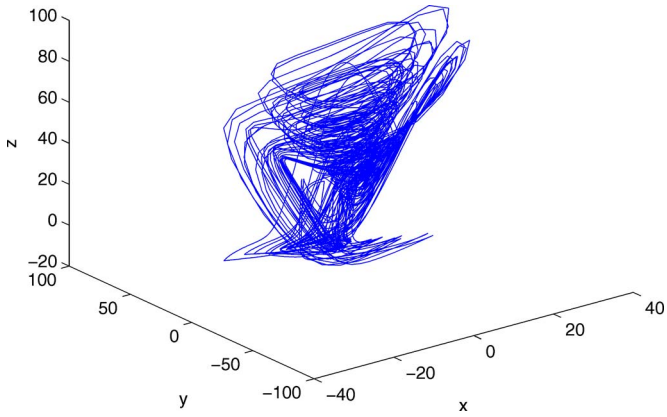

FIG. 5. (Color online) Trajectories of the drive system (6).

$$V[e(t)] = \tfrac{1}{2}[e_1^2 + e_2^2 + e_3^2 + (k_1 - p)^2], \tag{40}$$

where p is a positive constant. Differentiating V along the solution of Eqs. (38) and (39), similar to the above process, one has

$$\dot{V}[e(t)] \leqslant \left\{ -25\beta(t) - a + \rho_1 \frac{[a+b-10\beta(t)-z_r]^2}{2} + \frac{\rho_2 y_r^2}{2} - p \right\} e_1^2 + \left[29\beta(t) - c + \frac{1}{2\rho_1} \right] e_2^2 + \left[-\frac{\beta(t)+f}{3} + \frac{1}{2\rho_2} \right] e_3^2 - g e_2^2 - [1-g(t)]e_3^2. \tag{41}$$

Choosing $c > 29 \geqslant \max|29\beta(t)|$, $f > 1 \geqslant \max|\beta(t)|$, sufficient large positive constants ρ_i, and appropriate p, one obtains

$$\dot{V}[e(t)] \leqslant -e_1^2 - \varepsilon_1 e_2^2 - \varepsilon_2 e_3^2, \tag{42}$$

where ε_1 and ε_2 are positive constants. From Eq. (42), one knows that the response system (37) synchronizes with the drive system (36). Thus, the plaintext message can be recovered by $\hat{h}(t) = s_2 + s_3 - y_r - z_r$, since $y_r \to y_d$ and $z_r \to z_d$ as $t \to \infty$. As discussed in the above subsection, in order to guarantee the system chaotic, we often choose $0 < c \leqslant 2$ and $0 \leqslant \beta(t) < c/29$.

V. NUMERICAL EXAMPLES

In this section, the simulation results are given to verify the effectiveness and feasibility of the proposed methods.

A. Adaptive synchronization of the switching system

First, the numerical results about the adaptive synchronization of the switching system are shown. Consider the drive system (6) with parameters $(a,b,c,f,m,n,l) = (10,28,1,8,0.2,0.2,5.7)$, $\omega = 1.2$, and $\beta(t) = [1+\sin(t)]/2$. The response system is Eq. (7) with the controllers and adaptive laws as Eq. (9). The dynamical behavior of the drive system (6) is shown in Fig. 5, from which we can find it is chaotic. The trajectories of error dynamical system (8) are depicted in Fig. 6, which illustrates the receiver system (7) synchronizes with the drive system (6). In addition, the adap-

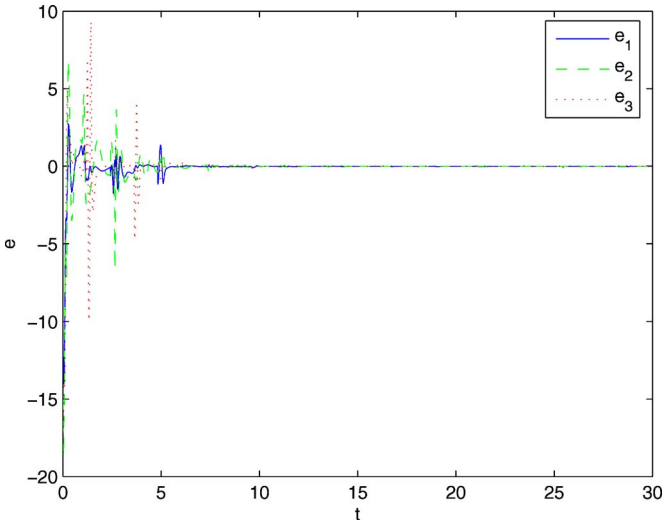

FIG. 6. (Color online) Error states of the drive system (6) and the response system (7).

tive functions $\hat{a}$, $\hat{b}$, $\hat{c}$, $\hat{f}$, $\hat{m}$, $\hat{n}$, $\hat{l}$, k_i, and k_i' in receiver system (7) are drawn in Figs. 7 and 8, respectively. As can be seen from Fig. 7, the parameters a, b, c, f, m, n, and l can be estimated by the response system parameters $\hat{a}$, $\hat{b}$, $\hat{c}$, $\hat{f}$, $\hat{m}$, $\hat{n}$, and $\hat{l}$, respectively.

1. Chaotic masking

Consider the drive system (13) with the parameters $(a,b,c,f,m,n,l)=(9,27,7,8,-0.2,0.2,5.5)$, $\omega=1$, and $\beta(t)=3[1+\sin(t)]/29$. The response system is Eq. (14) with the controllers and adaptive laws (15). The plaintext $h(t)=10\cos(t)$ and the transmitted signal is $s_2(t)=h(t)+y_d$. The error states and adaptive functions $\hat{f}$, $\hat{n}$, and $\hat{l}$ in response system (14) are illustrated in Figs. 9 and 10, respectively. One can find that the message $h(t)$ can be recovered successfully by $\hat{h}(t)=s_2(t)-y_r$ from Fig. 11. The error between the

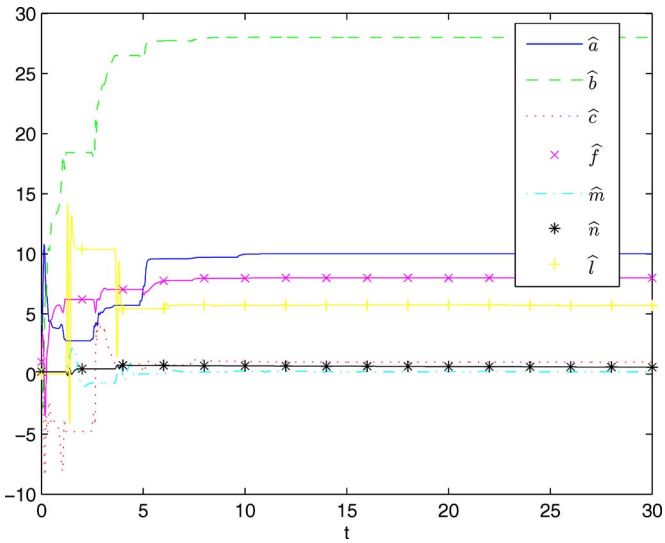

FIG. 7. (Color online) States of functions $\hat{a}(t)$, $\hat{b}(t)$, $\hat{c}(t)$, $\hat{f}(t)$, $\hat{m}(t)$, $\hat{n}(t)$, and $\hat{l}(t)$ in the response system (7).

