Vol 14 No 2, February 2005
1009-1963/2005/14(02)/0274-05

Chinese Physics

© 2005 Chin. Phys. Soc.
and IOP Publishing Ltd

Chaos communication based on synchronization of discrete-time chaotic systems*

Lu Jun-Guo(卢俊国)† and Xi Yu-Geng(席裕庚)

Department of Automation, Shanghai Jiaotong University, Shanghai 200030, *China*

(Received 14 March 2003; revised manuscript received 23 September 2004)

A novel chaos communication method is proposed based on synchronization of discrete-time chaotic systems. This method uses a full-order state observer to achieve synchronization and secure communication between the transmitter and the receiver. Further, we present a multiple-access chaotic digital communication method by combining the observer with the on-line least square method. Simulation results are also given for illustration.

Keywords: chaos, chaos synchronization, chaos communication, on-line least square method
PACC: 0545

1. Introduction

Chaos dynamics is deterministic but extremely sensitive to initial conditions. Even infinitesimal changes in the initial condition will lead to exponential divergence of orbits. Moreover, a broad-spectrum and noise-like chaotic signal is particularly appropriate for secure communications.[1] Over the last decade synchronization of chaotic systems and its application to secure communication have received considerable attention.[1−12] Different chaos communication methods have been developed in order to hide the contents of a message using chaotic signals. Apart from Refs.[10–12], most of the previous researches on chaos synchronization and communication have concentrated on continuous-time rather than discrete-time chaotic systems. All of the above analogue communication schemes show an intrinsic weak robustness; i.e. the unavoidable errors in the values of the circuit components as well as the disturbances generated by the communication link can heavily influence the synchronization process and can make it ineffective.[10] This may be a drawback for practical applications. Synchronization of discrete-time chaotic systems with potential applications in discrete communication has not been thoroughly discussed. In this paper, we firstly design a full-order observer in the receiver to implement synchronization and secure communication with the transmitter. Further, based on the proposed observer and the on-line least square method, a multiple-access chaotic digital secure communication method is proposed. Finally, simulation results are used to show the effectiveness of the proposed theory.

2. The proposed method

Consider a discrete-time chaotic system described by

$$x(k+1) = Ax(k) + bf(x(k)) + c, \tag{1}$$

where $x(k) \in R^n$ is the state vector, $f : R^n \to R$ is a nonlinear vector field, $A \in R^{n\times n}$, $b \in R^{n\times 1}$ and $c \in R^{n\times 1}$ denote constant matrices. A block diagram illustrating the proposed approach is shown in Fig.1. The transmitter is constructed as

$$\begin{aligned} x(k+1) =& Ax(k) + bf(x(k)) + c + b_0\, s(k), \\ y'(k) =& d^{\mathrm{T}}x(k) + Kf(x(k)) + s(k) \\ =& y(k) + s(k), \end{aligned} \tag{2}$$

where $s(k) \in R$ is the information signal masked by the chaotic signal $y(k)$, $y'(k) \in R$ is the signal transmitted to the receiver and the constant matrix b_0 must be selected.

*Project supported by the National Postdoctoral Science Foundation of China and the National Natural Science Foundation of China (Grant No 60404005).

†E-mail: jglu@sjtu.edu.cn

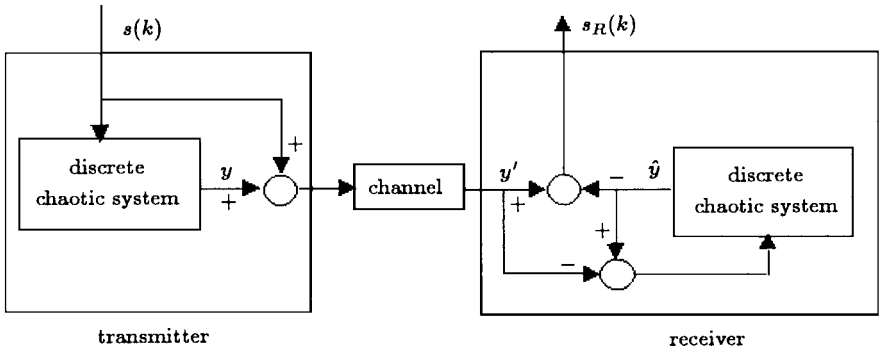


Fig.1. A block diagram illustrating the proposed method.

