New communication schemes based on adaptive synchronization

Wenwu Yu[a)]
Department of Mathematics, Southeast University, Nanjing 210096, China,
Department of Electrical Engineering, Columbia University, New York, New York 10027, USA,
and Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China

Jinde Cao[b)]
Department of Mathematics, Southeast University, Nanjing 210096, China

Kwok-Wo Wong[c)]
Department of Electronic Engineering, City University of Hong Kong, Hong Kong, China

Jinhu Lü[d)]
Institute of Systems Science, Academy of Mathematics and Systems Science, Chinese Academy of Sciences,
Beijing 100080, China and Department of Ecology and Evolutionary Biology,
Princeton University, Princeton, New Jersey 08544, USA

(Received 10 April 2007; accepted 9 July 2007; published online 12 September 2007)

In this paper, adaptive synchronization with unknown parameters is discussed for a unified chaotic system by using the Lyapunov method and the adaptive control approach. Some communication schemes, including chaotic masking, chaotic modulation, and chaotic shift key strategies, are then proposed based on the modified adaptive method. The transmitted signal is masked by chaotic signal or modulated into the system, which effectively blurs the constructed return map and can resist this return map attack. The driving system with unknown parameters and functions is almost completely unknown to the attackers, so it is more secure to apply this method into the communication. Finally, some simulation examples based on the proposed communication schemes and some cryptanalysis works are also given to verify the theoretical analysis in this paper. © *2007 American Institute of Physics*. [DOI: 10.1063/1.2767407]

Chaos synchronization has been intensively investigated due to its wide applications in secure communication, automatic control, artificial neural networks, chemical reactor, physics, etc. One of the most interesting applications is secure communication. Adaptive synchronization with unknown parameters of unified chaotic systems is investigated in this paper by using the Lyapunov method and adaptive control approach. Different from the previous results, the transmitted signal can be modulated into the chaotic system by using the modified adaptive synchronization method, and it cannot only be the digital signal but also an analog signal. Thus, the transmitted plaintext message can be successfully recovered by adaptive synchronization between the unified driving and response systems. Moreover, the proposed communication schemes can resist the return map attack and hence can increase the security of the communication. Finally, through simulation examples, the proposed schemes are validated.

I. INTRODUCTION

In 1963, Lorenz found the first chaotic attractor, subsequently named the Lorenz attractor, which produces the best well-known canonical chaotic attractor in a simple three-dimensional autonomous system.[1] In 1999, Chen and Ueta found another similar but nonequivalent chaotic attractor,[2] which is known as the dual of the Lorenz system. Later in 2002, Lü and Chen discovered a new chaotic attractor,[3,4] which bridges the gap between the Lorenz system and the Chen system. In 2002, a unified chaotic system, which can unify the aforementioned three chaotic systems, was introduced in Ref. 5, and in this paper some analysis about the synchronization between these unified systems is given.

Since some pioneer works proposed by Ott, Gregogi, and York[6] and by Pecora and Carroll,[7] chaos control and synchronization have received increasing attention due to its potential applications in secure communication, chemical reaction, biological systems, and so on. In Ref. 7, the authors used a new method (driving response) to control chaos synchronization between two identical systems. The signals of the driving system can be received by the response system, which tracks the transmitted signal and achieves synchronization with the driving system. Until now, there have been many kinds of control methods, such as feedback controller,[8] delayed feedback approach,[9] adaptive method,[10–17] etc., and chaos synchronization and control has become a popular topic nowadays.

Recently, the chaotic system and its synchronization for communication have received great interest.[10,18–21] Actually, some investigations about how to modulate the signals into the chaotic system were performed in Refs. 8, 18, 19, and

[a)]Electronic mail: wenwuyu@gmail.com; wy2137@columbia.edu
[b)]Electronic mail: jdcao@seu.edu.cn
[c)]Electronic mail: itkwwong@cityu.edu.hk
[d)]Electronic mail: jhlu@iss.ac.cn; jinhulu@princeton.edu

22–25 based on feedback control method. However, in a real situation, some or all of the parameters of the driving system are unknown. The uncertainties in this driving system will destroy the synchronization and hence it is more secure to use such kind of adaptive synchronization with unknown parameters for communication. Furthermore, it would be better if the parameters of the driving system are unknown to an intruder.

In this paper, new communication schemes based on the adaptive synchronization of a unified chaotic system are proposed. In the literature, many strategies have been proposed, such as chaotic masking,[26,27] chaotic shift key,[19,21,28] and chaotic modulation.[8,10,18,22,25,29–31] In Ref. 27 (1993), the authors developed a new communication scheme known as chaotic masking. The chaotic masking scheme consists of two identical chaotic systems in both the transmitter and the receiver. A chaotic signal is added to the plaintext to obtain the ciphertext, and the synchronized receiver can recover the plaintext by simply subtracting the masked chaotic signal. In 1993 as well, the authors designed another communication scheme, the chaotic shift key, to transmit a digital message signal.[28] In this scheme, the message signal, which is a digital signal, is used to switch the transmitted signal between two statistically similar chaotic attractors, which are respectively used to encode bit 0 and bit 1 of the message signal. These two attractors are generated by two chaotic systems with the same structure and different parameters. At the receiver end, the received signal is used to drive a chaotic system, which is identical to any of the two chaotic systems in the transmitter. In Ref. 30 (1994), the authors proposed a communication scheme known as chaotic modulation. In chaotic modulation, the message signal is directly modulated into the chaotic attractor in the phase space. The transmitter in chaotic modulation is switched among different trajectories of the same chaotic attractor, and the receiver is able to recover it through the inverse process. In fact, the chaotic shift key can be considered as a special case of chaotic modulation. A binary signal by switching the parameters of the systems is modulated into the systems. For more detailed information, please refer to Ref. 32.

In the recent years, adaptive synchronization with unknown parameters and its application in secure communication have already discussed in Refs. 10, 21, 29, and 33. In Ref. 10, the author proposed a new scheme by modulating transmitted signals into the system parameters, which is a pretty good idea. Nonetheless, the receiver can only work based on the assumption that the derivative of the plaintext message should be known first [Eq. (13) in Ref. 10]. It is meaningful only if the derivative of the information signal is null, and therefore it would be "secure" for communication schemes based on the shift-key technique. In Ref. 29, though the adaptive synchronization with unknown parameters is discussed, the application for secure communication used the feedback control, which is the same as in Ref. 8. In Ref. 21, only the chaotic shift key method was studied for application by using adaptive synchronization. However, in this paper, three different kinds of communication schemes, such as chaotic masking, chaotic shift key, and chaotic modulation, are all proposed by modified adaptive synchronization method.

During the same time when some communication schemes were proposed based on chaos synchronization, some cryptography and cryptanalysis work was also presented in Refs. 22, 23, 25, 34, and 35. In Ref. 35, the authors first found that an intruder, without any knowledge of the parameters of the system, may extract the message from the transmitted signal by producing a return map where the dynamics of the system is attracted to an almost one-dimensional set. Later, in Ref. 22, the authors proposed a simple modulation method to improve the security of chaos synchronization based on secure communications against return map attack, where periodic signal is used to effectively blur the constructed return map. Later, in Ref. 25, the authors successfully cryptanalyzed the method used in Ref. 22 based on the periodicity of zero-crossing points of the modulating signals. Further cryptanalysis work was investigated in Ref. 23. In this paper, it is easy to find that the proposed communication schemes can resist the return map attack. In particular, the parameters of the driving system are both unknown to the attackers and the receiver; thus, it is more secure to use such kind of communication schemes.

The rest of the paper is organized as follows. In Sec. II, the unified chaotic system is introduced for simplicity. In Sec. III, adaptive synchronization with unknown system parameters is discussed by using the Lyapunov approach and adaptive control method. Three communication schemes are then proposed based on the modified adaptive synchronization method in the following section. In Sec. V, simulation examples are constructed to verify the theoretical analysis of adaptive synchronization and its application in communication. Some cryptanalysis works are also presented to reveal that these communication schemes can resist the well-known return map attack. In Sec. VI, the conclusions are drawn.

II. THE UNITED CHAOTIC SYSTEM

In this section, we study the same unified chaotic system introduced by Lü *et al.* in Ref. 5. Consider the following unified chaotic model:

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

where $\alpha \in [0,1]$. According to Ref. 36, the linear part of system (1) provides a critical value $a_{12}a_{21}$, which classifies the chaotic systems: if $\alpha \in [0,0.8)$, then it is easy to have $a_{12}a_{21} > 0$ in system (1). Thus, system (1) belongs to the generalized Lorenz chaotic system;[1] when $\alpha = 0.8$, it belongs to the Lü system[3] since in this case $a_{12}a_{21} = 0$; when $\alpha \in (0.8,1]$, it is the generalized Chen system formulated in Refs. 36 and 37 because $a_{12}a_{21} < 0$ for this case. From the theoretical analysis in Ref. 5, system (1) is chaotic when $\alpha \in [0,1]$. When parameter α changes from 0 to 1, system (1) evolves from the Lorenz system to the Chen system. In the

following sections, we will study the adaptive synchronization of unified system (1) with unknown parameters and its application in secure communication.

