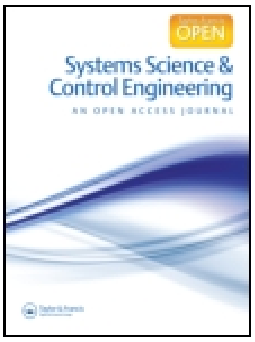

Taylor & Francis
Taylor & Francis Group

Systems Science & Control Engineering: An Open Access Journal

ISSN: (Print) 2164-2583 (Online) Journal homepage: https://www.tandfonline.com/loi/tssc20

Parameter modulation for secure communication via the synchronization of Chen hyperchaotic systems

Jianbin He & Jianping Cai

To cite this article: Jianbin He & Jianping Cai (2014) Parameter modulation for secure communication via the synchronization of Chen hyperchaotic systems, Systems Science & Control Engineering: An Open Access Journal, 2:1, 718-726, DOI: 10.1080/21642583.2013.860057

To link to this article: https://doi.org/10.1080/21642583.2013.860057

Published online: 27 Nov 2013.

Systems Science & Control Engineering: An Open Access Journal, 2014
Vol. 2, 718–726, http://dx.doi.org/10.1080/21642583.2013.860057

Parameter modulation for secure communication via the synchronization of Chen hyperchaotic systems

Jianbin He* and Jianping Cai

College of Mathematics and Statistics, Minnan Normal University, Zhangzhou, People's Republic of China

(*Received 8 September 2013; final version received 24 October 2013*)

The Chen hyperchaotic systems are synchronized via linear feedback control and the parameter is identified by using the adaptive control techniques even though the parameter is unknown. It is proved by the Lyapunov stability theory that the response system is able to track the driving system well and the parameter is estimated exactly. Based on the synchronization of Chen hyperchaotic systems, a scheme of secure communication using the parameter modulation method is presented and the transmitted plaintext message can be successfully recovered. Finally, white Gaussian noise in different kinds of signal-to-noise ratio is conducted to evaluate the performance of the proposed secure communication scheme. The return maps of the transmitted signals are provided to show the higher degree of security. Numerical simulation shows its feasibility.

Keywords: secure communication; parameter modulation; hyperchaos; adaptive control; return map

1. Introduction

Chaos is a very interesting nonlinear phenomenon because it is sensitively dependent on the initial conditions. In the past few decades, many chaotic systems have been proposed such as the Lorenz system, Chua's circuit, Chen system, and hyperchaotic system (Chen & Lü, 2002; Chen, Lu, Lü, & Yu, 2006; Lorenz, 1963; Ueta & Chen, 2000). Their complex behaviors have been widely studied, and several techniques have been used to control the chaotic system. The synchronization of chaotic system has been investigated since the pioneering work of Pecora and Carroll (1990), a series of synchronization schemes are proposed such as active–passive decomposition (Kocarev & Parlitz, 1995), linear feedback control (Tao, Xiong, & Hu, 2006), slide mode control (SMC) (Cai, Jing, & Zhang, 2010), and controllable probabilistic particle swarm optimization algorithm (Tang, Wang, & Fang, 2011). Wang, Han, Xie, & Zhang (2009) develop the chaos control problem for a general class of chaotic systems using a feedback controller to guarantee asymptotical stability of the chaotic system based on the SMC theory. The distributed synchronization of networks composed of agent systems with multiple randomly occurring nonlinearities, multiple randomly occurring controllers, and multiple randomly occurring updating laws has been achieved by Tang, Gao, Zou, and Kurths (2013) in mean square under certain criteria. The synchronization criteria and the observed phenomena are demonstrated by several numerical simulation examples and the advantage of distributed adaptive controllers over conventional adaptive controllers is illustrated.

Since 1990, the synchronization of chaotic systems has attracted much attention due to its potential applications in secure communication, analysis of chemical reactions, information processing, and so on (Arman, Kia, Naser, & Henry, 2009; Xiang, Cheng, & Liao, 2008; Xiao & Cao, 2009). The characteristics of broadband, noiselike, and unpredictability make chaotic signals ideal for information encryption or hiding in secure communication. Chaotic secure communications have been proposed, and there are many methods such as chaos masking (Cuomo, Oppenheim, & Strogatz, 1993), chaos parameter modulation (Yang & Chua, 1996), chaotic shift keying (Dedieu, Kennedy, & Hasler, 1993), and impulsive synchronization to secure communication (Yang, 2004). The key is to complete the synchronization of the slave–master systems by driving the slave with a signal derived from the master. It is easy to synchronize the master–slave systems when the parameters of the master system are known. But their parameters are usually unknown in advance, such an adaptive controller should be designed to synchronize the master–slave systems and identify the unknown parameters. Thus, the synchronization of chaotic systems in the presence of unknown parameters is more essential and useful in real-world applications (Chen, 2012). Tang represents the first attempt to include two measures of controllability into one unified framework, and the detection problem of controlling regions in cortical

*Corresponding author. Email: jbh2012yml@126.com

networks is converted into a constrained optimization problem, then the detection of controlling regions of a weighted and directed complex network is thoroughly investigated (Tang, Wang, Gao, Stephen, & Kurths, 2012). Song and Cao (2004) propose a secure communication scheme via Chua chaos using an adaptive learning mechanism that the parameters are applied to modulate the discrete message signals, but it does not make any security analysis of the proposed scheme. Based on the modified adaptive method, Yu proposes some secure communication schemes that 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 (Yu, Cao, Wong, & Lü, 2007). Li and Zhao (2011) proposed a scheme in which controllers not only realize the synchronization of the state vectors, but also synchronize the unknown response parameters to the given drive parameter as time goes to infinity; however, the update laws of the parameters are questionable. One can use the return map attack to break both chaotic masking and chaotic modulating systems. Li points out that the security of the modulation-based schemes proposed by Wu, Hu, and Zhang (2004) is not so satisfactory from a pure cryptographical point of view and the improved scheme is still insecure against a new attack (Li, Alvarez, & Chen, 2005). To overcome the security problems of most traditional chaos-based secure communication schemes, a number of new countermeasures have been proposed in recent years. One widely suggested measure is to use more complex chaotic systems rather than three-dimensional systems like the Lorenz and Chua systems (Li, Alvarez, Li, & Halang, 2007). Much different from the method above (Song & Cao, 2004; Yu et al., 2007), a fourth dimension hyperchaotic system is employed as the transmitter in this scheme. Using the high-dimension hyperchaotic systems that have multiple positive Lyapunov exponents may produce a more complex chaotic behavior to resist the return map attack. We explore the simple parameter modulation for secure communication by making use of hyperchaotic systems, and this method can resist the well-known return map attack, but note that the parameter embedded with message signals of driven system is unknown.

