# A Robust Secondary Secure Communication Scheme Based on Synchronization of Spatiotemporal Chaotic Systems

Xing-Yuan Wang and Hao Zhang

Faculty of Electronic Information and Electrical Engineering, Dalian University of Technology,
Dalian 116024, China

Reprint requests to H. Z.; E-mail: zhangh545@yahoo.com.cn

Z. Naturforsch. **68a,** 573 – 580 (2013) / DOI: 10.5560/ZNA.2013-0046
Received May 17, 2012 / revised June 18, 2013 / published online July 31, 2013

This paper deals with the synchronization of spatiotemporal chaotic systems and presents a new robust secondary chaotic secure communication system for digital signal transmissions which can recover digital signal even though the transmitted signal is influenced by limited noise. The transmitter terminal and the receiver terminal both contain a spatiotemporal chaotic system and a hyperchaotic system. The asymptotic convergence of the errors between the states of the transmitter terminal and the receiver terminal has been proved based on the Lyapunov stable theory and active–passive decomposition (APD) method. Moreover, a random digital signal and a binary Lena image are encrypted and decrypted successfully to verify the efficiency of the proposed robust secure communication system.

*Key words:* Spatiotemporal Chaotic System; APD Method; Robust Secure Communication; Chaotic Synchronization.

*PACS numbers:* 89.75.-k; 05.45.Xt; 05.45.Gg

## 1. Introduction

In 1990, Ott, Grebogi, and Yorke from Maryland University has completed to control chaotic system using the Ott–Grebogi–Yorke (OGY) method [1]. Then, Pecora and Carroll implemented the synchronization of two coupled isomorphism chaotic systems using the circuit signal [2]. Because of the characteristic properties such as noise-like signals and unpredictability, chaotic systems are widely used in a variety of areas such as chemical reaction, biological system, secure communication, and so on. Moreover, chaotic synchronization is becoming a hot research field [3 – 5]. Typical secure communication methods based on chaotic synchronization are divided into chaotic mask, chaotic modulation, and chaotic-shift-keying [6 – 11]. Recently, researchers have done a lot of work on applying different chaotic synchronization methods and chaotic systems to secure communication and chaotic maps and systems are widely used in the secure communication scheme by researching on chaos theory [12 – 18]. However, with the development of low-dimensional chaotic systems, it is possible to infer the properties of low-dimensional chaotic systems. Furthermore, high-dimensional hyperchaotic systems or spatiotemporal chaotic systems have more than one positive Lyapunov exponents and their properties are more complex [19 – 22]. So the synchronization of high-dimensional hyperchaotic systems or spatiotemporal chaotic systems possesses more application prospects and development potentials.

The previous works always used the logistic map or Hénon map as the secure communication system for digital signals. In this paper, two new maps are taken into consideration and a novel secondary chaotic secure communication system which combines chaotic mask and chaotic modulation is presented. At the transmitter terminal, a parameter of the hyperchaotic system is controlled by a signal of the spatiotemporal chaotic system, and then the useful message is secretly modulated in the hyperchaotic system. The resulting signal is directly added into the chaotic state of the spatiotemporal chaotic system and the output signal is delivered through a public channel to the receiver terminal. Due to the complex properties of the spatiotemporal chaotic system, the signal is difficult to be intercepted. Even if it is intercepted, because of lack of parameters of the spatiotemporal chaotic system and the hyperchaotic system, it is impossible to decrypt the signal.

The rest of this paper is organized as follows. A brief description of the spatiotemporal chaotic system and the hyperchaotic system is presented in Section 2. Section 3 outlines a new secure communication scheme and the method of chaotic synchronization. Section 4 provides some numerical simulations to verify the validity of the proposed system. Finally, some concluding remarks are given in Section 5.