III. THE ADAPTIVE SYNCHRONIZATION METHOD WITH UNKNOWN PARAMETERS

In this section, chaos synchronization of the unified system with unknown system parameters is investigated. Some new communication schemes are then proposed in the next section based on the adaptive synchronization.

Consider the following unified chaotic driving system,

$$\begin{aligned}\dot{x}_d &= [25\beta(t)+a](y_d - x_d),\\ \dot{y}_d &= [b-35\beta(t)]x_d - x_d z_d + [29\beta(t)-c]y_d,\\ \dot{z}_d &= x_d y_d - \frac{\beta(t)+f}{3} z_d,\end{aligned} \tag{2}$$

where a, b, c, and f are unknown constant system parameters to the receiver or the response system. Here, $\beta(t) \in [0,1]$. The response system is

$$\begin{aligned}\dot{x}_r &= [25\beta(t)+\hat{a}(t)](y_r - x_r) + u_1,\\ \dot{y}_r &= [\hat{b}(t)-35\beta(t)]x_r - x_r z_r + [29\beta(t)-\hat{c}(t)]y_r + u_2,\\ \dot{z}_r &= x_r y_r - \frac{\beta(t)+\hat{f}(t)}{3} z_r + u_3,\end{aligned} \tag{3}$$

where $\hat{a}(t)$, $\hat{b}(t)$, $\hat{c}(t)$, and $\hat{f}(t)$ are functions with respect to time t, u_i $(i=1,2,3)$ are the controllers, and the subscripts d and r indicate the representation of driving system and response system, respectively. Subtracting driving system (2) from (3) yields the following error dynamical system:

$$\begin{aligned}\dot{e}_1 &= [25\beta(t)+a](e_2 - e_1) + [\hat{a}(t)-a](y_r - x_r) + u_1,\\ \dot{e}_2 &= [b-35\beta(t)]e_1 + [\hat{b}(t)-b]x_r + [29\beta(t)-c]e_2\\ &\quad - [\hat{c}(t)-c]y_r + e_1 e_3 - z_r e_1 - x_r e_3 + u_2,\\ \dot{e}_3 &= -\frac{\beta(t)+f}{3} e_3 - \frac{\hat{f}(t)-f}{3} z_r - e_1 e_2 + y_r e_1 + x_r e_2 + u_3,\end{aligned} \tag{4}$$

where $e_1 = x_r - x_d$, $e_2 = y_r - y_d$, and $e_3 = z_r - z_d$. The controllers and adaptive laws are designed by

$$\begin{aligned}&u_i = -k_i e_i, \quad \dot{k}_i = e_i^2, \quad \dot{\hat{a}} = -e_1(y_r - x_r),\\ &\dot{\hat{b}} = -e_2 x_r, \quad \dot{\hat{c}} = e_2 y_r, \quad \dot{\hat{f}} = e_3 \frac{z_r}{3},\end{aligned} \tag{5}$$

where $i=1,\ 2,\ 3$.

Choose the following Lyapunov function candidate:

$$\begin{aligned}V(e(t)) = \tfrac{1}{2}[&e_1^2 + e_2^2 + e_3^2 + (k_1 - l_1)^2 + (k_2 - l_2)^2 + (k_3 - l_3)^2\\ &+ (\hat{a}-a)^2 + (\hat{b}-b)^2 + (\hat{c}-c)^2 + (\hat{f}-f)^2],\end{aligned} \tag{6}$$

where l_1, l_2, and l_3 are positive constants. Differentiating V with respect to time along the solution of Eqs. (4) and (5), one obtains

$$\begin{aligned}\dot{V}(e(t)) &= e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + (k_1 - l_1)\dot{k}_1 + (k_2 - l_2)\dot{k}_2 + (k_3 - l_3)\dot{k}_3 + (\hat{a}-a)\dot{\hat{a}} + (\hat{b}-b)\dot{\hat{b}} + (\hat{c}-c)\dot{\hat{c}} + (\hat{f}-f)\dot{\hat{f}}\\ &= -(25\beta(t)+a)e_1^2 + [25\beta(t)+a]e_1 e_2 + [\hat{a}(t)-a]e_1(y_r - x_r) - k_1 e_1^2 + [b-35\beta(t)]e_1 e_2 + [\hat{b}(t)-b]e_2 x_r\\ &\quad + [29\beta(t)-c]e_2^2 - [\hat{c}(t)-c]e_2 y_r + e_1 e_2 e_3 - z_r e_1 e_2 - x_r e_2 e_3 - k_2 e_2^2 - \frac{\beta(t)+f}{3} e_3^2 - \frac{\hat{f}(t)-f}{3} e_3 z_r - e_1 e_2 e_3 + y_r e_1 e_3\\ &\quad + x_r e_2 e_3 - k_3 e_3^2 + (k_1 - l_1)e_1^2 + (k_2 - l_2)e_2^2 + (k_3 - l_3)e_3^2 + (\hat{a}-a)\dot{\hat{a}} + (\hat{b}-b)\dot{\hat{b}} + (\hat{c}-c)\dot{\hat{c}} + (\hat{f}-f)\dot{\hat{f}}\\ &= -[25\beta(t)+a]e_1^2 + [a+b-10\beta(t)-z_r]e_1 e_2 + [29\beta(t)-c]e_2^2 - \frac{\beta(t)+f}{3} e_3^2 + y_r e_1 e_3 - l_1 e_1^2 - l_2 e_2^2 - l_3 e_3^2\\ &\leqslant \left[-25\beta(t) - a + \frac{[a+b-10\beta(t)-z_r]^2}{2} + \frac{y_r^2}{2} - l_1\right] e_1^2 + \left[29\beta(t) - c + \frac{1}{2} - l_2\right] e_2^2 + \left[-\frac{\beta(t)+f}{3} + \frac{1}{2} - l_3\right] e_3^2.\end{aligned} \tag{7}$$

Note that $\beta(t)$, $y_r(t)$, and $z_r(t)$ are bounded. Let $l_1 = \max\{-25\beta(t) - a + [a+b-10\beta(t)-z_r]^2/2 + y_r^2/2\} + 1$, $l_2 = 30\frac{1}{2} - c$, and $l_3 = -f/3 + 1/2 + 1$. One then has

$$\dot{V}(e(t)) \leqslant -e_1^2 - e_2^2 - e_3^2. \tag{8}$$

From (8), one knows that the response system (3) synchronizes with the driving system (2).

Next, we focus mainly on how to apply the adaptive synchronization into the communication. $\beta(t)$ is a function of time t and it can be considered as a key function since the driving system exhibits very complex dynamical behaviors if $\beta(t)$ changes. When β changes from 0 to 1, the driving system evolves from the Lorenz system to the Chen system. In addition, system parameters a, b, c, and f are also known to both the attackers and the receiver. The driving system can use different a, b, c, and f each time to transmit driving signals and these signals vary distinguishably. The driving system are almost unknown to the attackers, so it is very difficult to recover the original system. Suppose $g(t)$ is a bounded function, i.e.,

$$M_1 \leqslant g(t) \leqslant M_2,$$

for all $t \in R$, where M_1 and M_2 are minimum and maximum values, respectively, of message g through time t. Using the transformation

$$\beta(t) = \frac{g(t) - M_1}{M_2 - M_1},$$

one has $\beta(t) \in [0,1]$ for all time t. Thus, each bounded function $g(t)$ could be used as the key function by the transformation.

IV. NEW COMMUNICATION SCHEMES BASED ON ADAPTIVE SYNCHRONIZATION

In this section, three new communication schemes concerning the chaotic masking, chaotic shift key, and chaotic modulation are proposed based on the modified adaptive control method.

A. Chaotic masking

In this subsection, a new communication scheme based on the chaotic masking is designed, where the components x_d and y_d are used as driving signals, and z_d is added into the plaintext message $m(t)$ for masking the signal. It will be shown that the signals x_d and y_d are enough to let the following discussed driving system synchronize with the response system. If we use the transmitted signal $s_2(t)=z_d+m(t)$, then $m(t)$ can be recovered by $\hat{m}=s_2-z_r$, since $z_r \to z_d$ as $t \to \infty$. The chaotic masking scheme is illustrated in Fig. 1.

Consider the following driving system:

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

$$\dot{y}_d = [b - 35\beta(t)]x_d - x_d z_d + [29\beta(t) - c]y_d, \tag{9}$$

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

where a, b, and c are unknown system parameters to the receiver, f is a known constant parameter, and $\beta(t) \in [0,1]$. The response system is

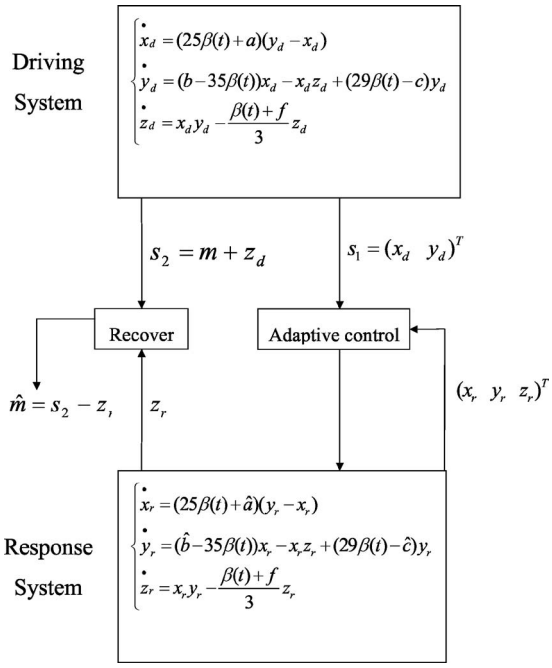

FIG. 1. Chaotic masking scheme.