In the present paper, we propose an adaptive synchronization method for the Chen hyperchaotic systems with unknown parameter, and a simple parameter modulation scheme for secure communication is explored. Based on the Lyapunov stability theory, a linear feedback controller is used to synchronize the hyperchaotic systems. An adaptive update law is derived which enables the receiver to retrieve the message signals sent by the transmitter. Simulations show that synchronization is achieved asymptotically and the modulated message signals are recovered well. Finally, the robustness to noise and the security analysis of the proposed scheme are given. It is found out that the return maps generated from the chaotic carrier blur and diffuse with each other; thus, to distinguish them is not so easy.

2. Systems description and synchronization between the Chen hyperchaotic systems

2.1. Systems description

The Chen hyperchaotic system is given by

$$\begin{aligned}
\frac{\mathrm{d}x_1}{\mathrm{d}t} &= a(x_2 - x_1) + x_4,\\
\frac{\mathrm{d}x_2}{\mathrm{d}t} &= \mathrm{d}x_1 - x_1x_3 + cx_2,\\
\frac{\mathrm{d}x_3}{\mathrm{d}t} &= x_1x_2 - bx_3,\\
\frac{\mathrm{d}x_4}{\mathrm{d}t} &= x_2x_3 + rx_4, \qquad (1)
\end{aligned}$$

where $x = [x_1, x_2, x_3, x_4]$ are state variables and a, b, c, d, r are real constants. When $a = 35$, $b = 3$, $c = 12$, $d = 7$, $0 \le r \le 0.798$ system (1) is chaotic, when $a = 35$, $b = 3$, $c = 12$, $d = 7$, $0.0085 \le r \le 0.798$, system (1) is hyperchaotic, when $a = 35$, $b = 3$, $c = 12$, $d = 7$, $0.798 \le r \le 0.9$, system (1) is periodic (Li, Tang, & Chen, 2005; Park, 2005).

We found that hyperchaos does exist in the Chen system. In the numerical simulations, the parameters are always chosen as $a = 35$, $b = 3$, $c = 12$, $d = 7$, $r = 0.5$, then hyperchaotic attractors can be found.

2.2. Simple parameter modulation for secure communication

We assume that the Chen hyperchaotic system is the master system, and it can be presented in the form of

$$\begin{aligned}
\frac{\mathrm{d}x_1}{\mathrm{d}t} &= a(x_2 - x_1) + x_4,\\
\frac{\mathrm{d}x_2}{\mathrm{d}t} &= \mathrm{d}x_1 - x_1x_3 + cx_2,\\
\frac{\mathrm{d}x_3}{\mathrm{d}t} &= x_1x_2 - bx_3,\\
\frac{\mathrm{d}x_4}{\mathrm{d}t} &= x_2x_3 + rx_4,\\
\frac{\mathrm{d}r}{\mathrm{d}t} &= 0. \qquad (2)
\end{aligned}$$

The response system can be presented in the form of

$$\begin{aligned}
\frac{\mathrm{d}y_1}{\mathrm{d}t} &= a(y_2 - y_1) + y_4 - k_1e_1,\\
\frac{dy_2}{dt} &= \mathrm{d}y_1 - y_1y_3 + cy_2 - k_2e_2,\\
\frac{\mathrm{d}y_3}{\mathrm{d}t} &= y_1y_2 - by_3 - k_3e_3,\\
\frac{\mathrm{d}y_4}{\mathrm{d}t} &= y_2y_3 + \hat{r}y_4 - k_4e_4,\\
\frac{\mathrm{d}\hat{r}}{\mathrm{d}t} &= f_r, \qquad (3)
\end{aligned}$$

where $y = [y_1, y_2, y_3, y_4]$ are the response system state variables, k_1, k_2, k_3, k_4 are feedback gains, $e_1 = y_1 - x_1$, $e_2 = y_2 - x_2$, $e_3 = y_3 - x_3$, $e_4 = y_4 - x_4$, $e_r = \hat{r} - r$, and f_r is a function for learning to be determined. The parameter r is the unknown constant parameter, $\hat{r}$ is the estimated parameter in the receiver side. Subtracting Equation (2) from Equation (3) we would obtain

$$\begin{aligned}
\frac{\mathrm{d}e_1}{\mathrm{d}t} &= ae_2 - ae_1 + e_4 - k_1e_1,\\
\frac{de_2}{\mathrm{d}t} &= (d - e_3)e_1 + ce_2 - k_2e_2 - x_3e_1 - x_1e_3,\\
\frac{\mathrm{d}e_3}{\mathrm{d}t} &= x_1e_2 - be_3 - k_3e_3 + x_2e_1 + e_1e_2,\\
\frac{\mathrm{d}e_4}{\mathrm{d}t} &= x_3e_2 + \hat{r}e_4 + x_4e_r - k_4e_4 + e_2e_3 + x_2e_3,\\
\frac{\mathrm{d}\hat{r}}{\mathrm{d}t} &= f_r.
\end{aligned} \tag{4}$$

We can try to find the function f_r in Equation (4) so that the synchronization between Equations (2) and (3) is realized, then all the states of receiver will track the corresponding states in transmitter, of course, $\hat{r}$ will track r. Therefore, r can be taken as the message signal carrier, and the modulation of r will be done.