The receiver is then constructed, which consists of a discrete-time chaotic system described by

$$\begin{aligned}\hat{x}(k+1) =& A\hat{x}(k) + bf(\hat{x}(k)) + b_0(y'(k) - \hat{y}(k)),\\ \hat{y}(k) =& d^{\mathrm{T}}\hat{x}(k) + Kf(\hat{x}(k)),\end{aligned} \tag{3}$$

where $\hat{x}(k) \in R^n$ is the state vector. Defining the synchronization error $e(k) = \hat{x}(k) - x(k)$ and $b_0 = b/K$, $K \neq 0$, we can obtain

$$\begin{aligned}e(k+1) =& \hat{x}(k+1) - x(k+1)\\ =& A\hat{x}(k) + bf(\hat{x}(k)) + b_0(y'(k) - \hat{y}(k))\\ & - Ax(k) - bf(x(k)) - b_0 s(k)\\ =& A\hat{x}(k) + bf(\hat{x}(k)) + b_0(d^{\mathrm{T}}x(k) + Kf(x(k))\\ & + s(k) - d^{\mathrm{T}}\hat{x}(k) - Kf(\hat{x}(k)))\\ & - Ax(k) - bf(x(k)) - b_0 s(k)\\ =& (A - b_0 d^{\mathrm{T}})e(k) + (b - Kb_0)\\ & \times \{f(\hat{x}(k)) - f(x(k))\}\\ =& (A - b_0 d^{\mathrm{T}})e(k)\\ =& (A - bd^{\mathrm{T}}/K)e(k).\end{aligned} \tag{4}$$

From the linear system theory,[13] we know that if all the uncontrollable eigenvalues of the system (A, b), if any, within the unit circle, then there exists d satisfying

$$\left|\lambda_i(A - bd^{\mathrm{T}}/K)\right| < 1, \quad i = 1, 2, \cdots, n$$

such that $e(k) \to 0$. Further, the recovered information signal $s_R(k)$ by the receiver satisfies

$$\begin{aligned}\lim_{t\to\infty} s_R(k) &= \lim_{t\to\infty}(y'(k) - \hat{y}(k))\\ &= \lim_{t\to\infty}(d^{\mathrm{T}}x(k) + Kf(x(k)) + s(k)\\ &\quad - d^{\mathrm{T}}\hat{x}(k) - Kf(\hat{x}(k)))\\ &= s(k).\end{aligned}$$

These results yield the following theorem.

Theorem 1 Let $s_R(k) = y'(k) - \hat{y}(k)$ be the information signal recovered by the receiver. If $b_0 = b/K$, $K \neq 0$ and (A, b) are stabilizable, then we can place all the eigenvalues of $A - bd^{\mathrm{T}}/K$ in the unit circle by a suitable d so that the receiver (3) is a global observer of the transmitter (2) and then $\lim_{k\to\infty} s_R(k) = s(k)$.

3. Extension to multiple-access chaos digital communication

To transmit $\mu \leq n$ digital information signals $m_j(i)$ $(j = 1, 2, \cdots, \mu)$ concurrently, where $m_j(i) \in \{-1, +1\}$, we first modulate the digital information signals $m_j(i)$ by chaotic signals in the transmitter as follows:

$$s(k) = \rho \sum_{j=1}^{\mu} m_j(i)x_j(k), \quad iT \leq k < (i+1)T, \tag{5}$$

where $T \geq \mu > 0$ is a bit interval and $\rho > 0$ is a factor.

Remark 1: To guarantee that the solutions of Eq.(2) remain chaotic, we can appropriately select K and ρ so that the term $b_0 s(k)$ that represents a perturbation to the chaotic system (1) is sufficiently small.