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

$$\dot{y}_r = [\hat{b}(t) - 35\beta(t)]x_r - x_r z_r + [29\beta(t) - \hat{c}(t)]y_r + u_2, \tag{10}$$

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

where the notations are the same as the above section. Here, the transmitted signal is $s_1(t)=(x_d\ y_d)$, and the following controllers and adaptive laws are established:

$$\begin{aligned} &u_i = -k_i e_i, \quad u_3 = 0, \quad \dot{k}_i = e_i^2, \\ &\dot{\hat{a}} = -e_1(y_r - x_r), \quad \dot{\hat{b}} = -e_2 x_r, \quad \dot{\hat{c}} = e_2 y_r, \end{aligned} \tag{11}$$

where $i=1,\ 2$. Note that only x_d and y_d are transmitted by the driving system and (11) is independent of z_d.

Choose the following Lyapunov function candidate:

$$\begin{aligned} V(e(t)) = \tfrac{1}{2}[&e_1^2 + e_2^2 + e_3^2 + (k_1 - l_1)^2 + (k_2 - l_2)^2 + (\hat{a} - a)^2 \\ &+ (\hat{b} - b)^2 + (\hat{c} - c)^2], \end{aligned} \tag{12}$$

where l_1 and l_2 are positive constants. Differentiating V with respect to time along the solution of (9)–(11), similarly to (7), one obtains

$$\dot{V}(e(t)) = -[25\beta(t)+a]e_1^2 + [a+b-10\beta(t)-z_r]e_1e_2 + [29\beta(t)-c]e_2^2 - \frac{\beta(t)+f}{3}e_3^2 + y_re_1e_3 - l_1e_1^2 - l_2e_2^2$$
$$\leqslant \left[-25\beta(t)-a+\frac{[a+b-10\beta(t)-z_r]^2}{2} + \rho\frac{y_r^2}{2} - l_1\right]e_1^2 + \left[29\beta(t)-c+\frac{1}{2}-l_2\right]e_2^2 + \left[-\frac{\beta(t)+f}{3}+\frac{1}{2\rho}\right]e_3^2. \quad (13)$$

Choosing $f>1\geqslant\max|\beta(t)|$, sufficient large positive constants ρ, and appropriate l_i, it is easy to obtain

$$\dot{V}(e(t)) \leqslant -e_1^2 - e_2^2 - \varepsilon e_3^2, \quad (14)$$

where ε is a positive constant. From Eq. (14), one knows that the driving system (9) synchronizes with the response system (10). Thus, the plaintext message $m(t)$ would be successfully recovered.

B. Chaotic modulation

In this subsection, the transmitted signal is modulated into the chaotic system, which is still a difficult problem since the designed controllers and adaptive laws in (5) and (11) are only dependent on the states of the driving system. Assume $s(t)$ is the transmitted signal, and the object of (5) and (11) is to achieve synchronization with $s(t)$. Thus, it is very hard to recover the plaintext $m(t)$ if it is involved in the error system (4), which is modulated into the driving system. In Refs. 8, 18, 22, 23, and 25, the feedback control method is used; thus, $m(t)$ is not included in the error system after subtracting the response system from the driving system. However, the adaptive control method is not so easy. In Ref. 29, the authors studied adaptive synchronization of chaotic systems and its application to secure communications. However, a modified model is investigated when they used this adaptive method for communication application, which is just the same as the feedback control in Refs. 8, 18, 22, 23, and 25. In Ref. 21, the proposed adaptive method is only applied in the chaotic shift key approach, but not in chaotic modulation. In this subsection, we will show how to apply the modified adaptive synchronization into chaotic modulation.

Consider the following driving system:

$$\dot{x}_d = [25\beta(t)+a](y_d - x_d),$$
$$\dot{y}_d = [b-35\beta(t)]x_d - x_dz_d + [29\beta(t)-c]y_d, \quad (15)$$
$$\dot{z}_d = x_dy_d - \frac{\beta(t)+f}{3}z_d + m(t),$$

where a, b, and c are unknown system parameters to the receiver, f is a known constant parameter, $\beta(t)\in[0,1]$, and $m(t)$ is the plaintext that is modulated into the chaotic driving system. The transmitted signal is $s=[x_d\, y_d\, z_d+m(t)]$ and the response system is

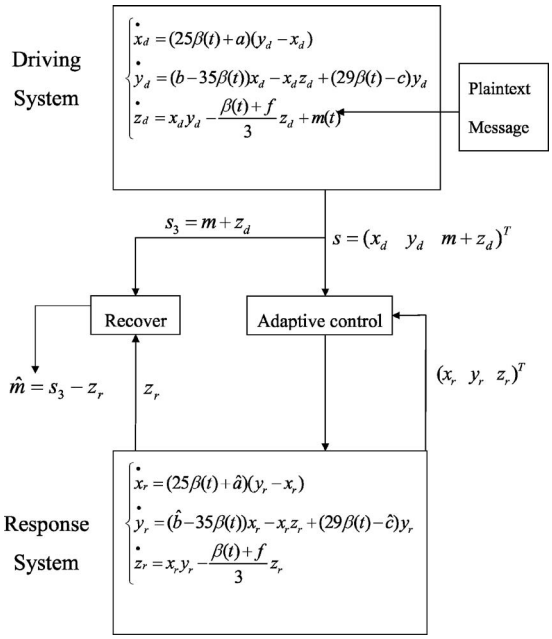

FIG. 2. Chaotic modulation scheme.

$$\dot{x}_r = [25\beta(t)+\hat{a}(t)](y_r - x_r) + u_1,$$
$$\dot{y}_r = [\hat{b}(t) - 35\beta(t)]x_r - x_rz_r + [29\beta(t) - \hat{c}(t)]y_r + u_2, \quad (16)$$
$$\dot{z}_r = x_ry_r - \frac{\beta(t)+f}{3}z_r + u_3.$$

The controllers and adaptive laws are designed by

$$u_i = -k_ie_i, \quad u_3 = -[z_r - z_d - m(t)], \quad \dot{k}_i = e_i^2,$$
$$\dot{\hat{a}} = -e_1(y_r - x_r), \quad \dot{\hat{b}} = -e_2x_r, \quad \dot{\hat{c}} = e_2y_r, \quad (17)$$

for $i=1$, 2. The chaotic modulation scheme is illustrated in Fig. 2. If the driving system (15) synchronizes with the response system (16), then the plaintext message can be recovered by $\hat{m}=s_3-z_r$ since $z_r\to z_d$ as $t\to\infty$, where $s_3=z_d+m(t)$.

Subtracting driving system (15) from (16) yields the following error dynamical system:

$$\dot{e}_1 = [25\beta(t)+a](e_2-e_1) + [\hat{a}(t)-a](y_r-x_r) - k_1e_1,$$
$$\dot{e}_2 = [b-35\beta(t)]e_1 + [\hat{b}(t)-b]x_r + [29\beta(t)-c]e_2 - [\hat{c}(t)-c]y_r + e_1e_3 - z_re_1 - x_re_3 - k_2e_2, \quad (18)$$
$$\dot{e}_3 = -\frac{\beta(t)+f}{3}e_3 - e_1e_2 + y_re_1 + x_re_2 - e_3,$$

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:

$$V(e(t)) = \tfrac{1}{2}[e_1^2+e_2^2+e_3^2+(k_1-l_1)^2+(k_2-l_2)^2+(\hat{a}-a)^2 + (\hat{b}-b)^2+(\hat{c}-c)^2], \quad (19)$$

where l_1 and l_2 are positive constants. Differentiating V with

respect to time along the solution of (17) and (18), one obtains

$$\begin{aligned}\dot{V}(e(t)) &= -[25\beta(t)+a]e_1^2+[a+b-10\beta(t)-z_r]e_1e_2\\ &\quad+[29\beta(t)-c]e_2^2-\frac{\beta(t)+f}{3}e_3^2\\ &\quad+y_re_1e_3-l_1e_1^2-l_2e_2^2-e_3^2\\ &\leqslant\left[-25\beta(t)-a+\frac{[a+b-10\beta(t)-z_r]^2}{2}\right.\\ &\quad\left.+\rho\frac{y_r^2}{2}-l_1\right]e_1^2+\left[29\beta(t)-c+\frac{1}{2}-l_2\right]e_2^2\\ &\quad+\left[-\frac{\beta(t)+f}{3}+\frac{1}{2\rho}-1\right]e_3^2. \end{aligned}\tag{20}$$

Choosing $f>\max|\beta(t)|$, sufficient large positive constants ρ, and appropriate l_i, it is easy to obtain

$$\dot{V}(e(t))\leqslant -e_1^2-e_2^2-e_3^2. \tag{21}$$

From (21), one obtains that the driving system (15) synchronizes with the response system (16). The plaintext would then be recovered by subtracting z_r from the transmitted signal $z_d+m(t)$ since $z_r\to z_d$ as $t\to\infty$. Thus, the plaintext is modulated into the chaotic driving system and is able to be recovered successfully by the receiver.