To this end, we take the Lyapunov function

$$V(e_1, e_2, e_3, e_4, e_r) = \frac{1}{2}\left(\frac{1}{\alpha}e_1^2 + e_2^2 + e_3^2 + e_4^2 + \frac{1}{\beta}e_r^2\right), \quad \alpha, \beta > 0. \tag{5}$$

Its derivative along the error dynamics (4) is

$$\begin{aligned}
\dot{V} &= \frac{1}{\alpha}e_1\dot{e}_1 + e_2\dot{e}_2 + e_3\dot{e}_3 + e_4\dot{e}_4 + \frac{1}{\beta}e_r\dot{e}_r\\
&= \frac{a}{\alpha}e_1e_2 - \frac{a}{\alpha}e_1^2 + \frac{1}{\alpha}e_1e_4 - \frac{k_1}{\alpha}e_1^2 + de_1e_2 + ce_2^2\\
&\quad - k_2e_2^2 - e_2e_1e_3 - x_3e_1e_2 - x_1e_2e_3 - be_3^2 - k_3e_3^2\\
&\quad + e_1e_2e_3 + x_1e_2e_3 + x_1e_1e_3 + x_2e_3e_4 + e_4e_2e_3\\
&\quad + \hat{r}e_4^2 + x_4e_4e_r + x_3e_2e_4 - k_4e_4^2 + \frac{1}{\beta}e_r\dot{e}_r\\
&= e_r\left(x_4e_4 + \frac{1}{\beta}\dot{e}_r\right) - \left(\frac{k_1}{\alpha} + \frac{a}{\alpha} - 3\right)e_1^2\\
&\quad - \left(k_2 - c - 2 - \frac{(a/\alpha + d - x_3)^2}{4}\right)e_2^2\\
&\quad - \left(k_3 + b - \frac{x_3^2}{4} - 1\right)e_3^2\\
&\quad - \left(k_4 - \frac{1}{4\alpha^2} - \frac{x_3^2}{4} - \frac{y_3^2}{4} - \hat{r}\right)e_4^2\\
&\quad - \left(e_1 - \frac{a/\alpha + d - x_3}{2}e_2\right)^2 - \left(e_1 - \frac{1}{2\alpha}e_4\right)^2\\
&\quad - \left(e_1 - \frac{x_1}{2}e_3\right)^2 - \left(e_2 - \frac{y_3}{2}e_4\right)^2 - \left(e_3 - \frac{x_2}{2}e_4\right)^2.
\end{aligned}$$

Obviously, if we let

$$\begin{aligned}
&\dot{e}_r = -\beta x_4e_4, \beta > 0, k_1 \geq \left(3 - \frac{a}{\alpha}\right)\alpha, k_2 \geq c + 2\\
&\quad + \frac{(a/\alpha + d - x_3)^2}{4},\\
&k_3 \geq \frac{x_2^2}{4} - b + 1, k_4 \geq \frac{1}{4\alpha^2} + \frac{y_3^2 + x_3^2}{4} + \hat{r} \quad \text{then}\\
&\dot{V} \leq -\left(e_1 - \frac{a/\alpha + d - x_3}{2}e_2\right)^2\\
&\quad - \left(e_1 - \frac{1}{2\alpha}e_4\right)^2 - \left(e_1 - \frac{x_1}{2}e_3\right)^2 - \left(e_2 - \frac{y_3}{2}e_4\right)^2\\
&\quad - \left(e_3 - \frac{x_2}{2}e_4\right)^2 < 0.
\end{aligned} \tag{6}$$

According to the Lyapunov theory, the inequality $\dot{V}(t) < 0$ indicates that $V(t)$ converges to zero and is bounded for all time, i.e. $V \in L_\infty$. The definition of $V(t)$ in Equation (5) indicates $e(t) \in L_\infty, \hat{r} \in L_\infty$. Inequalities of $\dot{V} < 0$ imply $\dot{e}(t) \in L_\infty$, it is noted that $e(t) \to 0$ as $t \to \infty$ by Babalat's lemma (Khalil, 1992). We have

$$e_1 \to 0, e_2 \to 0, e_3 \to 0, e_4 \to 0 \quad \text{as } t \to \infty.$$

That means asymptotical tracking of all states will be realized.

Meanwhile, from Equations (4) and (6), we have

$$\begin{aligned}
&\dot{e}_r = \dot{\hat{r}} - \dot{r} = -\beta x_4e_4 \quad \text{and}\\
&\dot{e}_4 = x_3e_2 + \hat{r}e_4 + x_4e_r - k_4e_4 = 0.
\end{aligned}$$

Hence $\dot{\hat{r}} = \dot{r} - \beta x_4e_4, x_4e_r = 0$, since $\dot{r} = 0$, and x_4 is not identically equal to zero. Therefore,

$$e_r \to 0.$$

Then the resulting receiver for modulating r is written as

$$\begin{aligned}
\frac{\mathrm{d}y_1}{\mathrm{d}t} &= a(y_2 - y_1) + y_4 - k_1e_1,\\
\frac{\mathrm{d}y_2}{\mathrm{d}t} &= dy_1 - y_1x_3 + cy_2 - k_2e_2,\\
\frac{\mathrm{d}y_3}{\mathrm{d}t} &= x_1y_2 - by_3 - k_3e_3,\\
\frac{\mathrm{d}y_4}{\mathrm{d}t} &= y_2x_3 + \hat{r}y_4 - k_4e_4,\\
\frac{\mathrm{d}\hat{r}}{\mathrm{d}t} &= -\beta x_4e_4.
\end{aligned} \tag{7}$$

3. Application to secure communication

In this section, the preceding adaptive law-based synchronization scheme is applied to chaotic secure communication. Figure 1 illustrates the proposed communication system consisting of a transmitter, modulation, and receiver at the receiving end of communication. At the transmitter side, the original message $m(t)$ is multiplied by a factor f and modulated by the parameter into the chaotic signals $x(t)$.

The scaling of factor f must be well chosen to reduce the message signal to a degree that it can be successfully modulated by the parameters and masked by $x(t)$.

We first use a "modulation rule" to modulate $s(t)$ in a parameter of the transmitter in Equation (2). Then an adaptive controller is used at the receiver to maintain synchronization by continuously tracking the changes in the modulation parameter. So that $s(t)$ can be recovered by this adaptive controller. In this section, we discuss the case when only a parameter of the transmitter is modulated while others remain constant.

