Secure communication based on spatiotemporal chaos*

Ren Hai-Peng(任海鹏)† and Bai Chao(白 超)

Department of Information and Control Engineering, Xi'an University of Technology, Xi'an 710048, *China*

(Received 27 November 2014; revised manuscript received 23 February 2015; published online 20 June 2015)

In this paper, we propose a novel approach to secure communication based on spatiotemporal chaos. At the transmitter end, the state variables of the coupled map lattice system are divided into two groups: one is used as the key to encrypt the plaintext in the N-shift encryption function, and the other is used to mix with the output of the N-shift function to further confuse the information to transmit. At the receiver end, the receiver lattices are driven by the received signal to synchronize with the transmitter lattices and an inverse procedure of the encoding is conducted to decode the information. Numerical simulation and experiment based on the TI TMS320C6713 Digital Signal Processor (DSP) show the feasibility and the validity of the proposed scheme.

Keywords: secure communication, spatiotemporal chaos, synchronization, N-shift function

PACS: 05.45.Vx, 05.45.Xt, 05.45.Jn, 05.45.–a **DOI:** 10.1088/1674-1056/24/8/080503

1. Introduction

Since chaotic signals are irregular, aperiodic, uncorrelated, broad band, easy to generate, and difficult to predict over a long time, the secure communication based on these inherent features of a chaotic signal has aroused ongoing and growing research interest.[1]

Chaotic secure communication has received extensive attention since the possibility of synchronization of two coupled chaotic systems was reported in the early 1990s.[2–6] The reported methods could be divided into three categories. 1) The methods use chaotic symbols to transmit information.[6,7] The symbolic dynamics of a chaotic electrical oscillator is controlled to carry the message by using small perturbing pulses. 2) The methods use chaotic synchronization for secure communication. The methods of this kind can be divided into chaotic masking, chaotic modulation, and chaotic shift keying. Oppenheim *et al.* proposed chaotic masking,[8] and this method depends on the degree of chaotic synchronization and is susceptible to channel noise. Moreover, it is subjected to the attacking of time-delay embedded[9] and return map decoding.[10] Halle *et al.* suggested chaotic parameter modulation.[11] This method shows better performance than chaotic masking, but it is still sensitive to noise, and it could be attacked by nonlinear dynamic (NLD) forecasting techniques[12] and the time series analysis method.[13] Dedieu *et al*. proposed chaotic shift keying communication;[14] these secure communication schemes could be broken using the short-time zero-crossing rate,[15] spectrogram analysis,[16] generalized synchronization,[17] and adaptive key identification.[18] Thus, this method shows the weak security. 3) The methods use chaos asynchronous communication technology, such as chaos-based asynchronous code division multiple access (CDMA) systems,[19] direct sequence spread spectrum system.[20] These methods use chaotic series to replace pseudo-random code, have better performance than the traditional pseudo-random code. But the advantages of the chaotic signal, like broad band, orthogonality, etc. are not demonstrated in these methods. Since the chaotic communication has been reported to be successfully used in a commercial fiber optic channel to obtain a higher bit transmission rate,[21] chaotic communication research has gained more attention from the practical application viewpoint recently.[22–25]

In this paper, we propose a novel approach to chaos communication based on spatiotemporal chaos. In this approach, the m-dimensional states of one-way coupled map lattices are divided into the two groups. One group is used as the inputs of the N-shift function to confuse $m/2$ plaintexts, then the outputs of the N-shift function are mixed with the other group of states to obtain the transmitted signals, which are used as not only transmission signals in the communication channel, but also the drive signals to synchronize the one-way coupled map lattices at the receiver end with those at the transmitter end. Once the synchronization between the receiver and the transmitter is established, the reverse operations at the receiver end will decode the transmitted information. This approach has three advantages: firstly, the spatiotemporal chaos system has the number of positive Lyapunov exponents equal to the dimension number of the system, which increases the randomness and unpredictability of the system. It is difficult to attack by using the time-delay embedded method. Secondly, the state variables of the coupled map lattice system are di-

*Project supported by the National Natural Science Foundation of China (Grant No. 61172070) and the Funds from the Science and Technology Innovation Team of Shaanxi Province, China (Grant No. 2013CKT-04).