C. Chaotic shift key

In this subsection, the chaotic shift key algorithm based on the adaptive synchronization is proposed. A binary signal with switching parameters m is modulated into the driving system,

$$\begin{aligned}\dot{x}_d&=[25\beta(t)+a](y_d-x_d),\\ \dot{y}_d&=[b-35\beta(t)]x_d-x_dz_d+[29\beta(t)-m]y_d,\\ \dot{z}_d&=x_dy_d-\frac{\beta(t)+f}{3}z_d,\end{aligned}\tag{22}$$

and the response system is

$$\begin{aligned}\dot{x}_r&=[25\beta(t)+\hat{a}(t)](y_r-x_r)+u_1,\\ \dot{y}_r&=[\hat{b}(t)-35\beta(t)]x_r-x_rz_r+[29\beta(t)-\hat{c}(t)]y_r+u_2,\\ \dot{z}_r&=x_ry_r-\frac{\beta(t)+\hat{f}(t)}{3}z_r+u_3.\end{aligned}\tag{23}$$

If m is a constant, one can easily obtain that the driving system (22) synchronizes with the response system (23) by using the adaptive controllers (5) based on the discussion in Sec. III. Actually, the adaptive synchronization method proposed in previous works[14,15,17] can precisely estimate the unknown constant of the driving system parameter as shown in Fig. 3, then one can expect that it can also estimate slow varying varies such that $\dot{m}\approx 0$ or piecewise constant such that $\dot{m}=0$ everywhere except at some discrete instants of time. In Ref. 17, synchronization based parameter identification of dynamical systems from time series is carefully revisited. A linear independence condition is pointed out, which is sufficient for such parameter identification of general dynamical systems. Therefore, if the parameter m of the driving system varies according to the level of a digital information signal, the response system can estimate these variations and hence demodulates the transmitted signal.

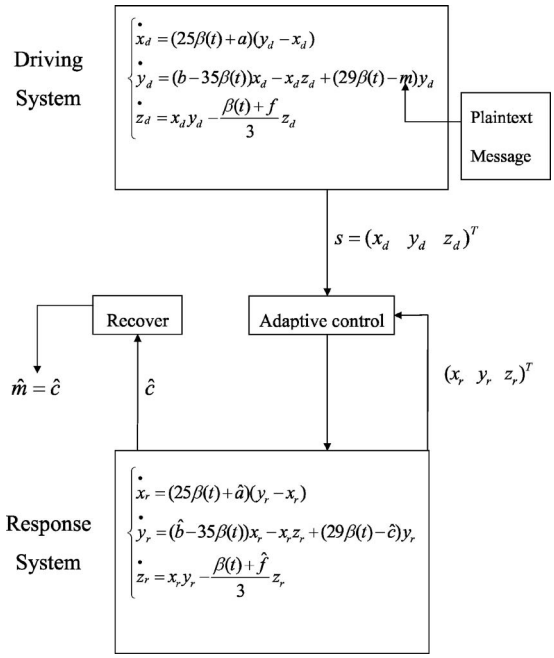

FIG. 3. Chaotic shift key scheme.

Remark. In this section, three chaotic communication schemes are investigated based on the adaptive synchronization with unknown parameters, which is still a difficult problem now. Comparing to the previous results, this work has some advantages. First, given two components x_d and y_d, the response system can synchronize with the driving system with unknown parameters as in the first subsection. Second, the plaintext $m(t)$ is modulated into the driving system, which is different from previous works.[10,21,29] In Ref. 21, only chaotic shift key method is studied, and it means that the modulated signal is a binary signal satisfying $\dot{m}=0$ everywhere except at some discrete instants of time, which is similar to Sec. III, where parameters are constants. Third, in Ref. 10, the authors proposed a communication scheme by modulating signals $m(t)$ into the parameters $\beta(t)$ of the driving system, and the unknown function $\beta(t)$ is recovered through function estimation, which is a pretty good idea. However, the derivative of $\beta(t)$ should be known *a priori*. Therefore, it is meaningful only if the derivative of the information signal is null, and it would be "secure" for communication schemes based on the shift-key technique. In this paper, chaotic modulation scheme based on adaptive synchronization is proposed.

V. NUMERICAL EXAMPLES

In this section, some simulation examples based on the adaptive method and its application in communication are investigated.

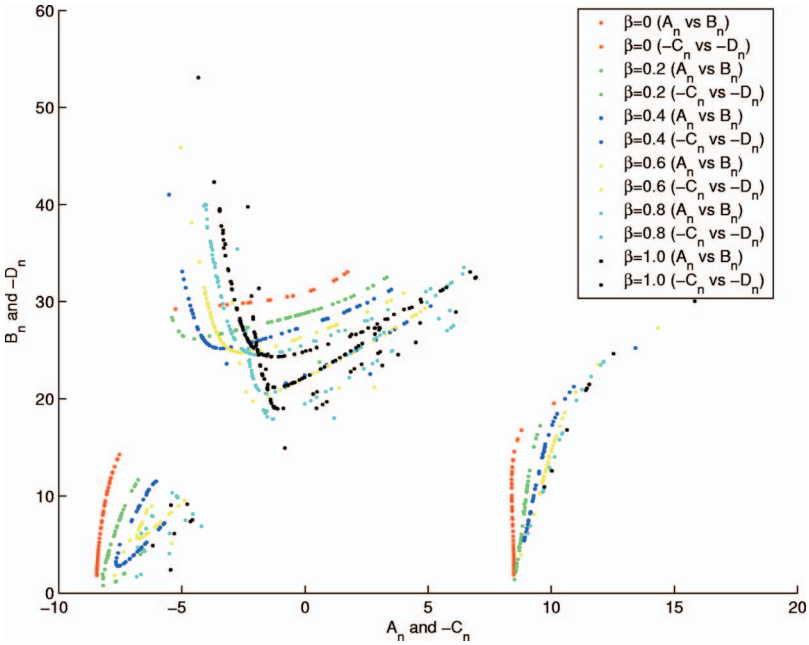

FIG. 4. (Color) Return maps of the driving system with different constant parameters.

A. Example 1: Adaptive synchronization and cryptanalysis

First, some cryptanalysis work on how this method can resist the well-known return map attack[35] is discussed. In Ref. 35, the two return maps, A_n versus B_n and $(-C_n)$ versus $(-D_n)$ are defined as follows: $A_n=(X_n+Y_n)/2$, $B_n=X_n-Y_n$, $C_n=(X_{n+1}+Y_n)/2$, and $D_n=Y_n-X_{n+1}$, where X_n and Y_n are nth local maxima and local minima of the transmitted signal, respectively. Once an attacker gets A_n versus B_n or $-C_n$ versus $-D_n$ return map, one can use the return map attack to break both chaotic masking and chaotic modulating systems.[35]

Consider the following driving system:

$$\dot{x}_d=[25\beta(t)+10](y_d-x_d),$$

$$\dot{y}_d=[28-35\beta(t)]x_d-x_dz_d+[29\beta(t)-1]y_d, \tag{24}$$

$$\dot{z}_d=x_dy_d-\frac{\beta(t)+8}{3}z_d.$$

The return maps of modulated chaotic signals x_d with different constant parameters β are illustrated in Fig. 4, which shows that the effect is a shift in the position of the segments of the attractor. Therefore, one may realize that the switching between the two parameters means also switching between two parallel splitting branches. It is very easy to track system parameter by observing the return map.

However, in this paper the function $\beta(t)$ is used instead of the constants. Here, we choose $\beta(t)=[1+\sin(5t)]/2$ with two different initial conditions; $\beta(t)=[1+\sin(6t)]/2$ and $\beta(t)=[1+\sin(7t)]/2$. The return maps of the driving system with these different functions are shown in Fig. 5. It is found out that this function $\beta(t)$ not only blur the return map generated from the chaotic carrier but also provides a hidden function that can be used as the secret key. Even the return maps of the same function $\beta(t)=[1+\sin(5t)]/2$ with different initial conditions distinguished from each other.

Furthermore, $\beta(t)$ can be a solution of the a chaotic signal. Suppose $\alpha=0.9$ and $\alpha=1$ with two different initial conditions in (1); then the chaotic signal $x(t)$ can be obtained, respectively. Consider the transformation

$$\beta(t)=\frac{x(t)-M_1}{M_2-M_1}, \tag{25}$$

where M_1 and M_2 are minimum and maximum values, respectively, of message $x(t)$ through time t. The return map of transmitted signal x_d in the driving system is shown in Fig. 6. All the maps blur and diffuse with each other; thus, to distinguish them is not so easy. Therefore, by using the function $\beta(t)$, this method can resist the well-known return map attack.