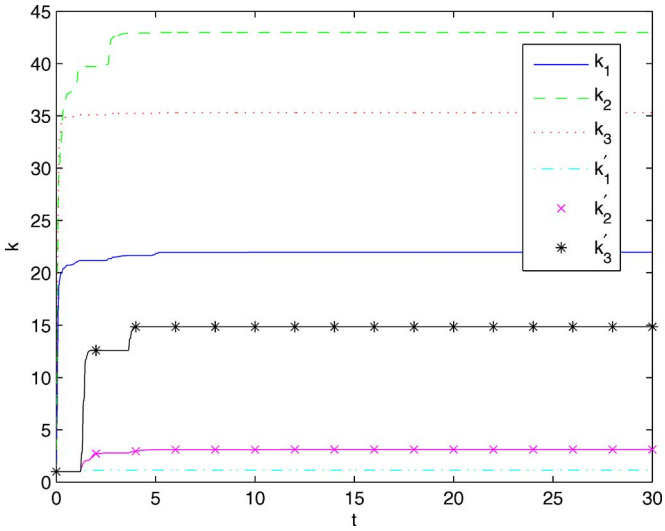

FIG. 8. (Color online) States of functions k_i and k_i' in the response system (7).

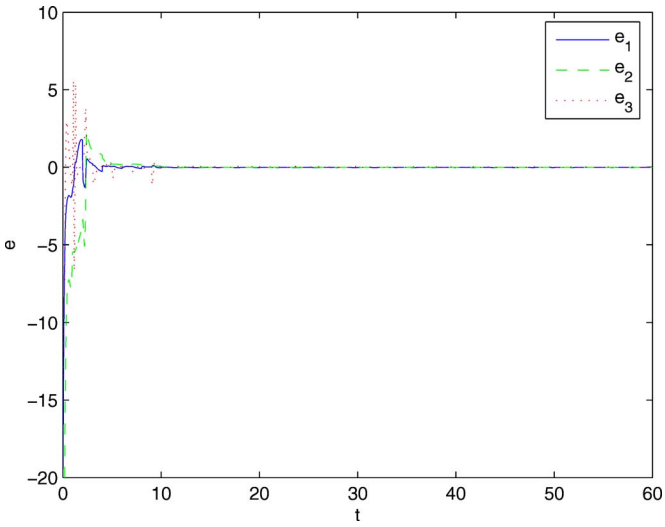

FIG. 9. (Color online) Error states of the drive system (13) and the response system (14) with $\omega=1$.

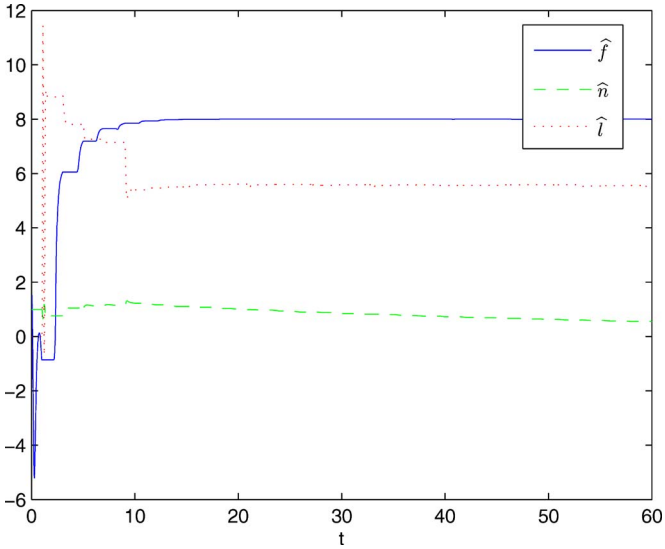

FIG. 10. (Color online) States of functions $\hat{f}(t)$, $\hat{n}(t)$, and $\hat{l}(t)$ in the response system (14) with $\omega=1$.

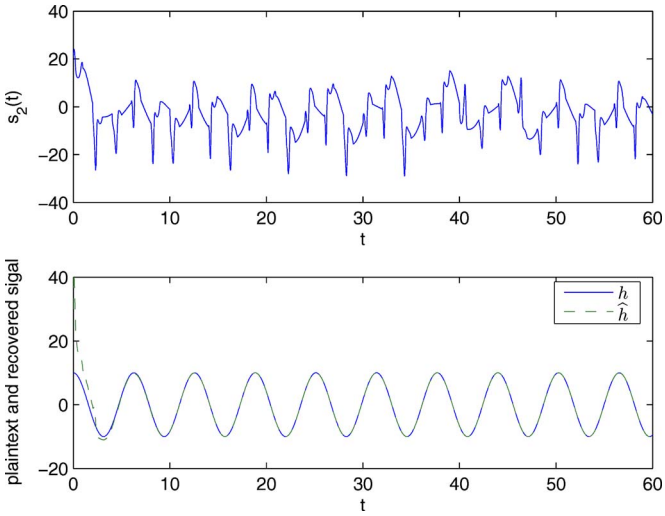

FIG. 11. (Color online) States of the transmitted signal $s_2(t)$, the plaintext $h(t)$, and the recovered signal $\hat{h}(t)$ (ω=1).