†Corresponding author. E-mail: haipengren@gmail.com

© 2015 Chinese Physical Society and IOP Publishing Ltd

vided into two groups, one group is used as the inputs of the N-shift encryption function to encrypt the plaintext, and the other group is mixed with the outputs of the N-shift function to further confuse the information. Neither the key nor the plaintext transmits through the public channel, it will confuse the return map attacking. Thirdly, the chaos synchronization between the transmitter lattice and the receiver lattice is implemented by using similar drive signals, which are average values of the transmitted signal at the transmitter end and the received signal at the receiver end. The average operation acts as a filter to reduce the effect of noise on the synchronization, which makes the scheme possess better robustness to noise. Simulation and experiment based on TI TMS320C6713 show the feasibility and validity of the proposed scheme.

2. Synchronization of one-way coupled map lattices

2.1. One-way coupled map lattices

A spatiotemporal chaos system processes a mutual influence in both time and space, which is sensitive to initial conditions, boundary conditions, and parameter changes. The one-way coupled map lattice (OCOML) is a special case of the spatiotemporal chaos system.

The state equations of OCOML are

$$\begin{aligned} &x_0(i) = \text{init}(i), \\ &x_t(0) = d(t), \\ &x_{t+1}(i) = (1-\varepsilon_i) f[x_t(i)] + \varepsilon_i f[x_t(i-1)], \\ &i = 1,2\ldots,m, \end{aligned} \tag{1}$$

where t represents the discrete time, m is the space dimension number of OCOML, init(i) the initial value of the i-th lattice, ε_i the coupling strength $0 < \varepsilon_i < 1$, $x_t(0) = d(t)$ the drive signal of the system, $t = 0,1,2,\ldots$ the discrete time, and $f(x)$ a nonlinear chaotic map given by $f(x) = 4x(1-x)$. The simulation result of this system is shown in Fig. 1, where i is the space position, t the discrete time, and $x_t(i)$ is the state of the i-th lattice at time t. The coupling strength used in Fig. 1 is $\varepsilon_i = 0.85$ $(i = 1,2,\ldots,m = 60)$. From Fig. 1, we see that the spatiotemporal chaos demonstrated by the OCOML is very complex, depending on both the time and space.

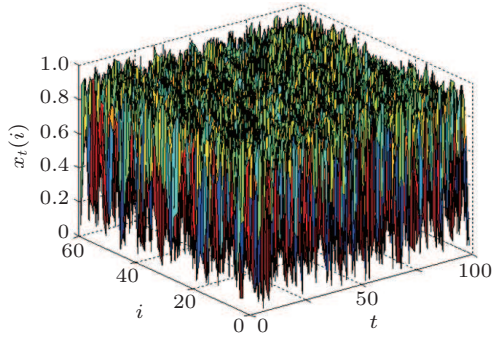


Fig. 1. (color online) State diagram of the spatiotemporal chaos of OCOML with 60 lattices.

2.2. Synchronization of OCOMLs

The transmitter OCOML is given as

$$x_{t+1}(i) = (1-\varepsilon_i) f[x_t(i)] + \varepsilon_i f[x_t(i-1)], \tag{2}$$

and the receiver OCOML is expressed as

$$y_{t+1}(i) = (1-\varepsilon_i) f[y_t(i)] + \varepsilon_i f[y_t(i-1)]. \tag{3}$$

The dynamics of receiver system (3) is identical to that of the transmitter system (2). The receiver and the transmitter are synchronized under the same drive time series on the 0th lattice, in other words, if $x_t(0) = y_t(0) = D(t)$, then the synchronization is achieved, where $D(t)$ is a random or chaotic drive signal (series), t represents discrete time like that in Eq. (1). The drive series can choose and use (i) uniformly distributed random series; (ii) the series generated by a chaotic system. When we choose the uniformly distributed random series as the drive signal, the synchronization results of the two systems both with 15 lattices are shown in Fig. 2. The time series of the 10th lattice of the two systems are given in Fig. 2(a). The error of these states is given in Fig. 2(b). The square error sum of all the states of the lattices is defined as $e_s = \sum_{i=1}^{m} [x_t(i) - y_t(i)]^2$, which is given in Fig. 2(c). From Fig. 2, we have that two systems are in synchronization with each other after a short transient state.