Choose $\beta(t)=[1+\sin(5t)]/2$, and consider the following driving system:

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

$$\dot{y}_d=[b-35\beta(t)]x_d-x_dz_d+[29\beta(t)-c]y_d, \tag{26}$$

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

where $a=10$, $b=28$, $c=1$, and $f=8$, which are unknown to the response system. The response system is (3) with the

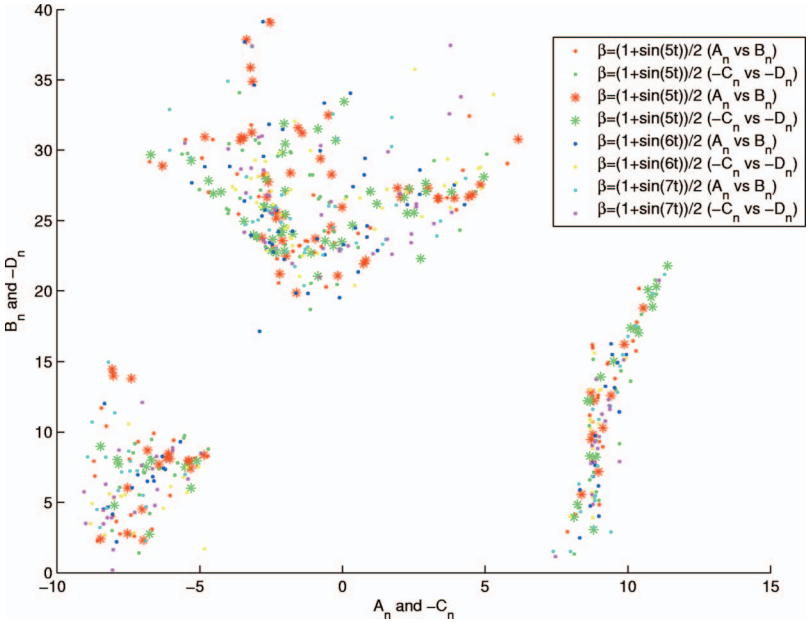

FIG. 5. (Color) Return maps of the driving system with different periodic functions.

controllers and adaptive laws as (5). The trajectories of driving system (26) are chaotic illustrated in Fig. 7 and the states of error dynamical system (4) are shown in Fig. 8. In addition, the adaptive functions $\hat{a}$, $\hat{b}$, $\hat{c}$, $\hat{f}$, and k_i in response system (5) are drawn in Figs. 9 and 10, respectively, which illustrates that the driving system (26) synchronizes with the response system (3) and (5) from Fig. 8. Furthermore, one may find that $\hat{a}$, $\hat{b}$, $\hat{c}$, and $\hat{f}$ in the response system converge to the parameters a, b, c, and f in the driving system, which means the parameters of the driving system can be estimated by the response system.

Note that the function $\beta(t)$, the parameters a, b, c, and f are all known to an intruder and the transmitter can change these parameters each time, which enhance the security of the proposed communication scheme.

B. Example 2: Chaotic masking

Next, a new chaotic masking scheme is proposed by using a simulation example. First, let $\alpha=1$ in the system (1) with a given initial condition, and use the same transformation as in (25). One can then get $\beta(t)$. Consider the following driving system:

$$\begin{aligned} \dot{x}_d &= [25\beta(t) + a](y_d - x_d), \\ \dot{y}_d &= [b - 35\beta(t)]x_d - x_d z_d + [29\beta(t) - c]y_d, \\ \dot{z}_d &= x_d y_d - \frac{\beta(t) + f}{3} z_d, \end{aligned} \tag{27}$$

where $a=9.5$, $b=27$, $c=0.9$, and $f=8$. The response system is (10) with the controllers and adaptive laws (11). The trans-

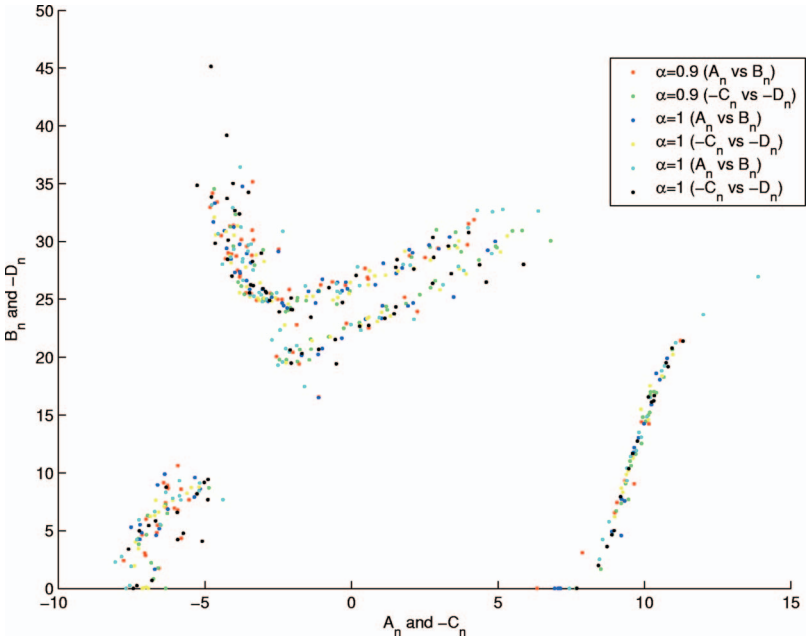

FIG. 6. (Color) Return maps of the driving system with different chaotic signals.

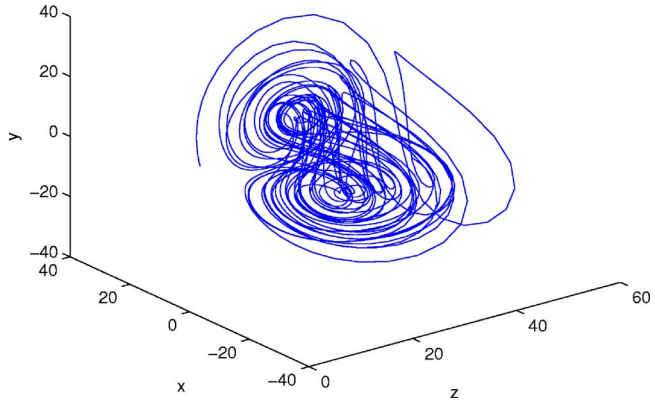

FIG. 7. (Color online) Trajectories of the driving system.

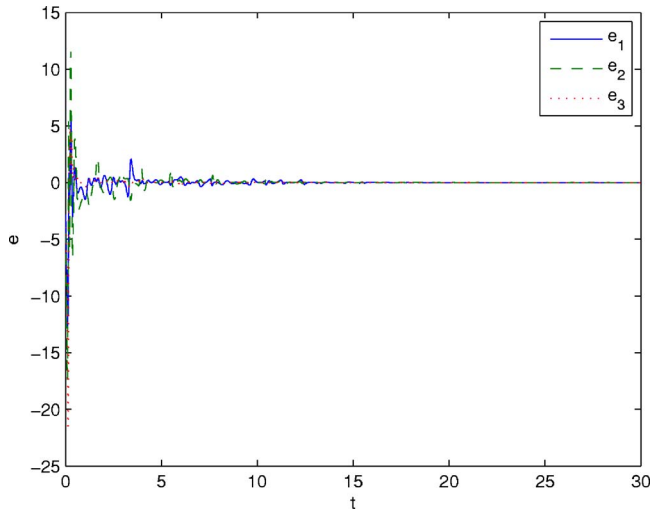

FIG. 8. (Color online) Error states of the driving system and response system.

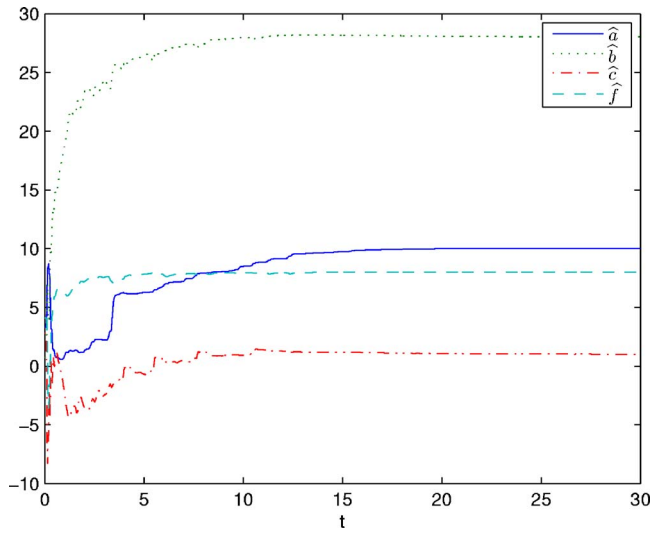

FIG. 9. (Color online) States of functions $\hat{a}(t)$, $\hat{b}(t)$, $\hat{c}(t)$, and $\hat{f}(t)$ in the response system.