## 2. System Descriptions

### 2.1. One-Way Coupled Map Lattice

Spatiotemporal chaotic systems are divided into the coupled differential equations, the coupled map lattice, and the cellular automaton based on the type of time variables, space variables, and state variables. The one-way coupled map lattice is typical, it is described by the following set of equations:

$$x_{n+1}(i) = (1-\varepsilon)f(x_n(i)) + \varepsilon f(x_n(i-1)), \quad (1)$$

where $x$ is the state variable, $\varepsilon$ is the coupled intensity, $n$ is the time index, $i$ ($i = 1,2,\cdots,L$) is the site index, and $L$ is the lattice length. The boundary conditions are periodic, and the local map $f$ is described as

$$x_{n+1} = \begin{cases} a(2x_n - 1), & 0 < x_n < 1, \\ a(2x_n + 1), & -1 < x_n \le 0. \end{cases} \quad (2)$$

Figure 1 depicts the bifurcation diagram of $f$. From Figure 1, we can obtain that map (2) bifurcates when $a = 0.5$, and for $a > 0.72$, it is chaotic. In this paper, we choose $a = 0.75$ and $x_0 = 1/3$. The largest Lyapunov exponent is $\lambda_1 = 0.4108$ which indicates that the local map is chaotic. So we can get the following chaotic map:

$$x_{n+1} = \begin{cases} 1.5x_n - 0.75, & 0 < x_n < 1, \\ 1.5x_n + 0.75, & -1 < x_n \le 0. \end{cases} \quad (3)$$

If we choose conditions as $\varepsilon = 0.5$, $a = 0.75$, $L = 30$, and $n = 200$, we can get the spatiotemporal chaotic system. The spatiotemporal diagram is shown in Figure 2.

The largest Lyapunov exponent of $x_n(30)$ in the spatiotemporal chaotic system is $\lambda_1 = 0.3431$ which presents that the signal $x_n(30)$ is chaotic when $\varepsilon = 0.5$, $a = 0.75$.

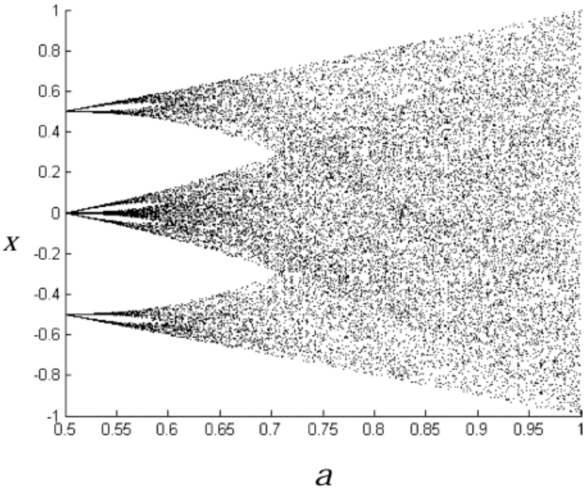


Fig. 1. Bifurcation diagram of local map versus $a$.

### 2.2. Hyperchaotic System

In this paper, we choose the following map as a chaotic map [23]:

$$y_{n+1} = 0.2 + 0.3y_n + 0.5z_n, \; z_{n+1} = -1.6 + \mu y_n^2, \quad (4)$$

where $\mu$ is the coefficient of the nonlinear section, $y$ and $z$ are the state variables, $n$ is the time index. The Lyapunov exponent spectrum of System (4) with $3 \le \mu \le 4.5$ is presented in Figure 3.

From Figure 3, we can see that when $3 \le \mu \le 4.5$, System (4) is hyperchaotic. So signals of System (4) are more complex and secure.

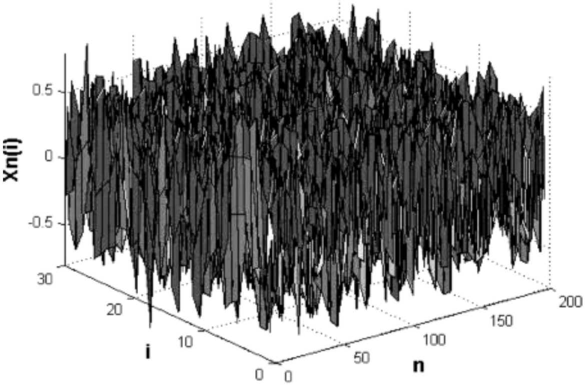


Fig. 2. Spatiotemporal diagram when $\varepsilon = 0.5$ and $a = 0.75$.