3.1. Parameter r-modulation

In this case, the parameter r is used to modulate the signal $s(t)$, the modulation rule is given by

$$R(t) = f(s(t)) = \frac{s(t)}{d} + 0.5, \tilde{R}(t) = f^{-1}\tilde{s}(t), \qquad (8)$$

where $d = 10$ and $\tilde{s}(t)$ is the recovered message signal. We choose the transmitted message signal as follows:

$$s(t) = \frac{\sin(t)}{2} + \frac{\cos(2t)}{3}.$$

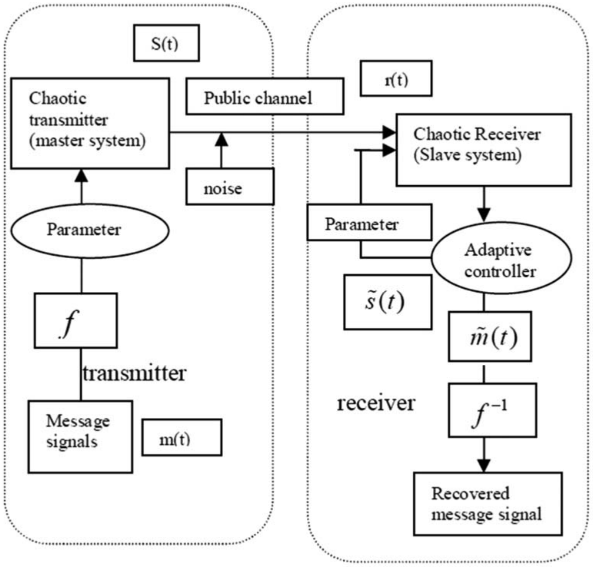

Figure 1. Secure communication systems based on parameters modulation and adaptive controller.

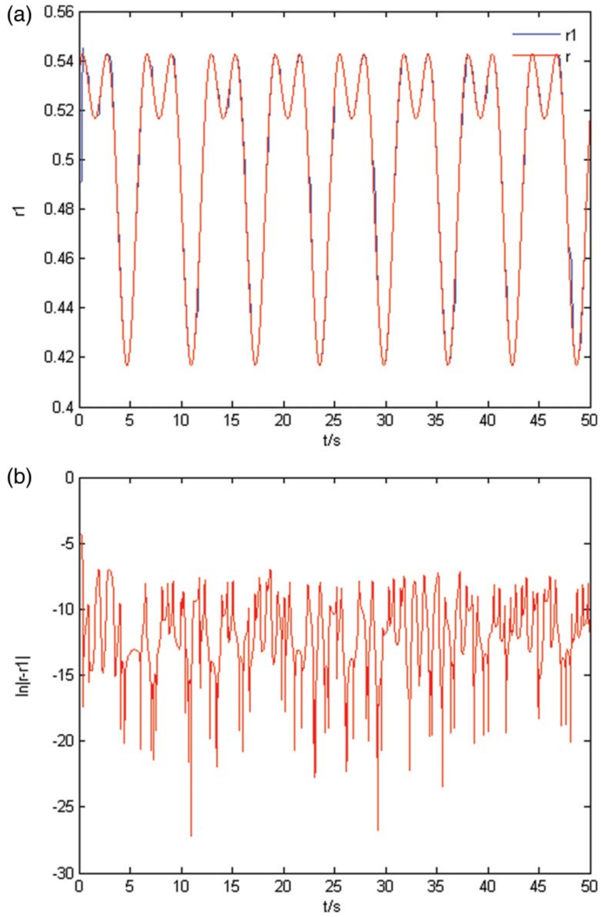

Figure 2. The estimation of unknown parameters r (a) and signal errors of $\ln|r(t) - \hat{r}(t)|$ (b).

The unknown parameters are chosen as $a = 35$, $b = 3$, $c = 12$, $d = 7$, $r = 0.5$. So the master system can exhibit a chaotic behavior. According to the rules (6), we assume $k_1 = 50$, $k_2 = 100$, $k_3 = 200$, $k_4 = 500$, $\alpha = 10$, $\beta = 100$. Simulation result is shown in Figure 2.

3.2. Security analyses

In the communication scheme, the transmitted message signals may be disturbed by random noise, attackers may retrieve the plaintext via some methods, such as return maps analysis, power-spectral (filtering) analysis, etc. So a good secure communication should resist all kinds of unknown attacks, some security analysis has been performed on the proposed secure communication scheme in this section.

3.2.1. Noise analyses

Channel noise is inevitable in secure communication. Not only is this transmission scheme accurate, but it is robust noise to some extent. Assume that the white Gaussian noise is considered in this scheme.

First, the signal-to-noise ratio (SNR) is defined as

$$dB = 10^{*} \log\left(\frac{S}{N}\right),$$

where S is the power of signal and N is the power of noise.

Then the continuous signal is taken as follows:

$$s(t) = \frac{\sin(2t)}{2} + \frac{\cos(t)}{3};$$

it is modulated by the rule in Equation (8). White Gaussian noise is added into the transmitter system as follows:

$$\begin{aligned}\frac{\mathrm{d}x_1}{\mathrm{d}t} &= a(x_2 - x_1) + x_4 + n_1(t),\\ \frac{\mathrm{d}x_2}{\mathrm{d}t} &= \mathrm{d}x_1 - x_1x_3 + cx_2 + n_2(t),\\ \frac{\mathrm{d}x_3}{\mathrm{d}t} &= x_1x_2 - bx_3 + n_3(t),\\ \frac{\mathrm{d}x_4}{\mathrm{d}t} &= x_2x_3 + rx_4 + n_4(t),\\ \frac{\mathrm{d}r}{\mathrm{d}t} &= 0,\end{aligned}$$

where $n_i(t) (i = 1, 2, 3, 4)$ are random white Gaussian noise. The transmitted message is modulated into the parameter r, so we take $n_i(t) \equiv 0 \ \ (i = 1, 2, 3)$.