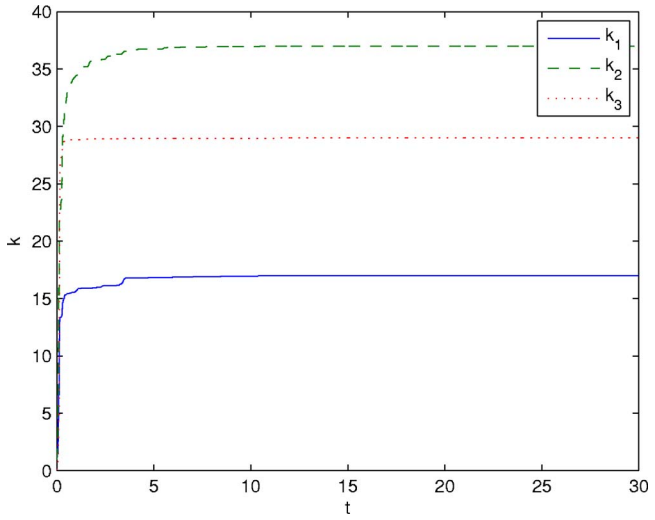

FIG. 10. (Color online) States of functions k_i in the response system.

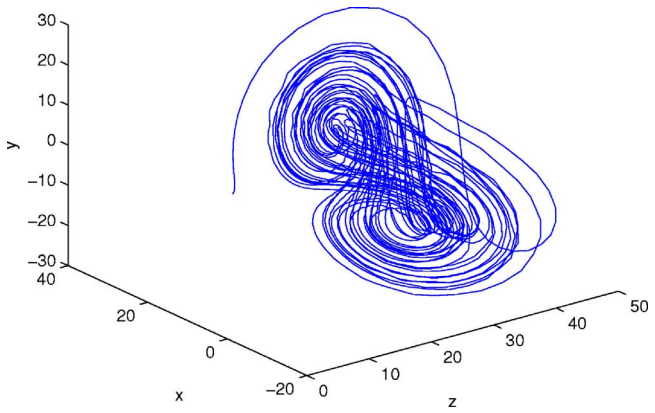

FIG. 11. (Color online) Trajectories of the driving system.

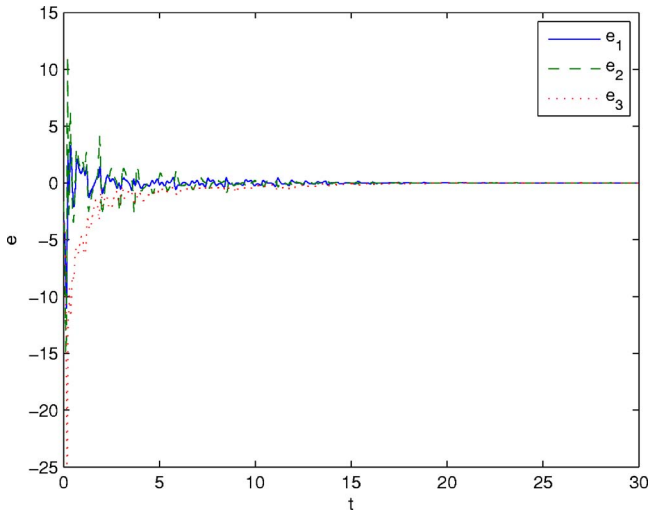

FIG. 12. (Color online) Error states of the driving system and response system.

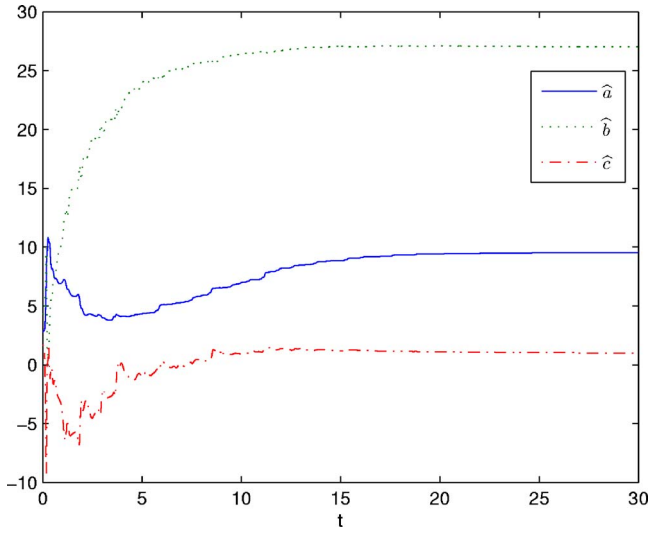

FIG. 13. (Color online) States of functions $\hat{a}(t)$, $\hat{b}(t)$, and $\hat{c}(t)$ in the response system.

mitted signal $s_1(t)=(x_d\ y_d)^T$ is used to let the driving system synchronize with the response system. The plaintext $m=10\sin(t)$ and the masking signal is $s_2(t)=m(t)+z_d$. Trajectories of the driving system, which is chaotic, are shown in Fig. 11. From Fig. 12, one obtains that the driving system (27) synchronizes with the response system (10) and (11). Furthermore, the adaptive functions $\hat{a}$, $\hat{b}$, and $\hat{c}$ in response system (11) are drawn in Fig. 13. The transmitted signal $s_2(t)$ and the recovered signal $\hat{m}(t)=s_2(t)-z_r(t)$ are illustrated in Fig. 14. It is obvious that the plaintext message $m(t)$ can be recovered by $\hat{m}$.

C. Example 3: Chaotic modulation

In this example, the transmitted signal is modulated into the driving chaotic system. First, let $\alpha=0$ in the system (1), then one can easily obtain $\beta(t)$ by using the same transformation as in (25). Consider the following driving system:

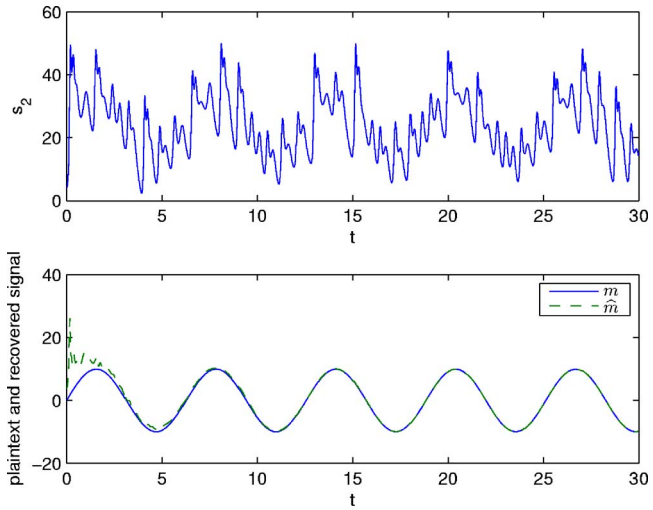

FIG. 14. (Color online) States of the transmitted signal and the recovered signal.

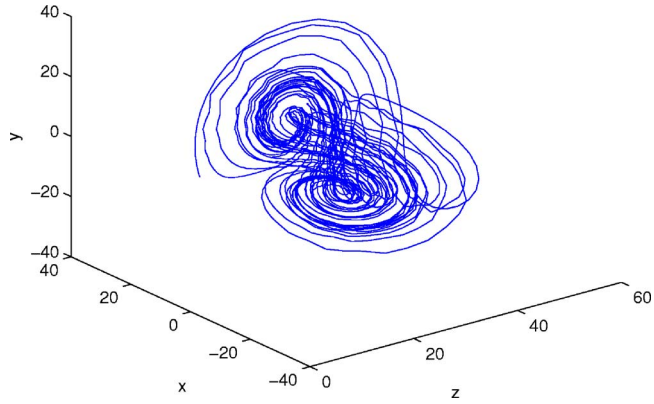

FIG. 15. (Color online) Trajectories of the driving system.

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

$$\dot{y}_d=[b-35\beta(t)]x_d-x_dz_d+[29\beta(t)-c]y_d, \tag{28}$$

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

where $a=10$, $b=28$, $c=1$, $f=8$, and $m(t)=10\cos(t)$. The response system is (16) with the controllers and adaptive laws (17). The transmitted signal $s_1(t)=[x_d\ y_d\ z_d+m(t)]^T$ is used to achieve synchronization, where $m(t)$ is the plaintext message. Trajectories of the driving system, which is chaotic, are shown in Fig. 15. From Fig. 16, one has that the driving system (28) synchronizes with the response system (16) and (17). Furthermore, the adaptive functions $\hat{a}$, $\hat{b}$, and $\hat{c}$ in response system (11) are drawn in Fig. 17. The transmitted signal $s_3(t)=z_d+m(t)$ and the recovered signal $\hat{m}(t)=s_3(t)-z_r(t)$ are illustrated in Fig. 18. It is certain that the plaintext message $m(t)$ can be recovered by $\hat{m}$, since $z_r\to z_d$ as $t\to\infty$. Moreover, the return maps of the same plaintext message $m(t)=10\cos(t)$ with different initial conditions in the driving system and a small variance $m(t)=10\cos(t)+0.01$ are shown in Fig. 19. One may easily find out that even modulating the

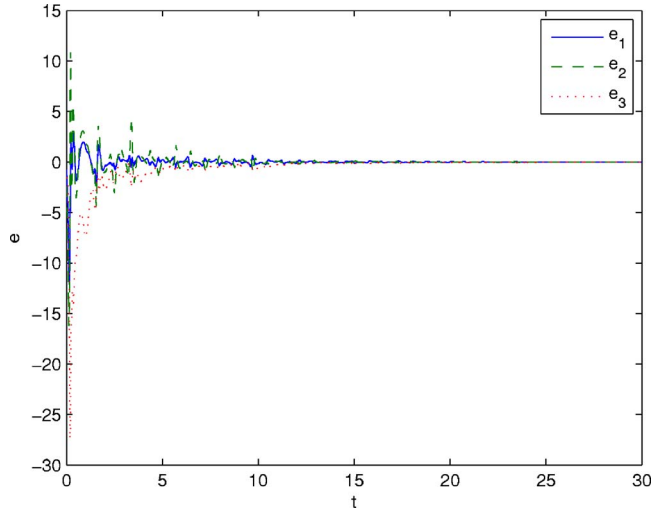

FIG. 16. (Color online) Error states of the driving system and response system.