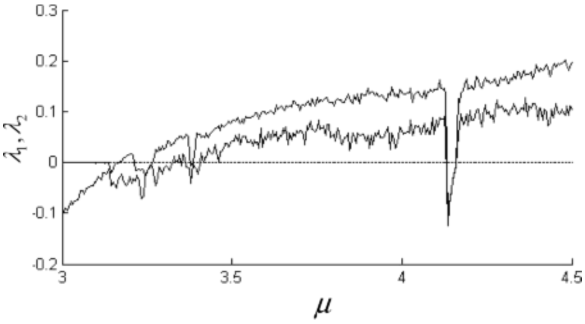


Fig. 3. Lyapunov exponents spectrum of System (4) with $3 \le \mu \le 4.5$.

## 3. Secure Communication Scheme Description

### 3.1. The Description of the Transmitter Terminal and the Receiver Terminal

In this paper, we define a communication scheme which consists of a transmitter terminal and a receiver terminal, and each terminal contains a spatiotemporal chaotic system and a hyperchaotic system. The transmitter terminal is defined as follows:

$$\begin{aligned} &x_{n+1}(1) = (1-\varepsilon)f(x_n(1)) + G\,,\\ &x_{n+1}(2) = (1-\varepsilon)f(x_n(2)) + \varepsilon f(x_n(1))\,,\\ &\quad\vdots\\ &x_{n+1}(i) = (1-\varepsilon)f(x_n(i)) + \varepsilon f(x_n(i-1))\,,\\ &i = 2,3,\cdots,L\,, \end{aligned} \tag{5}$$

and

$$\begin{aligned} y_{u_1,n+1} &= 0.2 + 0.3y_{u_1,n} + 0.5z_{u_1,n}\,,\\ z_{u_1,n+1} &= -1.6 + \mu_1 y^2_{u_1,n}\,, \end{aligned} \tag{6}$$

where $f$ is described as System (2), $G = r(m_n) + f(x_n(L))$, and $r$ is a function which is related to the signal of the hyperchaotic system, $m_n$ is the transmission signal, $\mu_1$ is a controller which is related to the signal $x(2)$ of System (5).

The receiver terminal is defined as follows:

$$\begin{aligned} &s_{n+1}(1) = (1-\varepsilon)f(s_n(1)) + G'\,,\\ &s_{n+1}(2) = (1-\varepsilon)f(s_n(2)) + \varepsilon f(s_n(1))\,,\\ &\quad\vdots\\ &s_{n+1}(i) = (1-\varepsilon)f(s_n(i)) + \varepsilon f(s_n(i-1))\,,\\ &i = 2,3,\cdots,L\,, \end{aligned} \tag{7}$$

and

$$\begin{aligned} y_{u_2,n+1} &= 0.2 + 0.3y_{u_2,n} + 0.5z_{u_2,n}\,,\\ z_{u_2,n+1} &= -1.6 + \mu_2 y^2_{u_2,n}\,, \end{aligned} \tag{8}$$

where $f$ is described as System (2), $G' = r(m_n) + f(x_n(L)) + 0.01\cdot\sin(t)$, $0.01\cdot\sin(t)$ is the limited noise, and $\mu_2$ is a controller which is related to the signal $s(2)$ of System (7).

### 3.2. APD Method

In 1990, Pecora and Carroll proposed the PC method, then Kocarev and Parlitz proposed the active-passive decomposition (APD) method [24] on the basis of the previous work. With this method, we can select the driving signal freely, and the systems will be completed synchronized. Therefore, the APD method can be widely used in secure communication.

The driving system is defined as

$$x_{n+1} = f(x_n, \xi)\,, \tag{9}$$

where $\xi$ is the parameter of the driving system, $f$ is the iterated function system, $x_n$ is the state variable, and $n$ is the time index. When the system is chaotic, (9) is translated to

$$x_{n+1} = Ax_n + G_n\,, \tag{10}$$

$$G_n = f(x_n, \xi) - Ax_n\,, \tag{11}$$

where $A$ is the coefficient matrix of the linear portion.

The response system is defined as

$$s_{n+1} = As_n + G_n\,, \tag{12}$$

so the error system can be defined as

$$e_{n+1} = Ae_n\,. \tag{13}$$

Then choose a proper $A$, which will make every eigenvalue fits $|\lambda_i| < 1$. According to the stable theory, the error array $\{e_n\}$ will converges, and synchronization will be achieved.