When the SNR is 103.7 dB, the transmission of a continuous signal can be recovered well as shown in Figures 3 and 4. The encrypted signals are almost chaotic and difficult to be identified by the attackers.

Similarly, when the SNR is 32.91 dB, the transmission of a continuous signal can be recovered as shown in Figure 5, as it is disturbed by white Gaussian noise, we can see that the recovered signal has been blurred. There are some experimental results in Table 1 with the different kinds of SNR. In Table 1, the $|r(t) - \hat{r}(t)|$ is the errors of the recovered signals and sum $|r(t) - \hat{r}(t)|/n$ is the average value of $|r(t) - \hat{r}(t)|$. As we can see, the high SNR of the transmitted signals can be recovered much better than the low one in Table 1.

In summary, the transmitted signals may be disturbed by the unknown channel noises. Compared with the results in Table 1, the original signal can be recovered well when the SNR is higher than 65.44 dB, and the average error of the $|r(t) - \hat{r}(t)|$ is lower than 0.0020 and bounds from 1.4789e–08 to 0.0560. On the other side, if the SNR is below to 32.91 dB, the original signal can be just identified roughly and even get poor results. So the proposed secure communication scheme is robust noise to some extent.

3.2.2. *Security of Chen hyperchaotic parameter modulation*

In this digital mode secure communication, as described by Perez and Cerdeira (1995), the key to extracting message from the chaotic mask is to recognize that a small change in the parameters of the sender not only frustrates the synchronization but also affects the attractor obtained in the return map. Following Perez and Cerdeira, two modified return maps are defined by

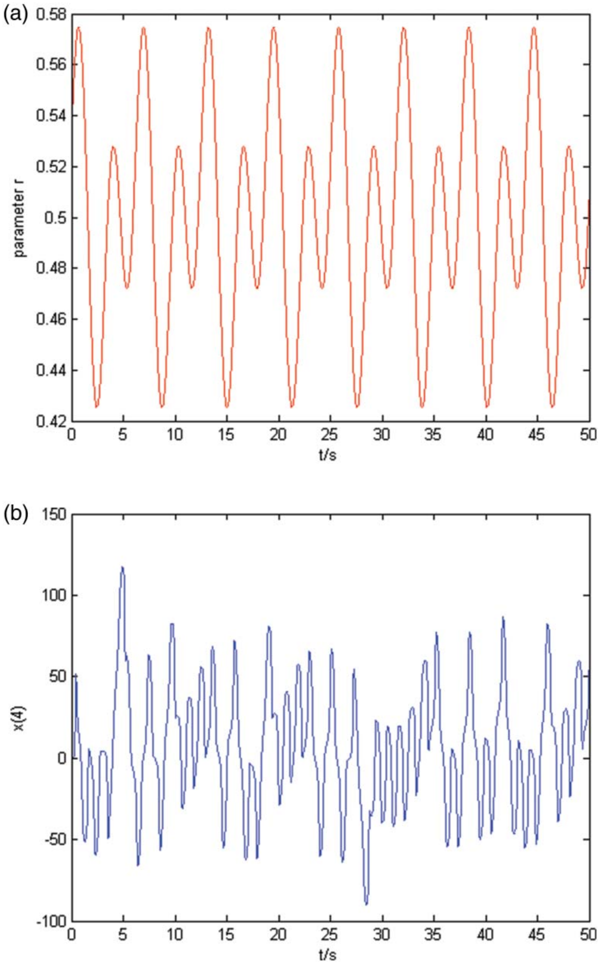

Figure 3. Original signal (a) and encrypted signal (b).

$$A_n = \frac{(X_n + Y_m)}{2}, \quad B_n = X_n - Y_m \quad \text{and}$$
$$C_n = \frac{(X_{n+1} + Y_m)}{2}, \quad D_n = X_n - Y_{m+1},$$

where X_n, Y_m denote the nth (local) maximum and mth (local) minimum of the transmitted signal, respectively.

In this paper, we choose the following parameters as the standard parameters: $a = 35, b = 3, c = 12, d = 7, r = 0.5$, and the system is hyperchaotic. First, a comparison of the return maps with a small error in the standard parameters is explored. Figure 6 shows the return maps A_n vs. B_n and $-C_n$ vs. $-D_n$ of the Chen hyperchaotic system with the standard parameters. From Figure 6(a), choose parameter $r = 0.5$ and $r = 0.5001$, and we can see that the return maps are scattered and diffused. It is sensitive to the parameter r, so the transmitted signals are difficult to be identified exactly. Then based on the proposed modulation rules in

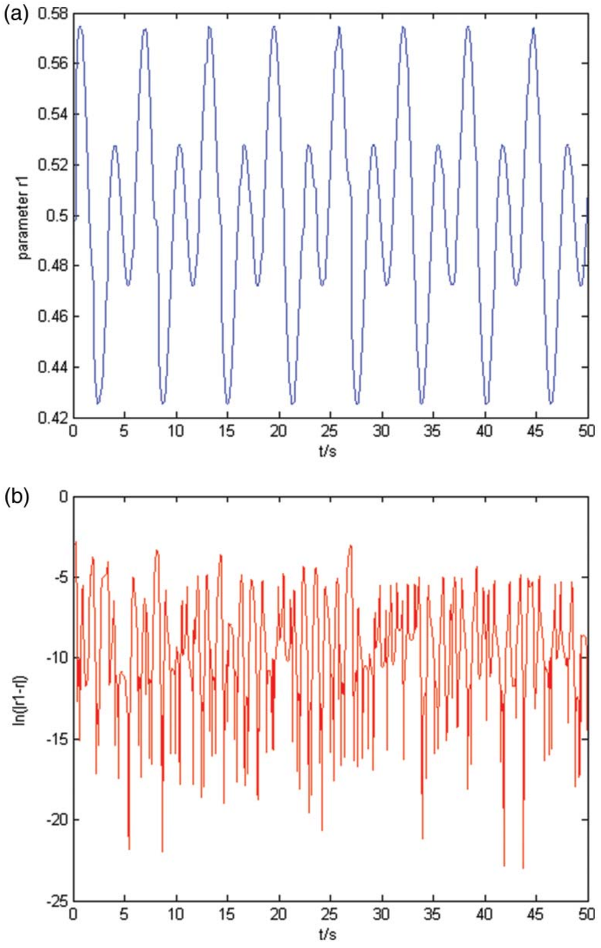

Figure 4. Recovered signal (a) and signal errors of $\ln|r(t) - \hat{r}(t)|$ (b).