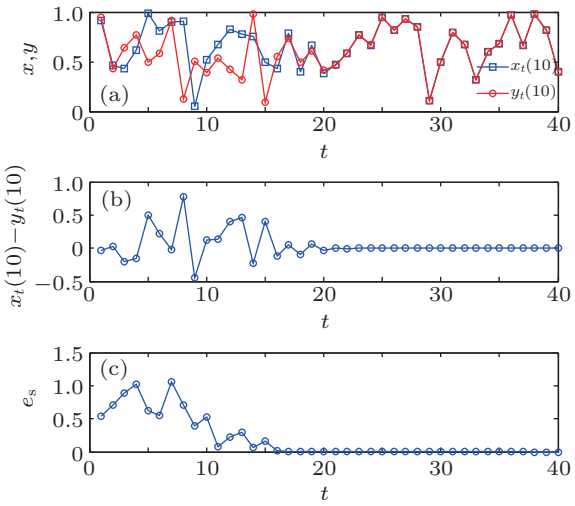


Fig. 2. (color online) The transient states of synchronization of the two systems under the same driven series. (a) The time series of the 10th lattice of the two systems. (b) The state error of the 10th lattices between the transmitter and receiver. (c) The square error sum of all states of the lattices.

3. Secure communication scheme based on the spatiotemporal chaos

The proposed secure chaotic communication scheme is shown in Fig. 3. There is an m-dimensional OCOML system at each of the transmitter end and the receiver end, and these two systems are referred to as OCOML-L and OCOML-R respectively.

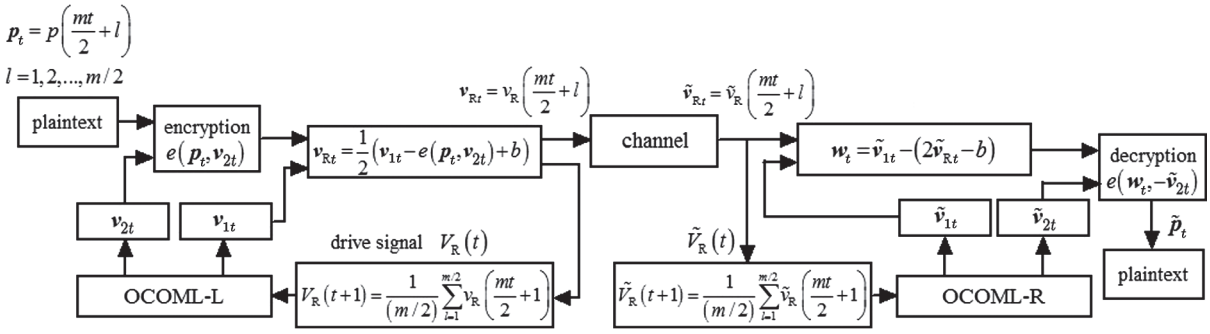


Fig. 3. Block diagram of the chaotic secure communication system.

At the transmitter end, the m-dimensional OCOML-L is given by Eq. (2), where $\varepsilon_i = 0.85$, $f(x) = 4x(1-x)$, and m is an even number.