### 3.3. Synchronization of the Spatiotemporal Chaotic Systems

According to System (3), the definitional domain is divided into $(-1,0]$ and $(0,1)$. Because of the ergodicity of chaotic orbit and the boundedness of noise, the following conditions will be satisfied along with the iterations sooner or later:

(i) $x_n(1) \approx s_n(1)$,
(ii) $x_n(1), s_n(1) \in (-1, 0]$ or $x_n(1), s_n(1) \in (0, 1)$.

So we can obtain $f(x_n(1)) \approx f(s_n(1))$. If we choose two suitable parameters $a$ and $\varepsilon$ which satisfy $0 < 2a(1-\varepsilon) < 1$ and define the error in lattice $i$ as $e_n(i) = s_n(i) - x_n(i)$, we can infer that $e_{n+1}(1) = 2a(1-\varepsilon)e_n(1)$ and $e_n(1)$ will converge exponentially.

After converging of $e_n(i)$, $e_n(i+1)$ is described as $e_{n+1}(i) = 2a(1-\varepsilon)e_n(i)$. When the following conditions (which will be satisfied along with the iterations sooner or later) are satisfied:

(i) $x_n(i) \approx s_n(i)$,
(ii) $x_n(i), s_n(i) \in (-1, 0]$ or $x_n(i), s_n(i) \in (0, 1)$,

$e_n(i+1)$ will converge exponentially.

Based on the preceding analysis, we find that one-way coupled map lattices synchronize one by one.

### 3.4. Synchronization of Hyperchaotic Systems

Choose signal $x_n(3)$ of System (5) as driving signal, then the systems (6) and (8) can be written as

$$\begin{aligned} y_{u_1,n+1} &= 0.2 + 0.3y_{u_1,n} + 0.5z_{u_1,n}\,, \\ z_{u_1,n+1} &= -1.6 + \mu_1 x_n^2(3) \end{aligned} \tag{14}$$

and

$$\begin{aligned} y_{u_2,n+1} &= 0.2 + 0.3y_{u_2,n} + 0.5z_{u_2,n}\,, \\ z_{u_2,n+1} &= -1.6 + \mu_2 s_n^2(3)\,. \end{aligned} \tag{15}$$

From Section 3.3, we can see that $x_n(2) = s_n(2)$, $x_n(3) = s_n(3)$, so the error system of System (14) and System (15) can be written as

$$\begin{aligned} e_{u_y,n+1} &= 0.3e_{u_y,n} + 0.5e_{u_z,n}\,, \\ e_{u_z,n+1} &= 0\,. \end{aligned} \tag{16}$$

It proved that System (16) will converge to zero.

We define the following Lyapunov function:

$$V_n = \left|e_{u_y,n}\right| + \left|e_{u_z,n}\right| = \left|e_{u_y,n}\right| \geq 0\,, \tag{17}$$

now, by taking the error System (16) into (17), we get the following inequation:

$$\begin{aligned} \Delta V_n = V_{n+1} - V_n &= \left|0.3e_{u_y,n}\right| - \left|e_{u_y,n}\right| \\ &= -0.7\left|e_{u_y,n}\right| \leq 0\,. \end{aligned} \tag{18}$$

It is obvious that the error system will converge to zero according to the stable theory.