We now consider how to recover the digital information signals in the receiver. After $x(k)$ and $\hat{x}(k)$ evolve in an identical fashion, the following equation holds:

$$\begin{aligned}&\rho \sum_{j=1}^{\mu} m_j(i)\hat{x}_j(k) + e(k) = s(k) + e(k) = s_R(k),\\ &iT \leq k < (i+1)T,\end{aligned} \tag{6}$$

where $e(k) \in R$ is an error which is caused by synchronization error and/or noise on a transmission line. From Eq.(6), the problem to acquire the digital information signals $m_j(i)$ $(j = 1, 2, \cdots, \mu)$ turns to a linear parameter identification problem and we can recover digital information signals on-line by adopting

the on-line least square method which is represented as follows:[14]

$$\begin{aligned}\hat{m}^{N+1}(i) =& \hat{m}^N(i) + K(N+1)[\rho^{-1} \cdot s_R(iT+N) \\ & - x_R^{\mathrm{T}}(iT+N) * \hat{m}^N(i)], \\ P(N+1) =& \frac{1}{\lambda}[P(N) - K(N+1)x_R^{\mathrm{T}}(iT+N)P(N)], \\ K(N+1) =& \frac{P(N)x_R(iT+N)}{\lambda + x_R^{\mathrm{T}}(iT+N)P(N)x_R(iT+N)}, \\ & N = 0, \cdots, T-1, \end{aligned} \tag{7}$$

where

$$x_R(j) = \left[\begin{array}{cccc} \hat{x}_1(j) & \hat{x}_2(j) & \cdots & \hat{x}_\mu(j) \end{array} \right]^{\mathrm{T}},$$

$\hat{m}_j^N(i)(j = 1, \cdots, \mu)$ are the recovered digital information signals, λ is the forgetting factor and usually chosen as a value between 0.95 and 1. The initial value $P(0)$ of the covariance matrix is usually chosen as $P(0) = \alpha \cdot I$ where α is a large positive scale and I is the unit matrix. The initial estimates $\hat{m}^0(i)$ can be taken as zero. To proceed, we need the following lemma from Ref.[14].

Lemma 1 After $x(k)$ and $\hat{x}(k)$ evolve in an identical fashion, if $P(0) = \alpha \cdot I$, $\alpha \gg 1$, $e(k) = 0$, $\lambda = 1$ and $\mathrm{rank}[x_R(iT), x_R(iT+1), \cdots, x_R(iT+\beta-1)] = \mu$ where $\hat{m}(i) \in R^\mu$, then the algorithm (7) will converge to $m(i)$ in β steps.

Since the systems (2) and (3) are chaotic, $x_R(iT)$, $x_R(iT+1), \cdots$, $x_R(iT+\beta-1)$ are linearly independent for $\beta \geq \mu$, i.e. $\mathrm{rank}[x_R(iT), x_R(iT+1), \cdots, x_R(iT+\beta-1)] = \mu$, and then the algorithm (7) will converge to $m(i)$ in β steps. So, the bit interval T should satisfy $T \geq \beta \geq \mu$ and then from the recovered signal $\hat{m}_j(i)$, the binary digital signal $\tilde{m}_j(i)$ can be demodulated as follows:

$$\tilde{m}_j(i) = \begin{cases} +1, & \dfrac{1}{T-\beta+1} \displaystyle\sum_{N=\beta}^{\mathrm{T}} \hat{m}_j^N(i) \geq 0, \\ -1, & \dfrac{1}{T-\beta+1} \displaystyle\sum_{N=\beta}^{\mathrm{T}} \hat{m}_j^N(i) < 0, \end{cases} \tag{8}$$

and the mean of $\hat{m}_j^N(i)$ is approximately equal to $m_j(i)$ for $\beta \leq N \leq T$.

If each user only can use one x_j, then the secure communication system at most can be used for n users and assigns a spread spectrum series for each user. The secure communication system becomes a CDMA system. On the other hand, if one user can use all the x_j, then the communication system is a communication system for "M"-ARY.