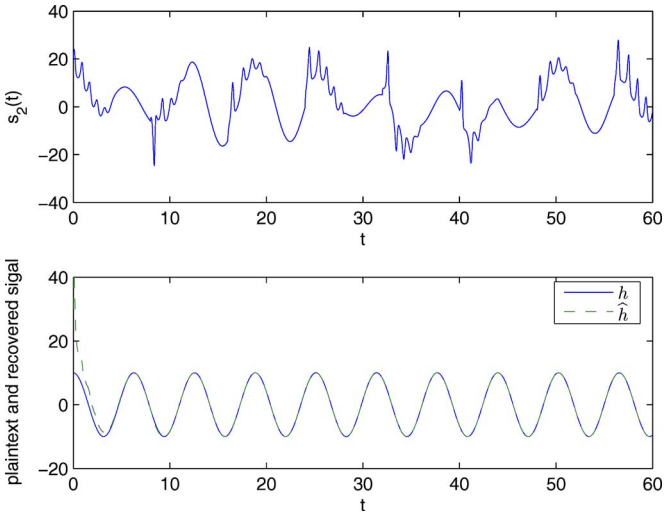

FIG. 13. (Color online) States of the transmitted signal $s_2(t)$, the plaintext $h(t)$, and the recovered signal $\hat{h}(t)$ (ω=4).

original information signal $h(t)$ and the recovered one $\hat{h}(t)$ are depicted in Fig. 12. From Fig. 12, it is easy to find that the information signal $\hat{h}(t)$ is recovered after $t \approx 11$ with fluctuation for mismatch $|h(t)-\hat{h}(t)| \leqslant 2^{-4}$.

Different values of ω in the step function $g(t)$ can lead to different speed for recovering the information signal. When the values of the parameters are taken as above except ω =4 and ω=1/4, the corresponding numerical results are illustrated in Figs. 13 and 14, and Figs. 15 and 16, respectively. In Fig. 14 when ω=4, it takes a little longer time ($t \approx 48$) to recover the information signal with fluctuation for mismatch $|h(t)-\hat{h}(t)| \leqslant 2^{-4}$. When ω=0.25, as can be seen from Fig. 16, the information signal is recovered after $t \approx 28$ with fluctuation for smaller mismatch $|h(t)-\hat{h}(t)| \leqslant 2^{-5.5}$.

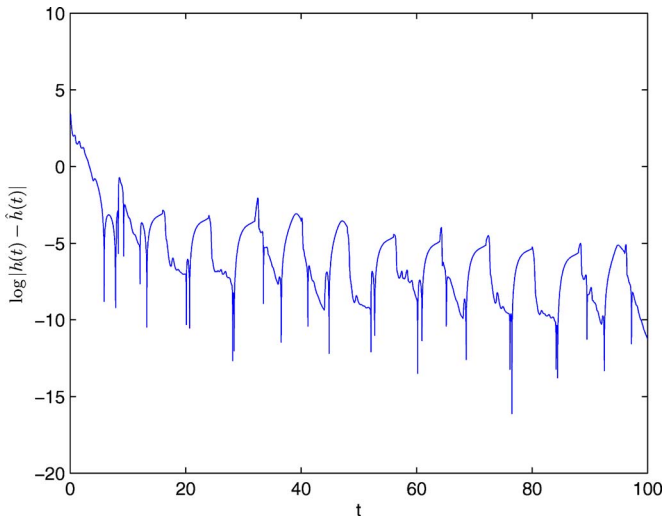

FIG. 14. (Color online) The variation of $\log|h(t)-\hat{h}(t)|$ with the time scale t (ω=4).

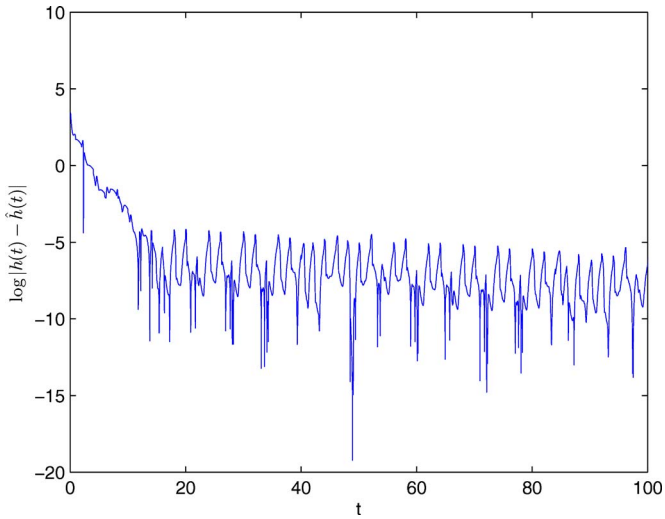

FIG. 12. (Color online) The variation of $\log|h(t)-\hat{h}(t)|$ with the time scale t (ω=1).

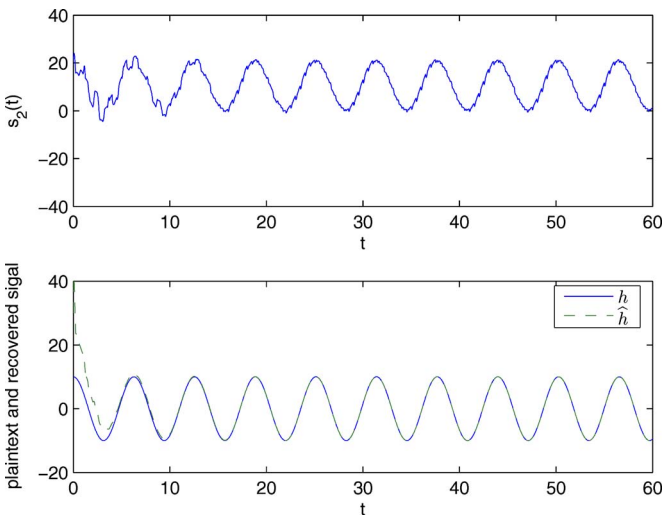

FIG. 15. (Color online) States of the transmitted signal $s_2(t)$, the plaintext $h(t)$, and the recovered signal $\hat{h}(t)$ (ω=0.25).

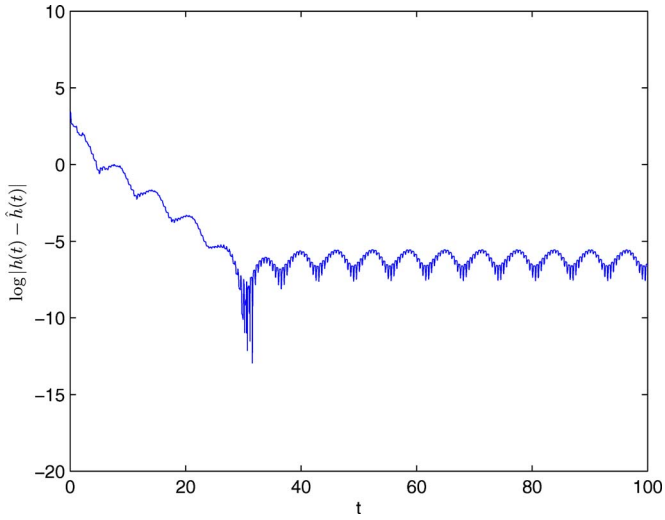

FIG. 16. (Color online) The variation of $\log|h(t)-\hat{h}(t)|$ with the time scale t ($\omega=0.25$).