Section 3.1, the return maps of the transmitted signal are shown in Figure 6(b), and it is difficult to distinguish the changes in the attractors because the two return maps are also scattered.

In many cases, only amplitude return maps are not enough to detect message signals. They also need some return maps which can reveal frequency information. Suppose that the state $X_4(t)$ is the transmitted condition. From $X_4(t)$ we can construct different kinds of return maps. Let $t_n^{\max}$ be the moment when $X_4(t)$ get its nth local maximum $X_{\max}(n)$, and $t_n^{\min}$ be the moment when $X_4(t)$ gets its nth local minimum $X_{\min}(n)$. Assume that Y_n is the value of $X_4(t)$ at that minimum moment, let $T_{\max}(n) = t_n^{\max} - t_{n-1}^{\max}$ and $T_{\min}(n) = t_n^{\min} - t_{n-1}^{\min}$ be two time intervals, then we define the following return maps (Yang, Yang, & Yang, 1998):

$$r_{\max}^A : X_{\max}(n) \mapsto X_{\max}(n+1),$$

$$r_{\min}^A : Y_{\min}(n) \mapsto Y_{\min}(n+1),$$

$$r_{\max}^T : T_{\max}(n) \mapsto X_{\max}(n),$$

$$r_{\min}^T : T_{\min}(n) \mapsto Y_{\min}(n).$$

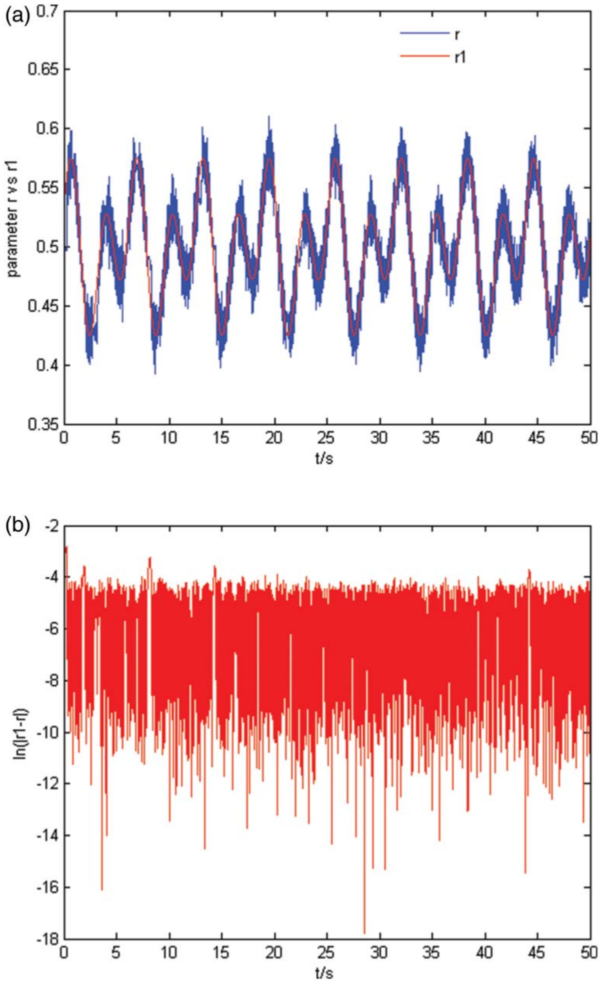

Figure 5. Recovered signal (a) and signal errors of $\ln|r(t) - \hat{r}(t)|$ (b).

Table 1. The errors of estimated parameters $\hat{r}$ with different SNR.

Case	SNR (db)	sum $\lvert r(t) - \hat{r}(t)\rvert/n$	$\lvert r(t) - \hat{r}(t)\rvert$
1	103.7	0.0017	1.1138e–09~0.0560
2	89.88	0.0018	5.0526e–09~0.0560
3	83.98	0.0018	7.6003e–09~0.0560
4	70.05	0.0017	1.3541e–08~0.0561
5	65.44	0.0020	1.4789e–08~0.0560
6	44.57	0.0032	1.5475e–09~0.0598
7	38.80	0.0048	1.3459e–07~0.0596
8	32.91	0.0085	5.8395e–07~0.0603

In Figure 7(a), the return maps with standard parameters and modulated parameters are shown. We were not able to find some shape deformations because they are scattered and the two return maps are mixed or overlapped.

Compared with others existing works, such as the works of Li, Chen, and Alvarez (2006), the return maps of the Lorenz system is given in Figure 8; note that there are three segments in the return map, and each segment is further