4. Simulation results

Consider the Henon map, a second order well-known chaotic system, represented by the following equation:

$$\begin{aligned} x(k+1) &= \left[\begin{array}{cc} 0 & 1 \\ b & 0 \end{array} \right] x(k) + \left[\begin{array}{c} -a \\ 0 \end{array} \right] x_1^2(k) + \left[\begin{array}{c} 1 \\ 0 \end{array} \right] \\ &= Ax(k) + bf(x(k)) + c, \end{aligned} \tag{9}$$

where $A = \left[\begin{array}{cc} 0 & 1 \\ b & 0 \end{array} \right]$, $b = \left[\begin{array}{c} -a \\ 0 \end{array} \right]$, $c = \left[\begin{array}{c} 1 \\ 0 \end{array} \right]$, and $f(x(k)) = x_1^2(k)$. This map exhibits a chaotic behaviour in a large neighbourhood of the parameter values $a = 1.4$, $b = 0.3$. Based on the Henon map (9), we can use above our proposed method to implement multiple-access chaotic digital communication. In testing our proposed method, we chose $\rho = 0.005$, $d^{\mathrm{T}} = [0, \ -0.7143]$ and $K = 1$ so that $\lambda_i(A - bd^{\mathrm{T}}/K) = 0$, $i = 1, 2$. We transmit $\mu = 2$ digital information signals concurrently with $T = 10$ represented by

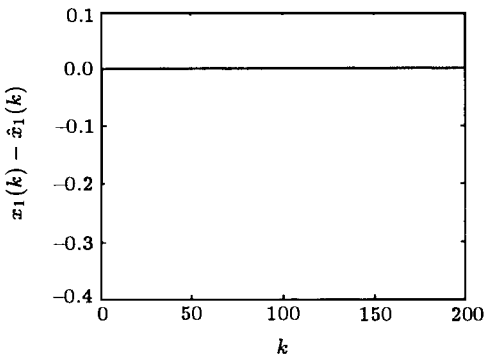
$$m_1 = [\ 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1\ ],$$

$$m_2 = [-1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1\ ].$$

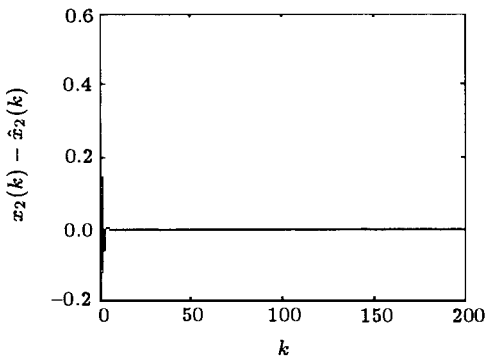
The simulation results are shown in Fig.2, in which (a) and (b) show the state synchronization error between the transmitter (2) and the receiver (3), (c) shows the modulated information signal $s(k)$, (d) shows the recovered information signal $s_R(k)$, and (e) shows the error between $s_R(k)$ and $s(k)$. From Fig.2. we can find that synchronization and communication between (2) and (3) has been achieved. Furthermore, by adopting the on-line least square method (7) and the binary digital signal (8) with $\beta = 5$, we can succeed in demodulating $\mu = 2$ digital information signals concurrently and obtain

$$\tilde{m}_1 = [\ 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1\ ],$$

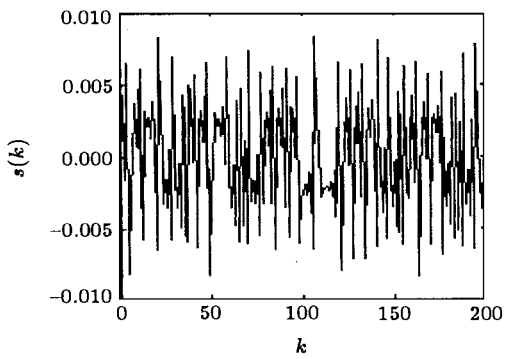
$$\tilde{m}_2 = [-1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1 \quad -1 \quad 1\ ].$$



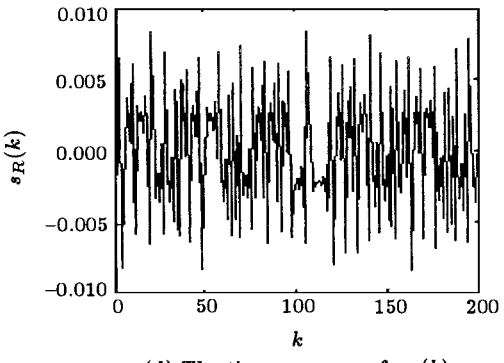
(a) The time response of $x_1(k) - \hat{x}_1(k)$.