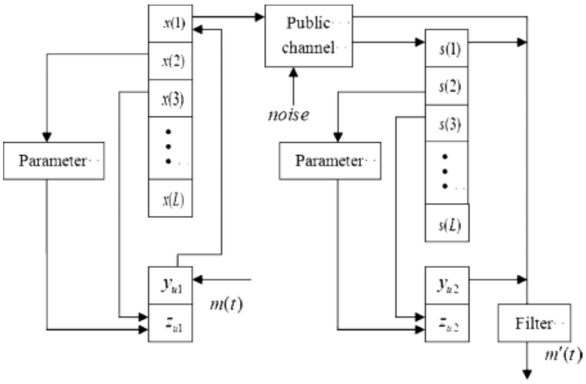


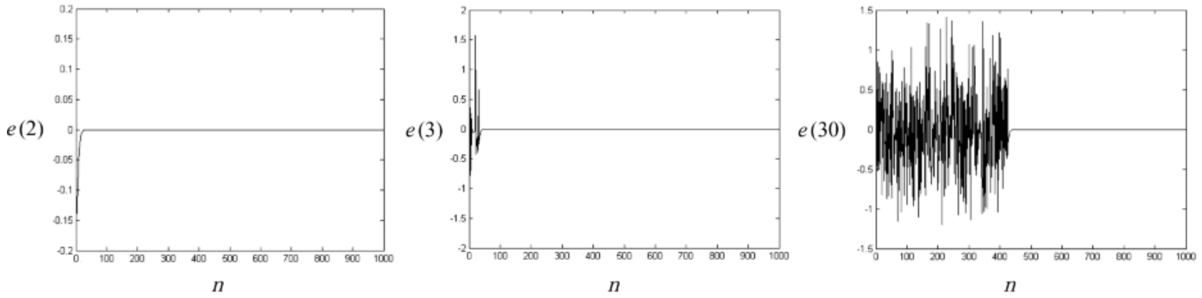
Fig. 4. Block diagram of the proposed secondary secure communication scheme.

### 3.5. Design of the Secondary Chaotic Secure Communication System

At the transmitter terminal, signal $x(2)$ of System (5) is used to control the parameter $\mu_1$ of System (6), signal $x(3)$ is the driving signal which is utilized to drive the hyperchaotic System (6), and the resulting signal $y_{u1}$ will be used to modulate the transmission signal $m_n$, then the modulated signal is added to $f(x_n(L))$, finally, the encrypted signal will be transmitted in the shape of $G$ in the public channel. At the receiver terminal, signal $G$ will be used to synchronize System (5) and System (7). After synchronizing, signal $s(2)$ of System (7) is used to control the parameter $\mu_2$ of System (8), signal $s(3)$ is the driving signal which is utilized to drive hyperchaotic System (8). Based on the preceding analysis, the transmitter terminal and the receiver terminal will be synchronized, and the transmitted signal will be recovered at the same time. Figure 4 depicts a block diagram of the proposed secondary secure communication scheme.

## 4. Simulation Results

The transmitter terminal and the receiver terminal are defined as systems (5), (6) and systems (7), (8). At the transmitter terminal and the receiver terminal, we choose the random initial conditions of the spatiotemporal chaotic systems as $x_0(i)$, $i = 2, 3, \cdots, L$, and $s_0(i)$, $i = 2, 3, \cdots, L$, respectively, with the lattice length being $L = 30$, iteration times being $n = 1000$, and the coupling parameter being $\varepsilon = 0.5$. The transmission signal $m_n$ is also randomly generated. We define the



(a) Error curve of $e_n(2)$ (b) Error curve of $e_n(3)$ (c) Error curve of $e_n(30)$

Fig. 5. Error curves of the spatiotemporal chaotic systems.

lattice map as System (3), the initial conditions of the hyperchaotic system at the transmitter terminal are defined as $y_{u_1} = 0.5$, $z_{u_1} = 0.5$, and at the receiver terminal, the initial conditions of the hyperchaotic system are defined as $y_{u_2} = 0.8$, $z_{u_2} = 0.2$. Controllers at each side are selected as