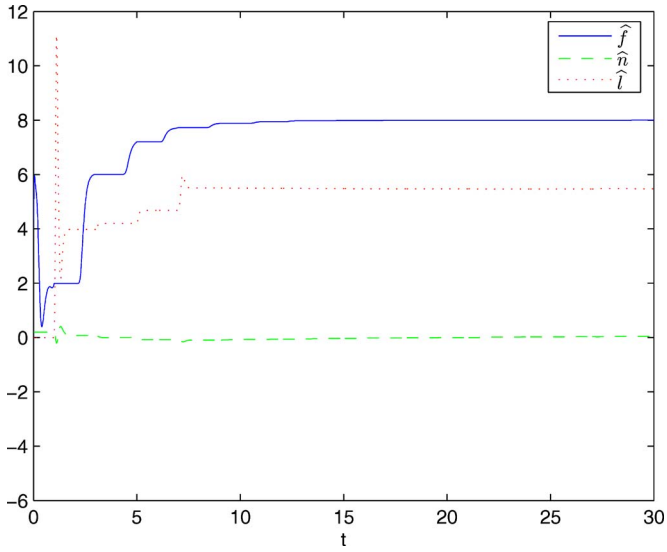

FIG. 18. (Color online) States of functions $\hat{f}(t)$, $\hat{n}(t)$, and $\hat{l}(t)$ in the response system (20).

2. Chaotic modulation

In this subsection, the plaintext is modulated into the drive switching system, which switches between the Rössler system and the unified system. The values of the parameters in system (19) are taken as $(a,b,c,f,m,n,l)=(12,25,7,8,-1,0.2,5.5)$, $\omega=1$, and $\beta(t)=3.4[1+\sin(t)]/29$. The plaintext message is $h(t)=10\sin(2t)$. The response system and the controllers and adaptive laws are Eqs. (20) and (22), respectively. The error states and adaptive functions $\hat{f}$, $\hat{n}$, and $\hat{l}$ in response system (20) are illustrated in Figs. 17 and 18, respectively. The transmitted signal $s_2(t)=h(t)+y_d$ and the recovered signal $\hat{h}=s_2(t)-y_r$ are drawn in Fig. 19, from which one can find that the message can be demodulated successfully.

In order to study the time required for recovering the information signal and the accuracy of the recovered signal, we use sinusoidal functions with three frequencies for simulation. Figures 19–24 show the transmitted signal, the recov-

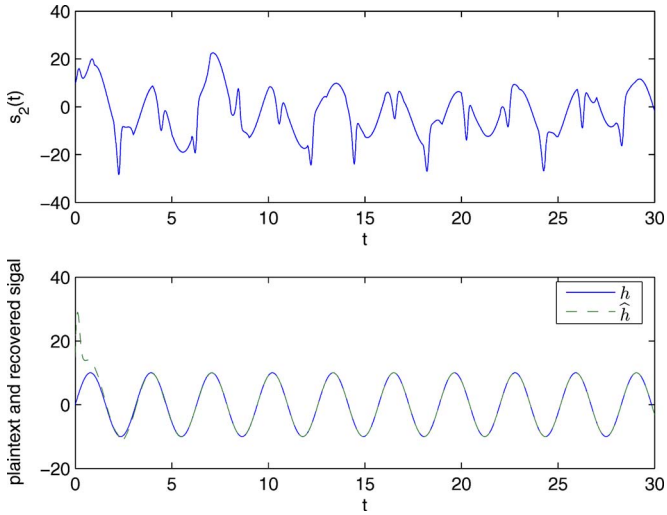

FIG. 19. (Color online) States of the transmitted signal $s_2(t)$ and the recovered signal $\hat{h}(t)$ where the plaintext is $h(t)=10\sin(2t)$.

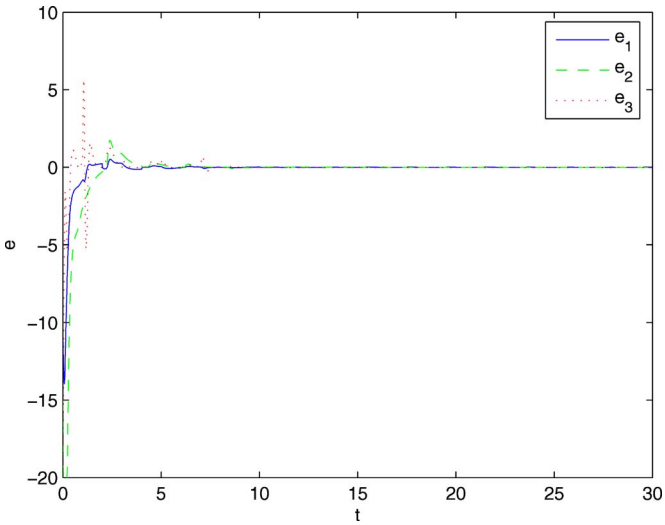

FIG. 17. (Color online) Error states of the drive system (19) and the response system (20).

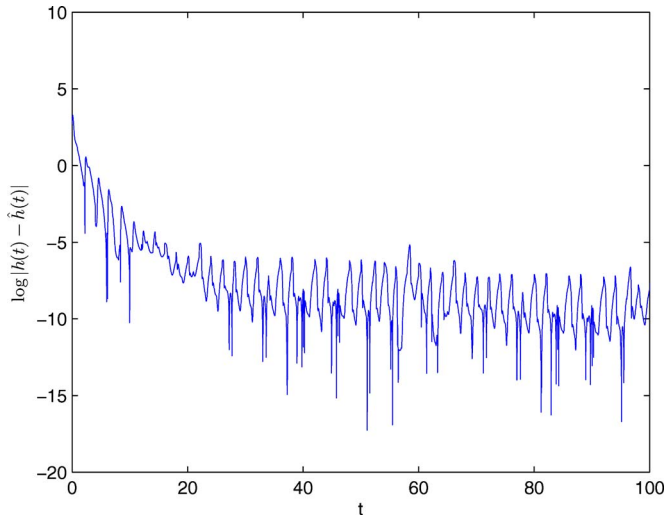

FIG. 20. (Color online) The variation of $\log|h(t)-\hat{h}(t)|$ with the time scale t where $h(t)=10\sin(2t)$.