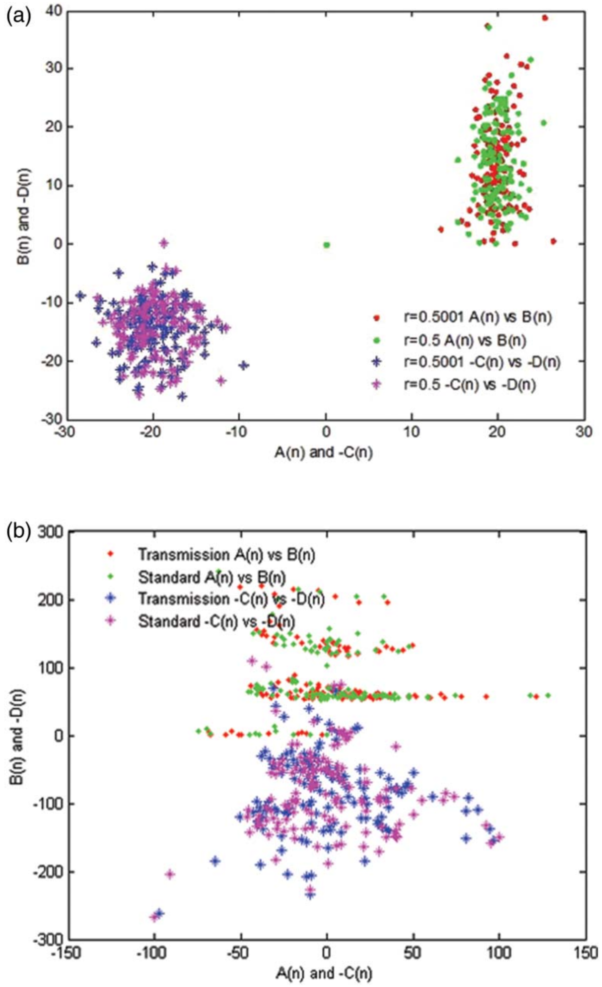

Figure 6. The return maps of the Chen hyperchaotic system with the parameter $r = 0.5$ and $r = 0.5001$ (a). The return maps ($A(n)$ and $-C(n)$ vs. $B(n)$ and $-D(n)$) of the transmitted signals with modulated parameters and standard parameters (b).

split into 10 strips. It is obvious that the split of the map is caused by the switching of the value of parameter b between $b0$ and $b1$, where $b0 = 3.1$ and $b1 = 4.0$. From Figure 6(a), however, it can be seen that the return maps of the Chen hyperchaotic system do not have a clear strip and it is scattered. In addition, it is much sensitive to the parameter r, so our scheme certainly can resist the return map attacks and the degree of security is high enough.

On the other hand, the changes of parameters not only change the sizes of the attractors but also their natural frequencies (Yang, 1995). From Figure 7(b), which shows $r^T_{\max}$ and $r^T_{\min}$, we obviously cannot find some vertical shifts between $r^T_{\max}$ and $r^T_{\min}$, which denote the changes in natural frequency. All the maps are blurred and diffused with each other; thus, distinguishing them is not easy. Therefore, by using the parameter modulation, this method can resist the well-known return map attack. This secure communication schemes whose return maps are complicated

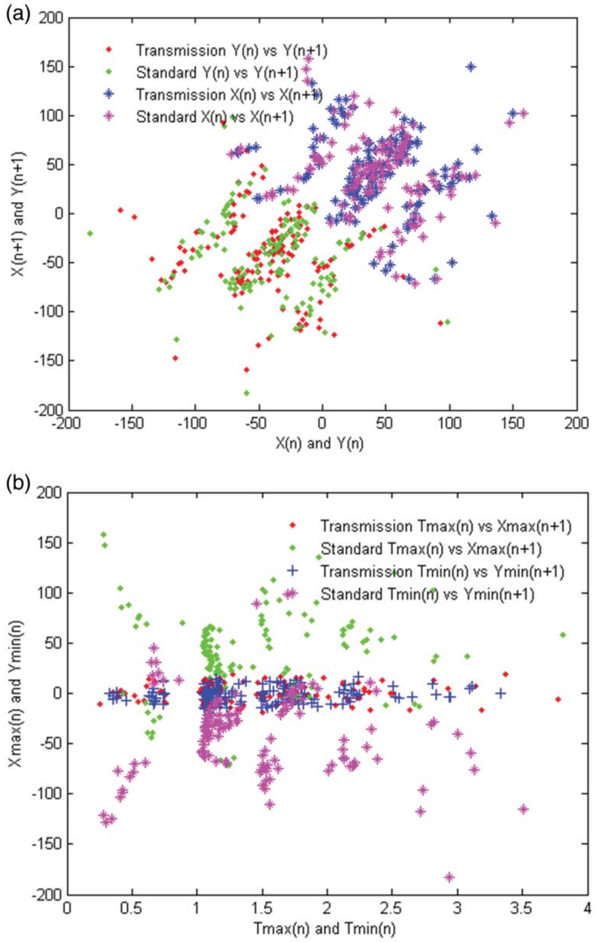

Figure 7. The return maps ($X(n)$ and $Y(n)$ vs. $X(n+1)$ and $Y(n+1)$) of the Chen hyperchaotic system with standard parameters and modulated parameters (a). The return maps ($T_{\max}(n)$ and $T_{\min}(n)$ vs. $X_{\max}(n)$ and $Y_{\min}(n)$) of $r^T_{\max}$ and $r^T_{\min}$ (b).

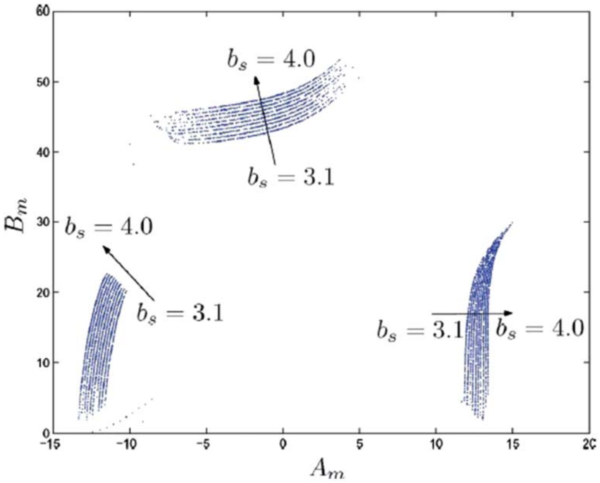

Figure 8. The return maps of the Lorenz system with different parameters.

and the changes of return maps are irregular, we know that the degree of security is high enough.

4. Conclusions

In this paper, the synchronization of Chen hyperchaotic systems with unknown parameter is presented. The parameter of transmitter can be identified exactly while the synchronization is completed. Theoretical analysis and numerical simulations are shown to verify the results. A new application with parameter modulation in the continuous signals transmission is given. We know that the continuous signals are recovered well from the simulations using the method of parameter modulation. The proposed scheme achieved robustness to noise to some extent, and different kinds of return maps show the higher degree of security. In the future, we will do more analysis and design a chaos-based system to secure communication.

Acknowledgements

The authors would like to thank the Editor and the referees for their valuable comments and suggestions that helped to improve the quality of this paper. Research is supported by the National Natural Science Foundation of China (Grant No: 61074012) and the Natural Science Foundation of Fujian Province, China (Grant No: 2011J01025).