The state variables of the OCOML-L are divided into two groups, and expressed as

$$\begin{aligned} \boldsymbol{v}_{2t} &= [ax_t(1), ax_t(3), \ldots, ax_t(m-1)], \\ \boldsymbol{v}_{1t} &= [ax_t(2), ax_t(4), \ldots, ax_t(m)], \end{aligned} \tag{4}$$

where $x_t(i)$ is the state variable of the i-th lattice at time t, and $0 < a < 1$ is a constant gain. Plaintext frame with $m/2$ messages is given as follows:

$$\boldsymbol{p}_t = \left[p\left(\frac{mt}{2}+1\right), p\left(\frac{mt}{2}+2\right), \ldots, p\left(\frac{m(t+1)}{2}\right) \right], \tag{5}$$

where t is corresponding to the discrete time of the OCOML-L. The plaintext vector $\boldsymbol{p}_t$ is encrypted by vector $\boldsymbol{v}_{2t}$ through using N-shift function $e(\boldsymbol{p}_t, \boldsymbol{v}_{2t})$, where N-shift cipher $e(z_1, z_2)$ is defined as

$$e(z_1, z_2) = \underbrace{f_1(\ldots f_1(f_1}_{N}(z_1, z_2), z_2), \ldots, z_2), \tag{6}$$

where $f_1(z_1, z_2)$ is given by

$$f_1(z_1, z_2) = \begin{cases} (z_1+z_2)+2h, & -2h \le (z_1+z_2) \le -h, \\ (z_1+z_2), & -h < (z_1+z_2) < h, \\ (z_1+z_2)-2h, & h \le (z_1+z_2) \le 2h. \end{cases} \tag{7}$$

The relationship between input and output of $f_1(.,.)$ is shown in Fig. 4.

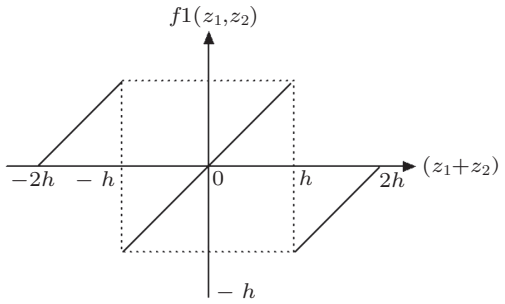


Fig. 4. Input–output relationship of shift function.

An appropriate parameter h makes z_1 and z_2 be in the range $(-h, h)$. The transmitted frame in the public channel is

$$\boldsymbol{v}_{\mathrm{R}t} = \frac{1}{2}\left(\boldsymbol{v}_{1t} - e\left(\boldsymbol{p}_t, \boldsymbol{v}_{2t}\right) + b\right), \tag{8}$$

where $0 < b < 1$ is a constant gain. The cryptograph frame is written as

$$\boldsymbol{v}_{\mathrm{R}t} = \left[v_{\mathrm{R}}\left(\frac{mt}{2}+1\right), v_{\mathrm{R}}\left(\frac{mt}{2}+2\right), \ldots, v_{\mathrm{R}}\left(\frac{m(t+1)}{2}\right) \right]. \tag{9}$$

The drive signal of the transmitter at moment t+1 is

$$x_{t+1}(0) = V_{\mathrm{R}}(t+1) = \frac{1}{(m/2)} \sum_{l=1}^{m/2} v_{\mathrm{R}}\left(\frac{mt}{2}+l\right). \tag{10}$$

So far, a plaintext frame has been encrypted by m state variables of the OCOML-L at time t.

At the receiver end, the transmitted plaintext can be recovered by using a reverse process of encryption. The m-dimensional OCOML-R is given by Eq. (3). Driven by the same signal, the OCOML-R and the OCOML-L will synchronize from any initial conditions after a transient state. The receiver is driven by

$$y_{t+1}(0) = \frac{1}{(m/2)} \sum_{l=1}^{m/2} \tilde{v}_{\mathrm{R}}\left(\frac{mt}{2}+l\right), \tag{11}$$

where $\tilde{v}_{\mathrm{R}}(mt/2+l)$ is the received signal of $v_{\mathrm{R}}(mt/2+l)$ after being transmitted in the public channel. The state variables of the OCOML-R are also divided into two groups as follows:

$$\begin{aligned} \tilde{\boldsymbol{v}}_{2t} &= [ay_t(1), ay_t(3), \ldots, ay_t(m-1)], \\ \tilde{\boldsymbol{v}}_{1t} &= [ay_t(2), ay_t(4), \ldots, ay_t(m)]. \end{aligned} \tag{12}$$