$$\mu_1 = 3.5 + \frac{|x_n(2)|}{2}, \quad \mu_2 = 3.5 + \frac{|s_n(2)|}{2}.$$

The primary modulation function is defined as

$$r(m_n) = \frac{2m_n - 1}{10} y_{u_1,n},$$

the secondary encryption modulation function is defined as

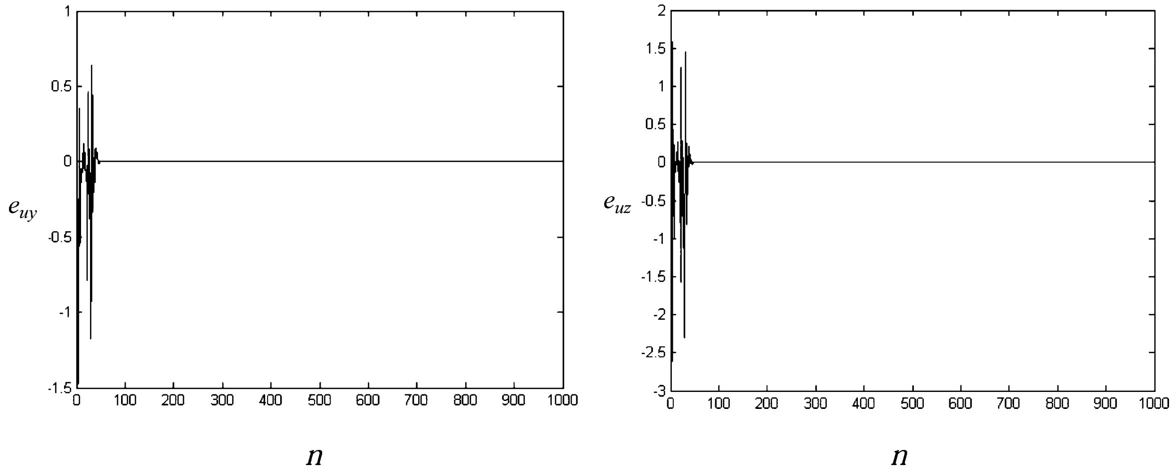
$$G = r(m_n) + f(x_n(L)).$$

And the limited noise in the public channel is $0.01 \cdot \sin(t)$.

Select the error signals which are related to the communication to observe; the error curves of the spatiotemporal chaotic systems (5) and (7) are shown in Figure 5. Error curves of the hyperchaotic discrete systems (6) and (8) are shown in Figure 6.

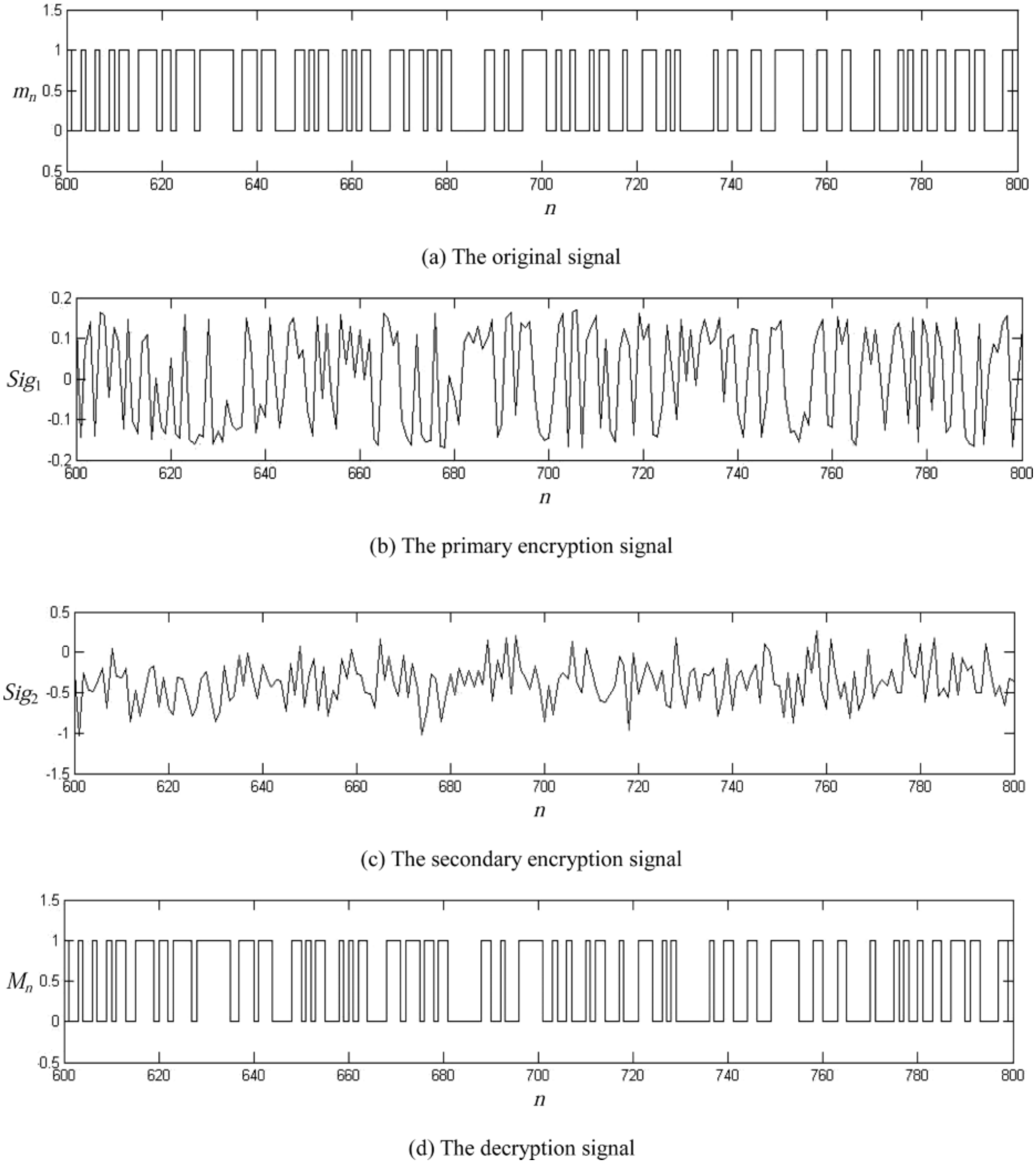
Because it will take a certain period of time before synchronization, we select a special encryption signal which is defined between 600 times and 800 times as desired signal to observe. The original signal $m_n$, primary encryption signal $\text{Sig}_1$, secondary encryption signal $\text{Sig}_2$, and recovery signal $M_n$ are shown in Figure 7.