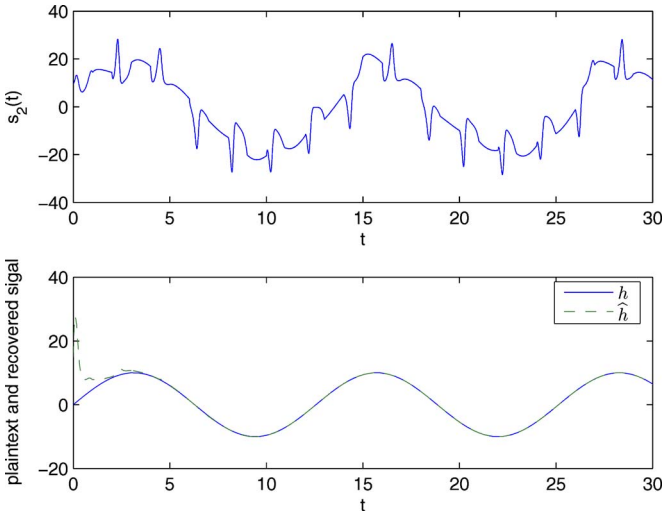

FIG. 21. (Color online) States of the transmitted signal $s_2(t)$ and the recovered signal $\hat{h}(t)$ where the plaintext is $h(t)=10\sin(t/2)$.

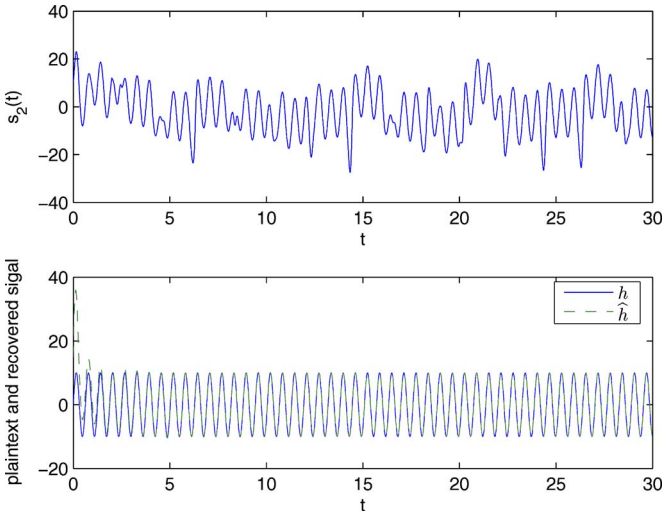

FIG. 23. (Color online) States of the transmitted signal $s_2(t)$ and the recovered signal $\hat{h}(t)$ where the plaintext is $h(t)=10\sin(10t)$.

ered signal, and the error between the original information signal and the recovered one for three different information signal $h(t)=10\sin(2t)$, $h(t)=10\sin(t/2)$, and $h(t)=10\sin(10t)$, respectively. In Fig. 20, when $h(t)=10\sin(2t)$, one can find that the information signal $h(t)$ is recovered after $t\approx 31$ with fluctuation for mismatch $|h(t)-\hat{h}(t)|\leqslant 2^{-6}$. In Fig. 22, when $h(t)=10\sin(t/2)$, it is found out that the signal $h(t)$ is recovered after $t\approx 23$ with fluctuation for mismatch $|h(t)-\hat{h}(t)|\leqslant 2^{-6}$. As for $h(t)=10\sin(10t)$, it is easy to find that the signal $\hat{h}(t)$ is recovered after $t\approx 19$ with fluctuation for smaller mismatch $|h(t)-\hat{h}(t)|\leqslant 2^{-7}$ from Fig. 24. Thus the conclusion can be drawn that the recovered signals almost have the same accuracy for the information signals with different frequencies. As for the time required for recovering the signal, if the frequency of the information signal is less or more than $\frac{1}{\pi}$ Hz, the time used to recover the signal is shorter than the time when the frequency of the information signal is equal to $\frac{1}{\pi}$ Hz.

3. Chaotic shift key

In this subsection, the plaintext message is modulated into different parameters of the chaotic switching system as time varies. Consider the drive system (26) with $(a,b,f,n,l)=(10,28,8,0.2,5.7)$, $\omega=1$, and $\beta(t)=[1+\sin(t)]/2$. The binary signal $h(t)$ shown in Fig. 27 is modulated into the system parameter c or m as time varies. The response system is Eq. (27) with adaptive laws (9). The error states between the drive system (26) and receiver system (27) are shown in Fig. 25. Furthermore, the adaptive functions $\hat{a}$, $\hat{b}$, $\hat{f}$, $\hat{n}$, and $\hat{l}$ in receiver system (27) are illustrated in Fig. 26. The transmitted message $h(t)$ can be recovered by $\hat{h}(t)=g(t)\hat{c}(t)+[1-g(t)]\hat{m}(t)$, and they are depicted in Fig. 27.

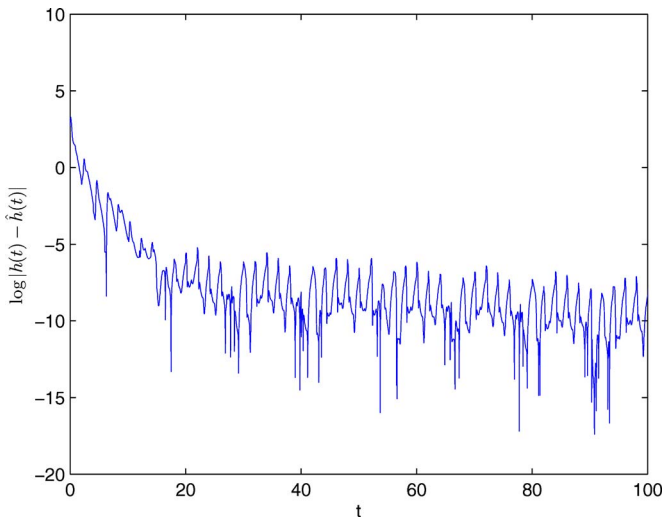

FIG. 22. (Color online) The variation of $\log|h(t)-\hat{h}(t)|$ with the time scale t where $h(t)=10\sin(t/2)$.

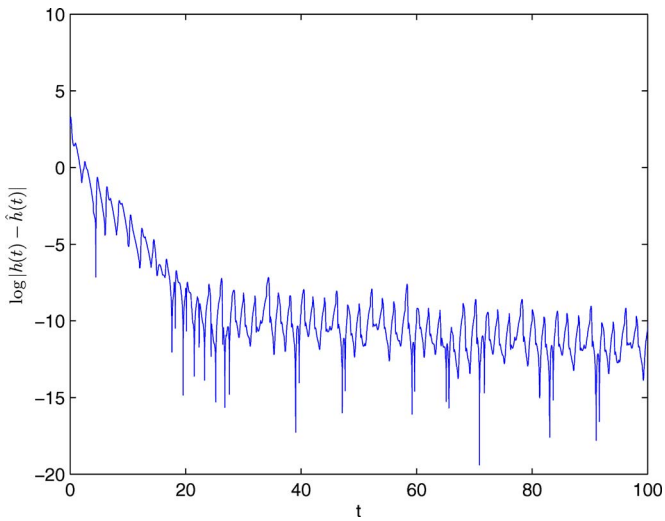

FIG. 24. (Color online) The variation of $\log|h(t)-\hat{h}(t)|$ with the time scale t where $h(t)=10\sin(10t)$.