The recovered frame is

$$\boldsymbol{w}_t = \tilde{\boldsymbol{v}}_{1t} - (2\tilde{\boldsymbol{v}}_{\mathrm{R}t} - b), \tag{13}$$

where

$$\boldsymbol{w}_t = \left[w\left(\frac{mt}{2}+1\right), w\left(\frac{mt}{2}+2\right), \ldots, w\left(\frac{m(t+1)}{2}\right) \right].$$

The plaintext can be decoded by N times iterations of the shift function (N-shift function), i.e.,

$$\tilde{\boldsymbol{p}}_t = e\left(\boldsymbol{w}_t, -\tilde{\boldsymbol{v}}_{2t}\right)$$

$$= \underbrace{f_1(\ldots f_1}_{N}(f_1(\boldsymbol{w}_t, -\tilde{\boldsymbol{v}}_{2t}), -\tilde{\boldsymbol{v}}_{2t}), \ldots, -\tilde{\boldsymbol{v}}_{2t}). \quad (14)$$

The values of N, h, a, b are the same as those used at the transmitter end. The $\tilde{\boldsymbol{p}}_t$ is the received decryption frame.

From the above scheme, we know that the proposed method has the following features. Firstly, our method is different from those in Refs. [10] and [12], since our proposed secure communication system is based on hyper-chaotic spatiotemporal system. The spatiotemporal chaos system has positive Lyapunov exponents equal to the dimension number of the system, i.e., m. Therefore, the phase space of the signal would be very complex. It is difficult to attack by the time-delay embedded method.[9] Secondly, unlike using the XOR operation in Refs. [4] and [5] to encrypt the plaintext, a more complicated iteration, i.e., the N-shift function, is used in the proposed method, where the key is used to encrypt the plain signal through N-shift function. Since the N-shift function is a more complicated nonlinear function of the plaintext and the chaotic signal, it is very difficult to predict the plaintext from the output of the N-shift function. Thirdly, the key stream is transmitted in the public channel directly in Refs. [4] and [8], however, in our proposed method, neither the key nor the plaintext is transmitted directly in the public channel, which hides both the dynamical and the statistical characteristics of both chaotic key and plaintext. It would confuse the return map message recovery method.[10] Finally, the drive signal at the receiver end is an average value of $m/2$ transmitted data, which acts as a filter to reduce the effect of noise on the synchronization, which makes the scheme possess better robustness to noise as compared with a conventional synchronization method, for example, the method in Ref. [8].

4. Simulation results

In this section, we show the performance of the proposed secure communication scheme. In the following simulations, the following parameters are used: $\varepsilon_i = 0.85$, $a = 0.4$, $b = 0.4$, $h = 0.7$, $m = 10$, and $N = 30$. In the first case, a sinusoidal signal is transmitted, the results are given in Fig. 5. The plaintext $\boldsymbol{p}_t = 0.2\sin(2\pi t)$ is given in Fig. 5(a); the transmitted signal is given in Fig. 5(b); the frequency spectrum of the transmitted signal is given in Fig. 5(c); the recovered signal is given in Fig. 5(d); the error between the plaintext and the recovered signal is given in Fig. 5(e).

From Fig. 5, we can see that the cryptographic signal is different from the original signal, and that the recovered signal is the same as the original signal. From Fig. 5(c), we know that the spectrum of the transmitted sinusoidal signal is fully embedded into the chaotic signal spectrum. From Fig. 5(d), we find that the plaintext is recovered after a transient state of synchronization.