We can draw the conclusion from Figure 6 that errors $e_n(2)$, $e_n(3)$, and $e_n(30)$ converge to zero after iterating about 30 times, 50 times, and 450 times, which



(a) Error curves of $e_{uy}$ (b) Error curves of $e_{uz}$

Fig. 6. Error curves of the hyperchaotic systems.



(a) The original signal

(b) The primary encryption signal

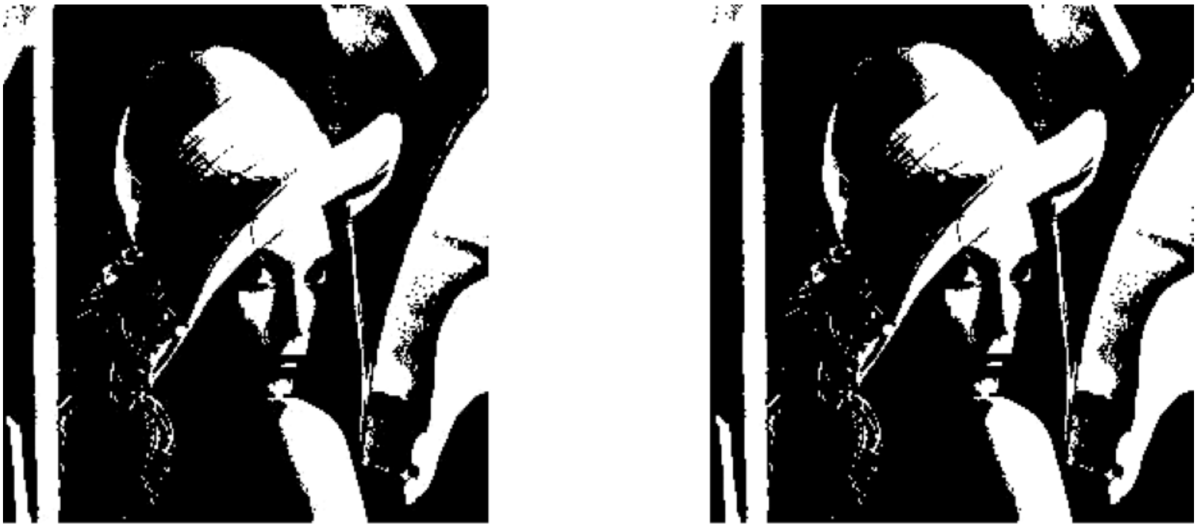
(c) The secondary encryption signal

(d) The decryption signal

Fig. 7. Signals during the communication.

indicates that the process of synchronization is gradual. In the drive of spatiotemporal chaos signal, the hyperchaotic systems also reach synchronization after about 100 times.

From Figure 7, we can draw the conclusion that the signal becomes very complex and can't be distinguished from the original signal after the first encryption, and the signal becomes more chaotic after



(a) The transmitted image

(b) The recoverd image

Fig. 8. (a) Transmitted and (b) recovered image.

secondary encryption. At the receiver terminal, the signal is completely recovered after decryption and the decryption signal is presented in Figure 7d, which shows the effectiveness of our secure communication scheme.