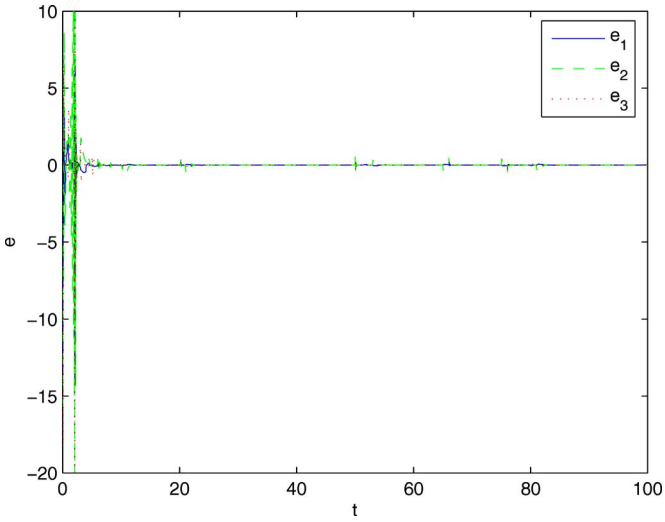

FIG. 25. (Color online) Error states of the drive system (26) and the response system (27).

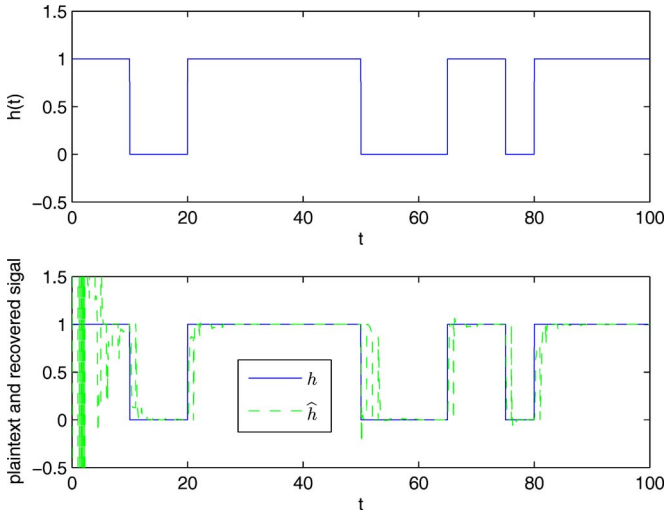

FIG. 27. (Color online) States of the binary signal $h(t)$ and the recovered signal $\hat{h}(t)=g(t)\hat{c}(t)+[1-g(t)]\hat{m}(t)$, since $h(t)$ is modulated into c when $g(t)=1$, and $h(t)$ is modulated into m when $g(t)=0$.

In addition, the signal can be modulated into several parameters of the switching system. Consider the following drive system:

$$\begin{aligned}
\dot{x}_d &= g(t)\{[25\beta(t)+a](y_d-x_d)\}+[1-g(t)][-y_d-z_d],\\
\dot{y}_d &= g(t)\{[b-35\beta(t)]x_d-x_dz_d+\}29\beta(t)\\
&\quad -\frac{h(t)}{3}y_d+[1-g(t)]\left[x_d+\frac{h(t)}{3}y_d\right], \qquad (43)\\
\dot{z}_d &= g(t)\left[x_dy_d-\frac{\beta(t)+\frac{h(t)}{3}}{3}z_d\right]\\
&\quad +[1-g(t)][n+z_d(x_d-l)],
\end{aligned}$$

where $(a,b,n,l)=(10,28,0.2,5.7)$, $\omega=1$, and $\beta(t)=[1+\sin(t)]/2$. The useful information distributes in three parameters c, m, and f of the system. The response system is Eq. (7) with adaptive laws (9). Thus the transmitted message $h(t)$ can be recovered by $\hat{h}(t)=\hat{c}(t)+\hat{f}(t)+\hat{m}(t)$, and they are illustrated in Fig. 28, respectively. One can also use two parameters to modulate the signal. For example, when the signal is modulated into c and f with $(a,b,m,n,l)=(10,28,0.2,0.2,5.7)$, the binary signal $h(t)$ and the recovered signal $\hat{h}(t)=\hat{c}(t)+\hat{f}(t)$ are shown in Fig. 29, from which one can find that the modulated signal would almost be recovered precisely when $t>10$. Figure 30 displays the case when f and m are used to modulate the signal with $(a,b,c,n,l)=(10,28,1,0.2,5.7)$. In fact, the parameters c, f, m, n, and l all could be used to modulate the signal. Thus, a wide choice range of the parameters enhances the security of this communication scheme.

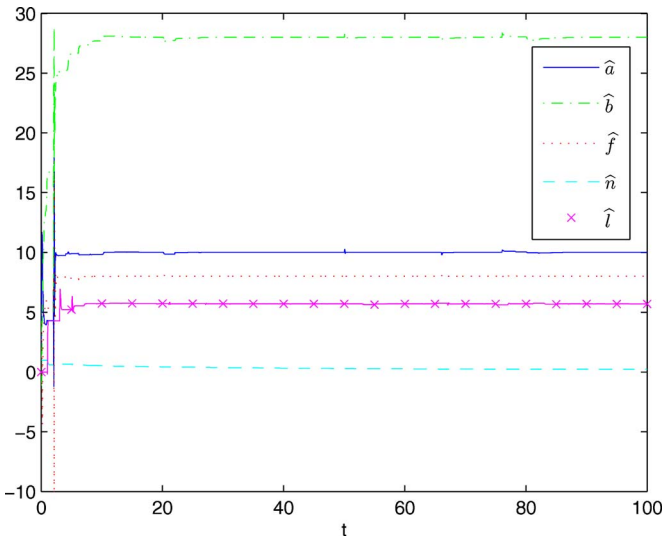

FIG. 26. (Color online) States of functions $\hat{a}(t)$, $\hat{b}(t)$, $\hat{f}(t)$, $\hat{n}(t)$, and $\hat{l}(t)$ in the response system (27).