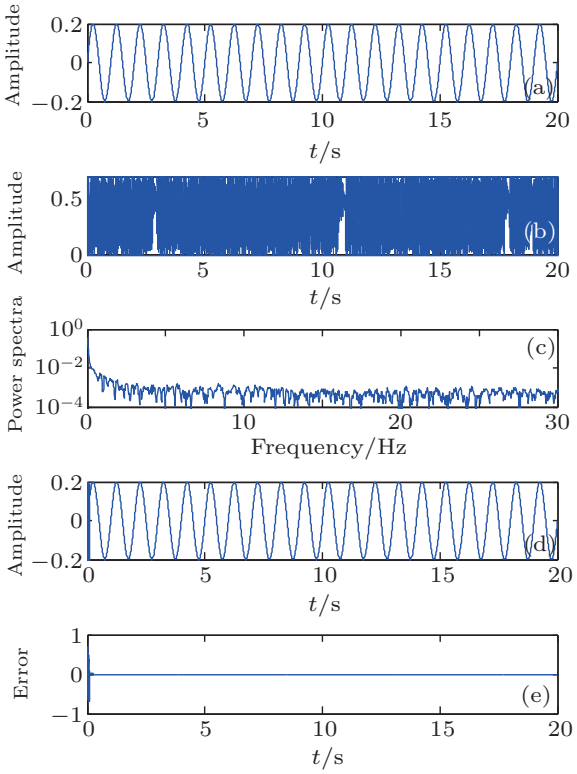


Fig. 5. (color online) Results of transmitting sinusoidal signal with using the proposed communication scheme. (a) The plaintext to be transmitted; (b) the transmitted signal in the public channel; (c) the power spectrum of the transmitted signal; (d) the recovered signal; (e) the error between the plaintext signal and the recovered signal.

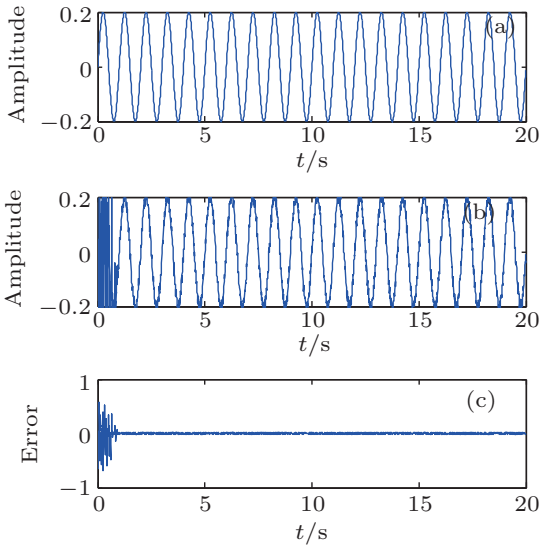


Fig. 6. (color online) Results of transmitting sinusoidal signal with using the proposed communication scheme in the presence of noise. (a) The plaintext to be transmitted; (b) the recovered signal from the transmitted signal is pulled by noise; (c) the error between the plaintext signal and the recovered signal.

In fact, the transmitted signal in a public channel is susceptible to the noise. The uniform distribution noise in the range $(-0.05A, 0.05A)$ (A is the amplitude of the transmitted signal) is incorporated into the transmitted signal. The simulation results are shown in Fig. 6, in which the transmitted signal, the recovered signal, and the error are given in Figs. 6(a), 6(b), and 6(c), respectively.

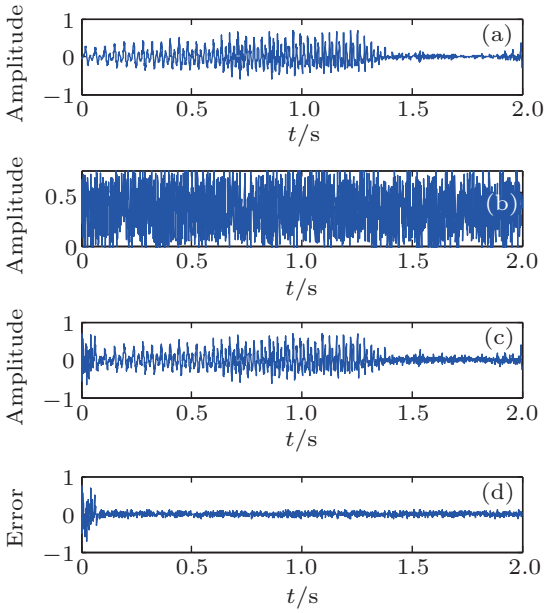


Fig. 7. (color online) Results of the secure voice communication with using the proposed scheme in the presence of noise. (a) The voice signal to be transmitted; (b) the transmitted signal in the public channel; (c) the recovered voice signal; (d) the error between the plaintext voice signal and the recovered voice signal.