At last, with the above method, we choose the binary Lena image as the transmitted image, which consists of 0 and 1. The transmitted image and the recoverd image are shown in Figure 8. We can conclude that the image is totally recovered at the receiver terminal and the effectiveness of our robust secure communication is visible.

## 5. Conclusions

In order to enhance the security of the digital signal transmission, in this paper, utilizing the characteristic properties of spatiotemporal chaos and hyperchaotic system, we have proposed a new secondary chaotic secure communication system. Under this structure, the digital signal can be successfully and secretly delivered via the chaotic synchronization, chaotic modulation, chaotic mask, signal transmitting and receiving. By the use of chaotic modulation and chaotic mask in high-dimension complex chaotic systems, namely spatiotemporal chaos system and the hyperchaotic system, we have greatly improved the security of digital signal transmission. Additionally, the structure of our system is simple and no extra controllers are needed, which makes the design of the system flexible and revelatory. Numerical simulations show the effectiveness and feasibility of our method.

*Acknowledgements*

This research is supported by the National Natural Science Foundation of China (Nos: 61173183, 60973152, and 60573172), the Doctoral Program Foundation of Institution of Higher Education of China (No: 20070141014), Program for Liaoning Excellent Talents in University (No: LR2012003), the National Natural Science Foundation of Liaoning province (No: 20082165), and the Fundamental Research Funds for the Central Universities (No: DUT12JB06).

[1] E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. B **64**, 1196 (1990).

[2] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. B **64**, 821 (1990).

[3] G. R. Wang, X. L. Yu, and S. G. Chen, Chaotic Control, Synchronization and Utilizing, National Defence Industry Press, Beijing 2001.

[4] X. Y. Wang, Chaos in the Complex Nonlinearity System, Electronics Industry Press, Bejjing 2003.

[5] G. R. Chen and J. H. Lü, Dynamical Analyses, Control and Synchronization of the Lorenz system family, Science Press, Beijing 2003.

[6] L. Kocarev, K. S. Halle, and K. Eckert, Int. J. Bifurc. Chaos **2**, 709 (1993).

[7] K. M. Cuomo, A. V. Oppenheim, and S. H. Strogatz, IEEE T. Circuits II **40**, 626 (1993).

[8] H. Dedieu, M. P. Kennedy, and M. Hasler, IEEE T. Circuits II **40**, 634 (1993).

[9] K. S. Halle, C. W. Wu, and M. Itoh, Int. J. Bifurc. Chaos **40**, 469 (1993).

[10] M. Itoh and H. Murakami, IEICE T. Fund. Electr. **BE78A**, 285 (1995).

[11] M. Itoh, C. W. Wu, and L. O. Chua, Int. J. Bifurc. Chaos **7**, 275 (1997).

[12] X. Wu and H. Zhang, Chaos Solitons Fract. **39**, 2268 (2009).

[13] X. Wu, Z. H. Guan, and Z. Wu, Nonlin. Anal. Theor. **68**, 1346 (2008).

[14] H. G. Zhang and Y. B. Quan, IEEE Transact. Fuzzy Sys. **9**, 349 (2001).

[15] X. M. Wang and J. S. Zhang, Phys. Lett. A. **357**, 323 (2006).

[16] H. G. Zhang, Z. L. Wang, and D. R. Liu, Int. J. Bifurc. Chaos **15**, 2603 (2005).

[17] H. G. Zhang, H. Wang, Z. L. Wang, and T. Y. Chai, Phys. Lett. A. **350**, 363 (2006).

[18] N. Smaoui, A. Karouma, and M. Zribi, Commun. Nonlin. Sci. Numer. Simul. **16**, 3279 (2011).

[19] K. A. Mires and J. C. Sprott, Phys. Lett. A. **254**, 275 (1999).

[20] S. Codreanu, Chaos Solitons Fract. **15**, 507 (2003).

[21] T. C. Newell, P. M. Alsing, and A. Gavrielids, Phys. Rev. E. **51**, 2963 (1995).

[22] H. Ma, K. E. Zhu, and T. L. Chen, Commun. Theor. Phys. **45**, 477 (2006).

[23] L. Cheng, L. Tao, Q. N. Huang, and J. H. Peng, J. Northeast Norm. Univ. **34**, 47 (2002).

[24] L. Koclrev and U. Parlitz, Phys. Rev. Lett. **74**, 5028 (1995).