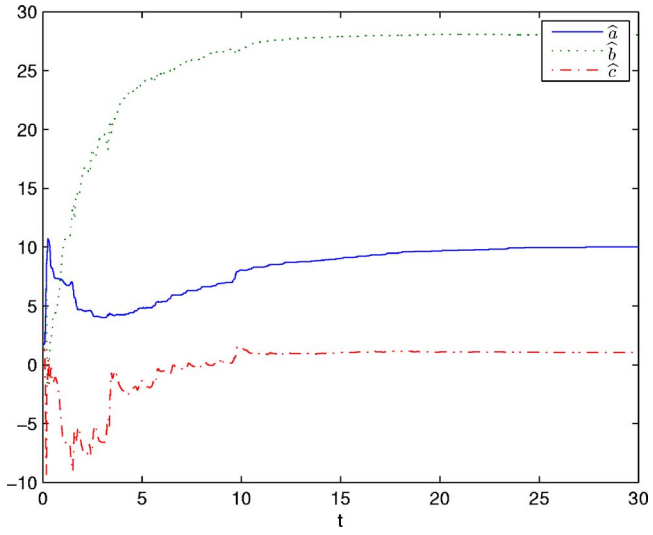

FIG. 17. (Color online) States of functions $\hat{a}(t)$, $\hat{b}(t)$, and $\hat{c}(t)$ in the response system.

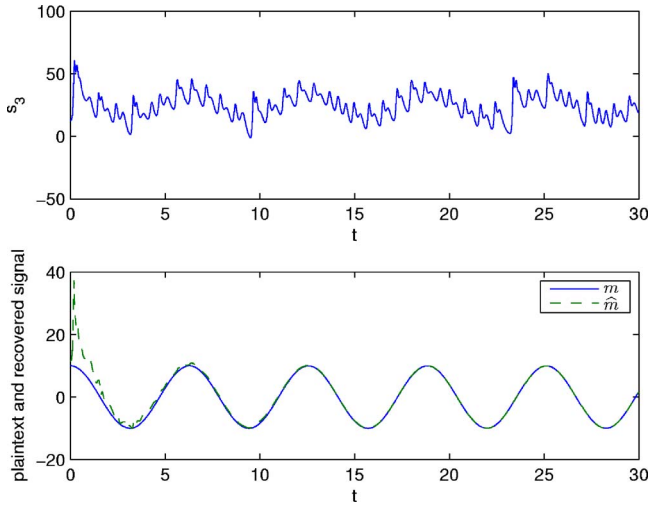

FIG. 18. (Color online) States of the transmitted signal and the recovered signal.

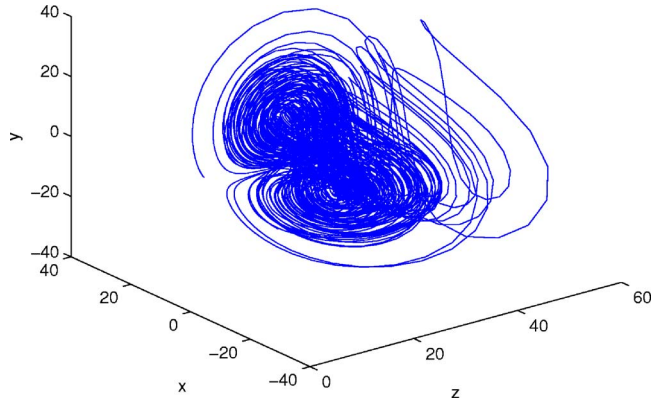

FIG. 20. (Color online) Trajectories of the driving system.

same plaintext message into the driving system with different initial conditions, the return maps are different.

D. Example 4: Chaotic shift key

From Figs. 9, 13, and 17, it is easy to see that parameters a, b, c, and f in driving system can be estimated by $\hat{a}$, $\hat{b}$, $\hat{c}$, and $\hat{f}$ in the response system. Consider the following driving system

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

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

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

where $a=9$, $b=26$, $f=8$, $\beta(t)=[(1+\sin(5t)]/2$, and m is a switching binary signal illustrated in Fig. 23. The response system is (23) with the controllers and adaptive laws (5). Trajectories of the driving system are shown in Fig. 20 which is chaotic. From Fig. 21, one obtains that the driving system (29) synchronizes with the response system (23) and (5). The

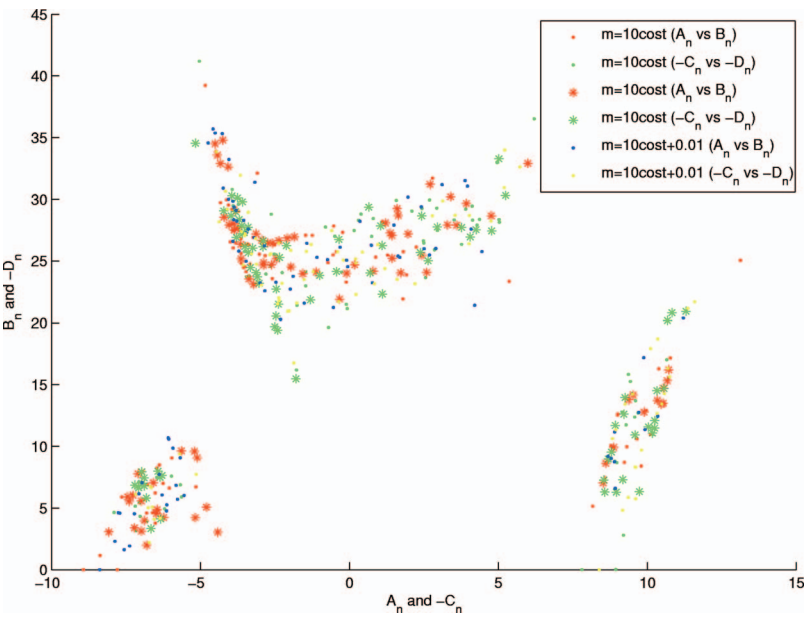

FIG. 19. (Color) Return maps of modulated chaotic signals with the same and different plaintext message.

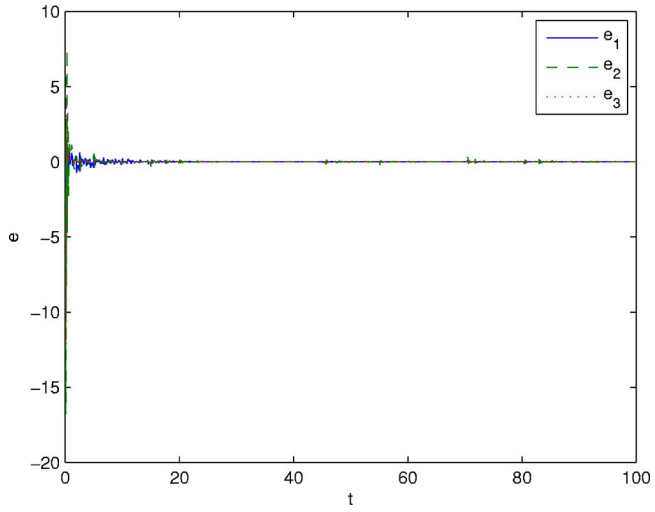

FIG. 21. (Color online) Error states of the driving system and response system.