From Fig. 6, we see that the plaintext can be recovered even though the transmitted signal is polluted by the noise. Although the noise pollutes the recovered signal, one can reduce the influence through some simple low-pass filters.

In the second case, the proposed scheme is also used for secure voice communication. There exists uniform distribution noise with the amplitude less than 10% of transmitted signal amplitude in the received signal. The result is shown in Fig. 7, where the plaintext signal is shown in Fig. 7(a), the signal in the communication channel is shown in Fig. 7(b), the recovered signal is shown in Fig. 7(c), the error between the recovered signal and the corresponding plaintext are given in Fig. 7(d). From Fig. 7, we see that the recovered signal is similar in wave form to the transmitted signal, and that the recovered voice is intelligible to be the same as that transmitted.

5. Experiment based on DSP

The experimental implementation of the proposed communication scheme is conducted using two floating-point DSPs, i.e., the TMS320C6713 develop starter kit (DSK) board. The block diagram of the experiment is given in Fig. 8. At the transmitter end, the voice signal is sampled by the embedded analog-to-digital (A/D) converter on a DSK board. The sampled signal is encrypted by the proposed algorithm, then the encrypted signal is transmitted through a multichannel buffered serial port (MCBSP) (a kind of series communication channel in the DSP chip) to the receiver end. At the receiver end, the received signal is used to decrypt the plaintext in DSP and replay them through the digital-to-analog (D/A) converter and the speaker.

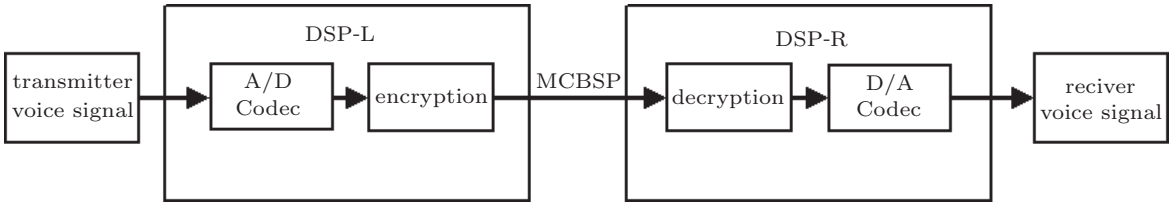


Fig. 8. Block diagram of the experimental setup for demonstrating the proposed secure communication scheme.

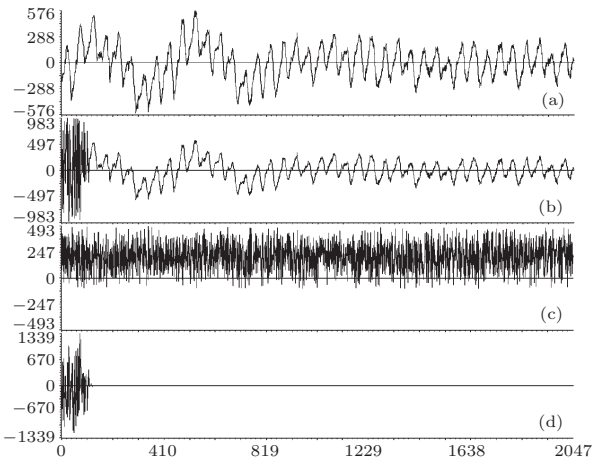


Fig. 9. Experimental results of voice communication with using DSPs.