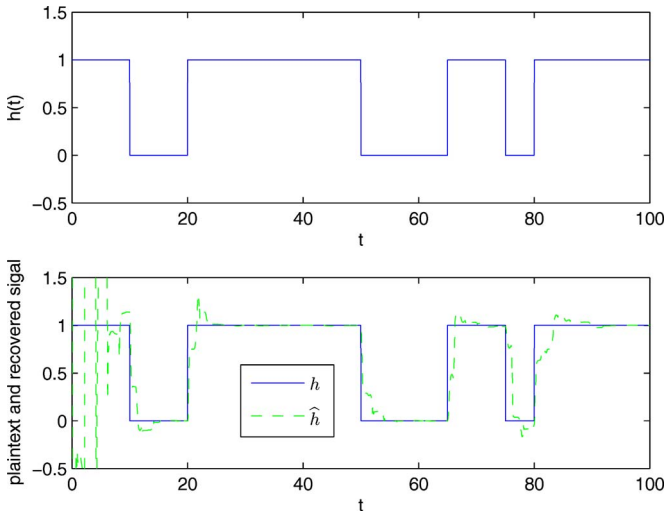

FIG. 28. (Color online) States of the binary signal $h(t)$ and the recovered signal $\hat{h}(t)=\hat{c}(t)+\hat{f}(t)+\hat{m}(t)$ since the binary signal is modulated into c, f, and m as shown in Eqs. (43).

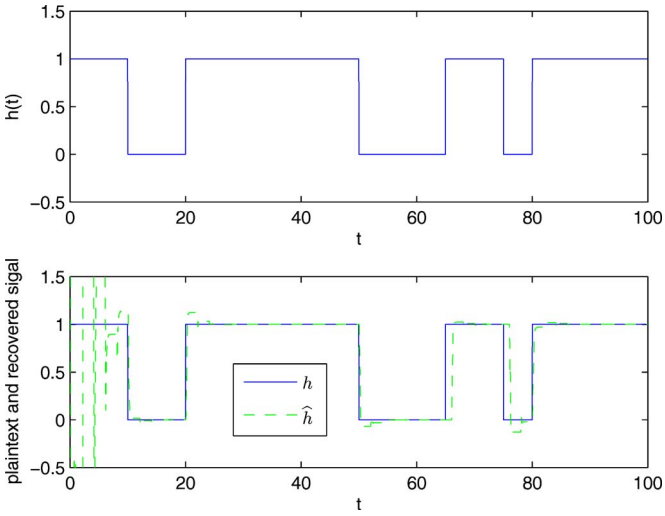

FIG. 29. (Color online) States of the binary signal $h(t)$ and the recovered signal $\hat{h}(t)=\hat{c}(t)+\hat{f}(t)$ as the binary signal is modulated into c and f.

B. Another two communication schemes

In this section, the unified system (2) is used as a transmitter. The chaotic signal used to mask or modulate the plaintext message is switching between two components of the unified system.

1. Switch scheme based on chaotic masking

Consider the drive system (29) with parameters $(a,b,c,f)=(9,28,2,7)$, $\omega=6$, and $\beta(t)=0.9[1+\sin(t)]/29$. The plaintext is $h(t)=10\sin(2t)$. The response system is (30) with adaptive laws (31). If we use the transmitted signal $s_2(t)=h(t)+g(t)z_d+[1-g(t)]y_d$, then the plaintext $h(t)$ can be recovered by $\hat{h}(t)=s_2(t)-\{g(t)z_r+[1-g(t)]y_r\}$, since $y_r\to y_d$, and $z_r\to z_d$ as $t\to\infty$. The transmitted signal and the recovered signal are illustrated in Fig. 31.

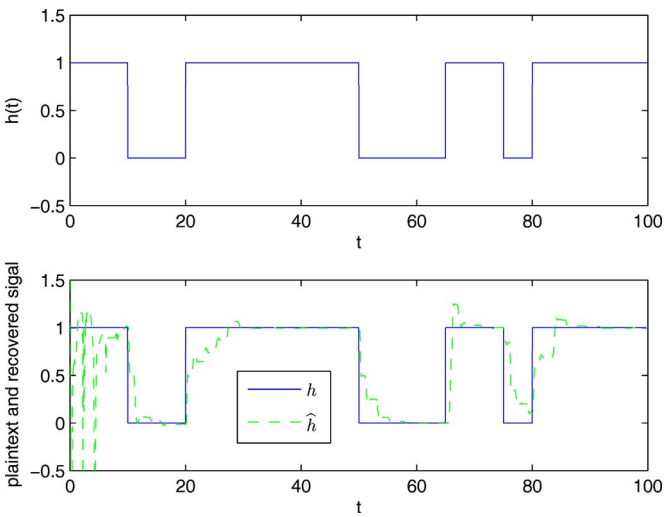

FIG. 30. (Color online) States of the binary signal $h(t)$ and the recovered signal $\hat{h}(t)=\hat{f}(t)+\hat{m}(t)$ as the binary signal is modulated into f and m.

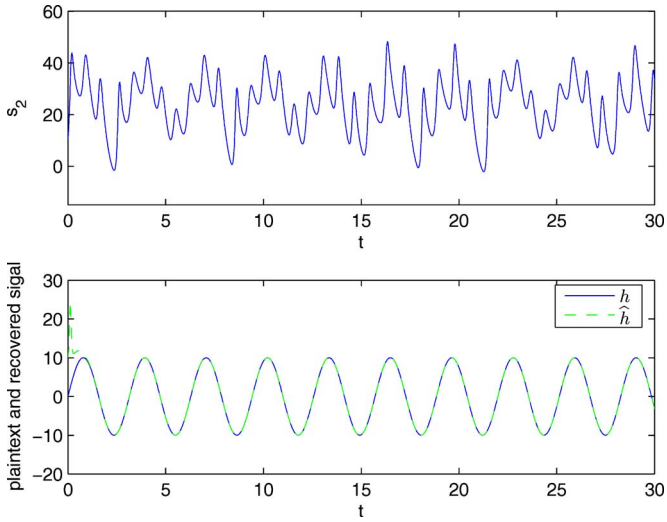

FIG. 31. (Color online) States of the transmitted signal and the recovered signal in the switch masking scheme.

2. Switch scheme based on chaotic modulation

In this example, the signal used to modulate the message switches between y_d and z_d. Consider the drive system (36) with parameters $(a,b,c,f)=(9.5,29,2,7)$, $\omega=6$, $\beta(t)=0.9[1+\sin(t)]/29$, and $h(t)=10\cos(2t)$. The response system is (37) with adaptive laws (38). If we use the transmitted signal $s_2(t)+s_3(t)=h(t)+y_d+z_d$, then the plaintext $h(t)$ can be recovered by $\hat{h}(t)=s_2(t)+s_3(t)-(y_r+z_r)$, since $y_r\to y_d$, and $z_r\to z_d$ as $t\to\infty$. The transmitted signal and the recovered signal are shown in Fig. 32.