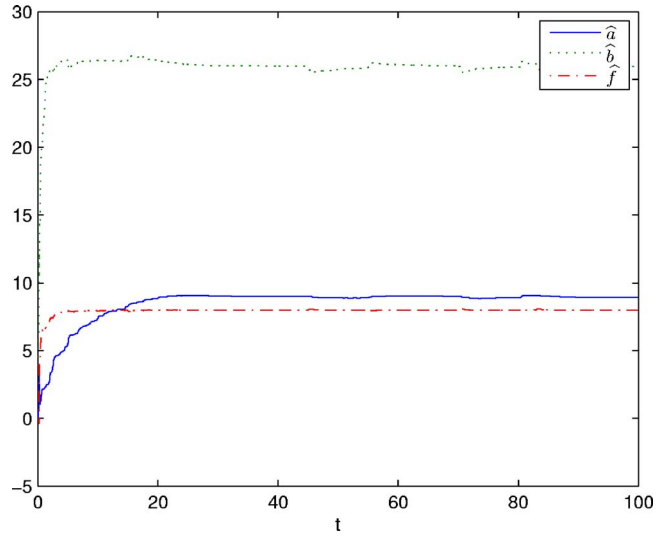

FIG. 22. (Color online) States of functions $\hat{a}(t)$, $\hat{b}(t)$, and $\hat{f}(t)$ in the response system.

adaptive functions $\hat{a}$, $\hat{b}$, and $\hat{f}$ in response system (11) are drawn in Fig. 22. The modulated signal $m(t)$ and the recovered signal $\hat{m}=\hat{c}(t)$ are illustrated in Fig. 23. Though $m(t)$ cannot be precisely recovered by $\hat{c}(t)$, much information can still be obtained. Thus, the plaintext signal would also be recovered by using the methods to filter some useless information.

In this section, simulation examples are constructed to verify the theoretical analysis in Sec. III and communication schemes in Sec. IV. In addition, some cryptanalysis based on return map are also used to attack these schemes, and in this paper we can see that this adaptive method can resist the return map attack. Thus, it is more secure to apply adaptive synchronization with unknown parameters into communication.

VI. CONCLUSION

In this paper, some new communication schemes based on adaptive synchronization with unknown parameters are proposed. Different from the existing secure communication schemes, the adaptive synchronization with unknown parameters is considered and the signal is modulated into a unified chaotic system. In addition, a function is used instead of the system parameters and hence increases the security of the proposed scheme. Actually, the system is almost unknown for the attackers, since parameters are unknown and the key function $\beta(t)$ is kept in secret. Therefore, it is pretty good to use adaptive synchronization with unknown system parameters for communication. The plaintext message can then be recovered successfully by the receiver.

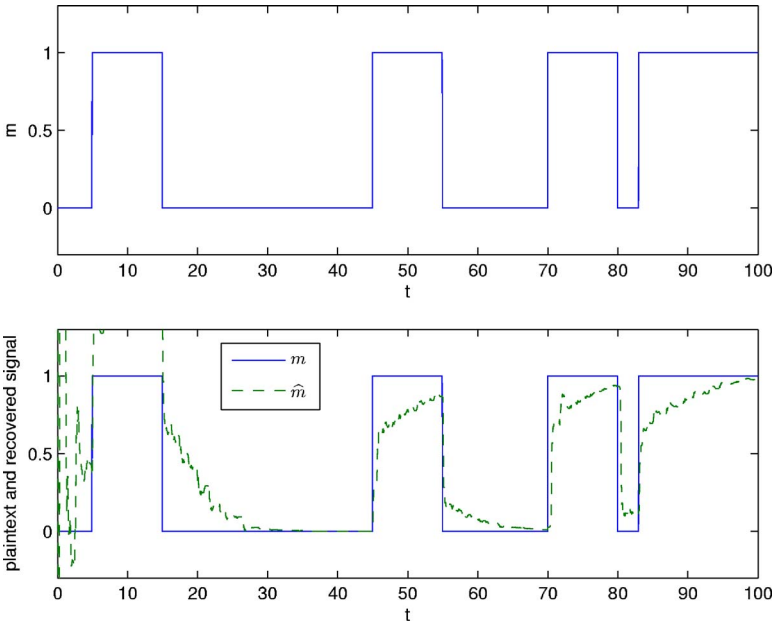

FIG. 23. (Color online) States of the transmitted signal and the recovered signal.

It is known to all that two nonidentical system can even synchronize, thus one may obviously think that it is not secure to use synchronization for secure communication. However, chaotic phenomenon is a very complex behavior, much essence of which is still not revealed, and more further work should be carried on in this topic.

ACKNOWLEDGMENT

This work was jointly supported by the 973 Program of China under Grant No. 2003CB317004, the National Natural Science Foundation of China under Grant No. 60574043, and the Natural Science Foundation of Jiangsu Province of China under Grant No. BK2006093. The authors thank Professor Guanrong Chen for helpful suggestions and Dr. Shujun Li for providing background information.

[1]E. N. Lorenz, "Deterministic nonperiodic flow," J. Atmos. Sci. **20**, 130 (1963).
[2]G. Chen and T. Ueta, "Yet another chaotic attractor," Int. J. Bifurcation Chaos Appl. Sci. Eng. **9**, 1465 (1999).
[3]J. Lü and G. Chen, "A new chaotic attractor coined," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 659 (2002).
[4]J. Lü, G. Chen, and S. Zhang, "Dynamical analysis of a new chaotic attractor," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 1001 (2002).
[5]J. Lü, G. Chen, D. Cheng, and S. Čelikovský, "Bridge the gap between the Lorenz system and the Chen system," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 2917 (2002).
[6]E. Ott, C. Grebogi, and J. A. Yorke, "Controlling chaos," Phys. Rev. Lett. **64**, 1196 (1990).
[7]L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," Phys. Rev. Lett. **64**, 821 (1990).
[8]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 (1999).
[9]W. Yu and J. Cao, "Synchronization control of stochastic delayed neural networks," Physica A **373**, 252 (2007).
[10]X. Wu, "A new chaotic communication scheme based on adaptive synchronization," Chaos **16**, 043118 (2006).
[11]W. Yu and J. Cao, "Adaptive Q-S (lag anticipated, and complete) time-varying synchronization and parameters identification of uncertain delayed neural networks," Chaos **16**, 023119 (2006).
[12]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 (2007).
[13]J. Cao and J. Lu, "Adaptive synchronization of neural networks with or without time-varying delays," Chaos **16**, 013133 (2006).
[14]D. Huang, "Adaptive-feedback control algorithm," Phys. Rev. E **73**, 066204 (2006).
[15]J. Zhou, T. Chen, and L. Xiang, "Adaptive synchronization of coupled chaotic delayed systems based on parameter identification and its applications," Int. J. Bifurcation Chaos Appl. Sci. Eng. **16**, 2923 (2006).
[16]W. Yu, J. Cao, and G. Chen, "Robust adaptive control of unknown modified Cohen-Grossberg neural networks with delay," IEEE Trans. Circuits Syst., II: Analog Digital Signal Process. **54**, 502 (2007).
[17]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).
[18]L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," Phys. Rev. Lett. **74**, 5028 (1995).
[19]K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to secure communications," Phys. Rev. Lett. **71**, 65 (1993).
[20]W. Yu and J. Cao, "Cryptography based on delayed chaotic neural networks," Phys. Lett. A **356**, 333 (2006).
[21]M. Feki, "An adaptive chaos synchronization scheme applied to secure communication," Chaos, Solitons Fractals **18**, 141 (2003).
[22]S. Bu and B. Wang, "Improving the security of chaotic encryption by using a simple modulating method," Chaos, Solitons Fractals **19**, 919 (2004).
[23]S. Li, G. Álvarez, and G. Chen, "Breaking a chaos-based secure communication scheme designed by an improved modulation method," Chaos, Solitons Fractals **25**, 109 (2005).
[24]U. Parlitz, L. Kocarev, T. Stojanovski, and H. Preckel, "Encoding messages using chaotic synchronization," Phys. Rev. E **53**, 4351 (1996).
[25]C. Chee, D. Xu, and S. Bishop, "A zero-crossing approach to uncover the mask by chaotic encryption with periodic modulation," Chaos, Solitons Fractals **21**, 1129 (2004).
[26]K. M. Cuomo and A. V. Oppenheim, "Chaotic signals and systems for communications," Proc. of International Conference on Acoustics, Speech, and Signal Processing, Minneapolis, 1993.
[27]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 (1993).
[28]H. Dedieu, M. P. Kennedy, 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 (1993).
[29]T. Liao and S. Tsai, "Adaptive synchronization of chaotic systems and its application to secure communications," Chaos, Solitons Fractals **11**, 1387 (2000).
[30]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 (1994).
[31]M. S. Baptista, S. Boccaletti, E. Allaria, R. Meucci, and F. T. Arecchi, "Controlling transient dynamics to communicate with homoclinic chaos," Chaos **13**, 921 (2003).
[32]T. Yang, "A survey of chaotic secure communication systems," Int. J. of Computational Cognition **2**, 81 (2004).
[33]S. Boccaletti, A. Farini, and F. T. Arecchi, "Adaptive synchronization of chaos for secure communication," Phys. Rev. E **55**, 4979 (1997).
[34]K. M. Short and A. T. Parker, "Unmasking a hyperchaotic communication scheme," Phys. Rev. E **58**, 1159 (1998).
[35]G. Pérez and H. A. Cerdeira, "Extracting message masked by chaos," Phys. Rev. Lett. **74**, 1970 (1995).
[36]A. Vanecek and S. Čelikovský, *Control Systems: From Linear Analysis to Synthesis of Chaos* (Prentice-Hall, London (1996).
[37]S. Čelikovský and G. Chen, "On a generalized Lorenz canonical form of chaotic systems," Int. J. Bifurcation Chaos Appl. Sci. Eng. **12**, 1789 (2002).