References

Arman, K. B., Kia, F., Naser, P., & Henry, L. (2009). A chaotic secure communication scheme using fractional chaotic systems based on an extended fractional Kalman filter. *Communications in Nonlinear Science and Numerical Simulation, 14*, 863–879.

Cai, N., Jing, Y., & Zhang, S. (2010). Modified projective synchronization of chaotic systems with disturbances via active sliding mode control. *Communications in Nonlinear Science and Numerical Simulation, 15*, 1613–1620.

Chen, A. M., Lu, J. A., Lü, J. H., & Yu, S. M. (2006). Generating hyper chaotic Lü attractor via state feedback control. *Physica A: Statistical Mechanics and its Applications, 364*, 103–110.

Chen, C. J. (2012). Robust synchronization of uncertain unified chaotic systems subject to noise and its application to secure communication. *Applied Mathematics and Computation, 219*, 2698–2712.

Chen, S. H., & Lü, J. H. (2002). Synchronization of an uncertain unified chaotic system via adaptive control. *Chaos, Solitons & Fractals, 14*, 643–647.

Cuomo, K. M., Oppenheim, A. V., & Strogatz, S. H. (1993). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Transactions on Circuits and Systems II, 40*, 626–633.

Dedieu, H., Kennedy, M. P., & Hasler, M. (1993). Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Transactions on Circuits and Systems II, 40*, 634–642.

Khalil, H. K. (1992). *Nonlinear systems*. New York: Macmillan Publishing Company.

Kocarev, L., & Parlitz, U. (1995). General approach for chaotic synchronization with applications to communication. *Physical Review Letters, 74*, 5028–5031.

Li, S. J., Alvarez, G., & Chen, G. R. (2005). Breaking a chaos-based secure communication scheme designed by an improved modulation method. *Chaos, Solitons & Fractals, 25*, 109–120.

Li, S. J., Alvarez, G., Li, Z., & Halang, W. A. (2007). *Analog chaos-based secure communications and cryptanalysis: A brief survey*. Proceedings of 3rd international IEEE scientific conference on physics and control (pp. 92–98), Potsdam, Germany.

Li, S. J., Chen, G. R., & Alvarez, G. (2006). Return-map cryptanalysis revisited. *International Journal of Bifurcation and Chaos, 16*, 1557–1568.

Li, Y. X., Tang, W. K. S., & Chen, G. R. (2005). Generating hyperchaos via state feedback control. *International Journal of Bifurcation and Chaos, 15*, 3367–3375.

Li, Z. B., & Zhao, X. S. (2011). The parametric synchronization scheme of chaotic system. *Communications in Nonlinear Science and Numerical Simulation, 16*, 2936–2944.

Lorenz, E. (1963). Deterministic nonperiodic flow. *Journal of the Atmospheric Sciences, 20*, 130–141.

Park, J. H. (2005). Adapive synchronization of hyperchaotic Chen system with uncertain parameters. *Chaos, Solitons & Fractals, 26*(3), 959–964.

Pecora, L., & Carroll, T. (1990). Synchronization in chaotic systems. *Physical Review Letters, 64*, 821–824.

Perez, G., & Cerdeira, H. A. (1995). Extracting message masked by chaos. *Physical Review Letters, 74*, 1970–1973.

Song, Y. X., & Cao, Z. W. (2004). *Secure communication via multiparameter modulation using Chua systems*. 5th Asian control conference (vol. 2, pp. 1107–1110), Melbourne, Victoria, Australia.

Tang, Y., Gao, H. J., Zou, W., & Kurths, J. (2013). Distributed synchronization in networks of agent systems with nonlinearities and random switchings. *IEEE Transactions on Cybernetics, 43*, 358–370.

Tang, Y., Wang, Z. D., & Fang, J. A. (2011). Controller design for synchronization of an array of delayed neural networks using a controllable probabilistic PSO. *Information Sciences, 181*, 4715–4732.

Tang, Y., Wang, Z. D., Gao, H. J., Stephen, S., & Kurths, J. (2012). A constrained evolutionary computation method for detecting controlling regions of cortical networks. *IEEE/ACM Transactions on Computational Biology and Bioinformatics, 9*, 1569–1581.

Tao, C. H., Xiong, H. X., & Hu, F. (2006). Two novel synchronization criterions for a unified chaos system. *Chaos, Solitons & Fractals, 27*, 115–120.

Ueta, T., &. Chen, G. R. (2000). Bifurcation analysis of Chen's equation. *International Journal of Bifurcation and Chaos, 10*, 1917–1931.

Wang, H., Han, Z. Z., Xie, Q. Y., & Zhang, W. (2009). Sliding mode control for chaotic systems based on LMI. *Communications in Nonlinear Science and Numerical Simulation, 14*, 1410–1417.

Wu, X., Hu, H., & Zhang, B. (2004). Analyzing and improving a chaotic encryption method. *Chaos, Solitons & Fractals, 22*, 367–373.

Xiang, T., Cheng, K. W., & Liao, X. (2008). An improved chaotic cryptosystem with external key. *Communications in Nonlinear Science and Numerical Simulation, 13*, 1879–1887.

Xiao, M., & Cao, J. (2009). Synchronization of a chaotic electronic system with cubic term via adaptive feedback control. *Communications in Nonlinear Science and Numerical Simulation, 14*, 3379–3388.

Yang, T. (1995). Recovery of digital signals from chaotic switching. *International Journal of Circuit Theory and Applications, 23*, 611–615.

Yang, T. (2004). A survey of chaotic secure communication systems. *International Journal of Computational Cognition, 2*, 81–130.

Yang, T., & Chua, L. O. (1996). Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I, 43*, 817–819.

Yang, T., Yang, L. B., & Yang, C. M. (1998). Cryptanalyzing chaotic secure communication using return maps. *Physics Letters A, 245*, 495–510.

Yu, W. W., Cao, J. D., Wong, K. W., & Lü, J. H. (2007). New communication schemes based on adaptive synchronization. *Chaos, 17*, 033114–033127.