VI. CONCLUSIONS

In this paper, a switching chaotic system which switches between the unified chaotic system and the Rössler system is proposed, and then its applications to secure communications are discussed. Different from the existing secure communication methods, the transmitted signal is modulated into a switching chaotic system instead of one chaotic system. In

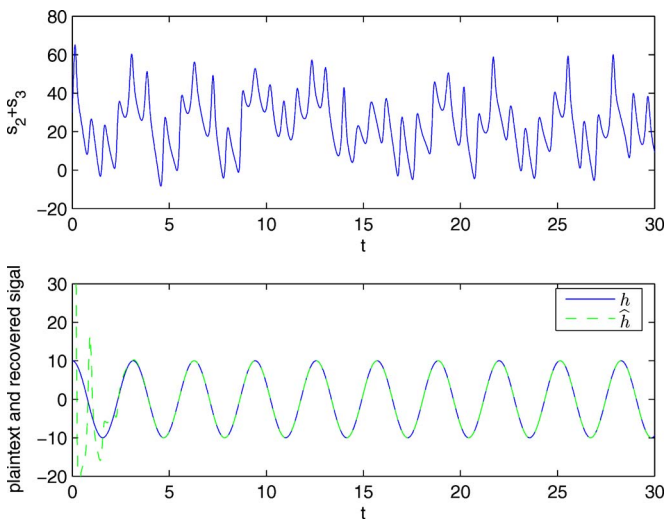

FIG. 32. (Color online) States of the transmitted signal and the recovered signal in the switch modulation scheme.

addition, the system parameters are assumed to be unknown. Furthermore, two new communication schemes in which the transmitted signal is masked by (or modulated into) a chaotic signal which switches between two components of the unified system are also proposed. Using the Lyapunov stability theory and adaptive control method, the receiver system will achieve synchronization with the drive system. Thus the message can be recovered successfully by the receiver. Numerical results have verified the effectiveness of the proposed methods.

ACKNOWLEDGMENTS

The authors thank the referees and the editor for their valuable comments and suggestions. This work was jointly supported by the National Natural Science Foundation of China under Grant No. 60574043, the Specialized Research Fund for the Doctoral Program of Higher Education under Grant No. 20070286003, and the Natural Science Foundation of Jiangsu Province of China under Grant No. BK2006093.

[1]E. N. Lorenz, "Deterministic nonperiodic flow," J. Atmos. Sci. **20**, 130–141 (1963).
[2]O. E. Rössler, "An equation for hyperchaos," Phys. Lett. **71A**, 155–157 (1979).
[3]G. Chen and T. Ueta, "Yet another chaotic attractor," Int. J. Bifurcation Chaos Appl. Sci. Eng. **9**, 1465–1466 (2002).
[4]J. Lü and G. Chen, "A new chaotic attractor coined," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 659–661 (2002).
[5]J. Lü, G. Chen, and S. Zhang, "Dynamical analysis of a new chaotic attractor," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 1001–1015 (2002).
[6]J. Lü, G. Chen, D. Cheng, and S. Čelikovshý, "Bridge the gap between the Lorenz system and the Chen system," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 2917–2926 (2002).
[7]L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett. **64**, 821–824 (1990).
[8]E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," Phys. Rev. Lett. **64**, 1196–1199 (1990).
[9]M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," Chaos, Solitons Fractals **18**, 141–148 (2003).
[10]X. Wu, "A new communication scheme based on adaptive synchronization," Chaos **16**, 043118 (2006).
[11]W. Yu, J. Cao, K. Wong, and J. Lü, "New communication schemes based on adaptive synchronization," Chaos **17**, 033114 (2007).
[12]H. N. Agiza and M. T. Yassen, "Synchronization of Rössler and Chen chaotic dynamical systems using active control," Phys. Lett. A **278**, 191–197 (2001).
[13]T. Liao and N. Huang, "An observer-based approach for chaotic synchronization with applications to secure communications," IEEE Trans. Circuits Syst., I: Fundam. Theory Appl. **46**, 1144–1150 (1999).
[14]J. Lu and J. Cao, "Adaptive complete synchronization of two identical or different chaotic (hyperchaotic) systems with fully unknown parameters," Chaos **15**, 043901 (2005).
[15]J. Cao and J. Lu, "Adaptive synchronization of neural networks with or without time-varying delays," Chaos **16**, 013133 (2006).
[16]G. Pérez and H. A. Cerdeira, "Extracting message masked by chaos," Phys. Rev. Lett. **74**, 1970–1973 (1995).
[17]S. Čelikovshý and G. Chen, "On a generalized Lorenz canonical form of chaotic systems," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 1789–1812 (2002).
[18]W. Yu, G. Chen, J. Cao, J. Lü, and U. Parlitz, "Parameter identification of dynamical systems from time series," Phys. Rev. E **75**, 067201 (2007).
[19]W. Yu and J. Cao, "Adaptive synchronization and lag synchronization of uncertain dynamical system with time delay based on parameter identification," Physica A **375**, 467–482 (2007).
[20]K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, "Synchronization of Lorenz based chaotic circuits with applications to communications," IEEE Trans. Circuits Syst., II: Analog Digital Signal Process. **40**, 626–633 (1993).
[21]T. Liao and S. Tsai, "Adaptive synchronization of chaotic systems and its application to secure communications," Chaos, Solitons Fractals **11**, 1387–1396 (2000).
[22]C. W. Wu and L. O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," Int. J. Bifurcation Chaos Appl. Sci. Eng. **3**, 1619–1627 (1994).
[23]H. Dedieu, M. P. Kenneddy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," IEEE Trans. Circuits Syst., II: Analog Digital Signal Process. **40**, 634–642 (1993).
[24]T. Yang, "A survey of chaotic secure communication systems," Int. J. of Computational Cognition **2**, 81–130 (2004).
[25]S. Boccaletti, A. Farini, and F. T. Arecchi, "Adaptive synchronization of chaos for secure communication," Phys. Rev. E **55**, 4979–4981 (1997).
[26]D. Liberzon and A. S. Morse, "Basic problems in stability and design of switched systems," IEEE Control Syst. Mag. **19**, 59–70 (1999).
[27]H. Huang, Y. Qu, and H. Li, "Robust stability analysis of switched Hopfield neural networks with time-varying delay under uncertainty," Phys. Lett. A **345**, 345–354 (2005).