The experiment results are given in Fig. 9. The plaintext signal is given in Fig. 9(a); the recovered signal is given in Fig. 9(b); the cryptograph signal is given in Fig. 9(c); the error between the plaintext signal and the recovered signal is shown in Fig. 9(d). The experimental results show the feasibility of the proposed method.

6. Conclusions

The OCOML system processes a mutual influence between lattices both on time and space, and it is sensitive to initial conditions, boundary conditions, and parameter changes. These features contribute to security communication. In this paper, we propose a novel approach to secure communication based on such a spatiotemporal chaos. The state variables of the coupled map lattice system are divided into two groups and are used as the key to encrypt the plaintext. Neither the key signal nor the plaintext is directly transmitted in the public channel, which hides both the dynamical and the statistical

characteristics of both chaotic key and plaintext. The level of security is enhanced. The proposed communication scheme is testified by DSP. The future work will be programming a secure exchange software based on the Android operation system to improve the security of personal cell phone communications.

References

[1] Ren H P, Baptist M and Grebogi C 2014 *Robustness of chaos to media with multipath propagation* (Boca Raton: CRC Press) pp. 423–437

[2] Carroll T L, Pecora and Louis M 1991 *IEEE Trans. Circuits Syst. II* **38** 453

[3] Ren H P and Li W C 2010 *Commun. Nonlinear Sci. Numer. Simul.* **15** 3058

[4] Wang X Y, Zhang N, Ren X L and Zhang Y L 2011 *Chin. Phys. B* **20** 020507

[5] Wang X Y and Wang Q 2014 *Chin. Phys. B* **23** 030503

[6] Ren H P, Baptist M and Grebogi C 2012 *Int. J. Bifur. Chaos* **22** 1250199

[7] Hayes S, Grebogi C, Ott E and Mark A 1994 *Phys. Rev. Lett.* **73** 1781

[8] Oppenheim A V, Wornell G W, Isabelle S H and Cuomo K M 1992 *Proc. IEEE ICASSP*, March 23–26, 1992, San Franciso, USA, p. 117

[9] Ponomarenko V I and Prokhorov M D 2002 *Phys. Rev. E* **66** 026215.

[10] Yang T, Yang L B and Yang C M 1998 *Phys. Lett. A* **245** 495

[11] Halle K S, Wu C W, Itoh M and Chua L O 1993 *Int. J. Bifur. Chaos* **3** 469

[12] Andrew T P and Kevin M S 2001 *IEEE Trans. CAS I* **48** 624

[13] Kevin M S 1994 *Int. J. Bifur. Chaos* **4** 959

[14] Dedieu H, Kennedy M P and Hasler M 1993 *IEEE Trans. CAS II* **40** 634

[15] Chin Y C, Dao L X and Steven R B 2004 *Chaos, Solitons and Fractals* **21** 1129

[16] Yang T, Yang L B and Yang C M 1998 *Phys. Lett. A* **247** 105

[17] Yang T, Yang L B and Yang C M 1998 *IEEE Trans. CAS I* **45** 1062

[18] Ren H P, Han C Z and Liu D 2008 *Chin. Phys. B* **17** 1202

[19] Gianluc M, Riccardo R and Gianluc S 2001 *IEEE Trans. CAS I* **48** 1445

[20] Ren H P, Kong Q J and Bai C 2015 *Proc. IEEE IWS*, March 30–April 1, 2015, Shenzhen, China, p. 82

[21] Argyris A, Syvridis D, Larger L, Annovazzi L V, Colet P, Fischer I, Garcia O J, Mirasso C R, Pesquera L and Shore K A 2005 *Nature* **438** 343

[22] Ren H P, Baptist M and Grebogi C 2013 *Phys. Rev. Lett.* **110** 184101

[23] Zhou J, Jiang H, Hisakazu K and Shao G F 2014 *Acta Phys. Sin.* **63** 140506 (in Chinese)

[24] Huang J W, Li G M, Feng J C and Jin J X 2014 *Acta Phys. Sin.* **14** 140502 (in Chinese)

[25] Wang X Y and Luan D P 2013 *Chin. Phys. B* **22** 110503