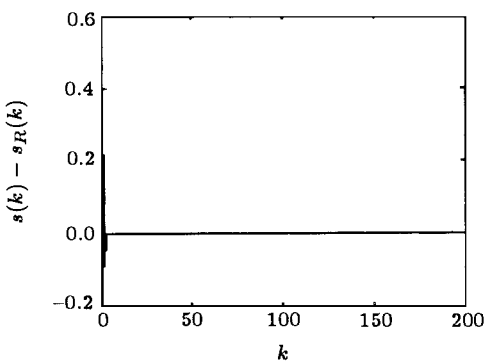
(b) The time response of $x_2(k) - \hat{x}_2(k)$.



(c) The time response of $s(k)$.



(d) The time response of $s_R(k)$.



(e) The time response of $s(k) - s_R(k)$.

Fig.2. Simulation results.

5. Discussion

Now, the advantages of the proposed approach are described as follows.

1) In our chaos communication scheme, chaotic synchronization and communication can be achieved simultaneously via a state observer design technique. This overcomes the drawback in Ref.[10] that the transmitter must repetitiously transmit the synchronization signal before the beginning of each information signal. Moreover, assuming a digital configuration with finite representation in our approach, the problem of parameter mismatching and transmission noise surely appears less critical.

2) Closely examining (2), we can find that the proposed communication scheme combines the chaotic masking with the chaotic modulation. The output $y(k)$ masks the information signal $s(k)$ and modulates the chaotic system. In the conventional chaotic masking method,[10] the receiver is driven by the sum of the encoded information signal and the output of the discrete time chaotic system, whose dynamics is autonomous. However, in the communication system proposed herein, the information signal is also fed back into the discrete time chaotic system. Hence, the dynamics of the transmitter is driven by a time-varying information signal $s(k)$, thereby implying that the transmitter is a nonautonomous system, which is generally more complicated.

3) The suggested approach enables synchronization to be achieved via a scalar transmitted signal. This is a remarkable feature, since a signal channel is usually available for communication applications. [15]

4) If (A, b) is controllable, all the eigenvalues of (4) can be arbitrarily assigned. Moreover, we find out that when $\left|\lambda_i(A - bd^{\mathrm{T}}/K)\right| = 0$, $i = 1, 2, \cdots, n$, the discrete-time chaotic maps can exhibit the appealing property of achieving synchronization in a finite number of steps, i.e. dead-beat synchronization.[10] As a consequence, it is possible to generate chaos communication systems characterized by short synchronization time, in order to avoid losing part of the message during the transient behaviour.

5)Though the proposed method has several advantages, its practical implementation needs to be further investigated.

6. Conclusion

In the paper, an observer is firstly designed to achieve synchronization and secure communication between a transmitter and a receiver. Based on the proposed observer and the on-line least square method, we further present a multiple-access chaotic digital secure communication method which has an ability to transmit a number of digital signals on one transmission line concurrently. To show the effectiveness of the proposed method, simulation results are given. Its practical implementation needs to be further investigated.

References

[1] Chen G R and Dong X N 1998 *From Chaos to Order: Methodologies, Perspectives, and Applications* (Singapore: World Scientific)

[2] Chen G R and Fardkov A L 2001 *Chaos Control and Synchronization Bibliographies* (1987-2001) available via the WWW: http://www.ee.cityu.edu.hk/~gchen/chaos-papers.html

[3] Yang T and Shao H H 2002 *Acta Phys. Sin.* **51** 742 (in Chinese)

[4] Chen S H, Zhao L M and Liu J 2002 *Chin. Phys.* **11** 543

[5] Zhang S H and Shen K 2002 *Chin. Phys.***11** 894

[6] Liao T L and Huang N S 1999 *IEEE Trans. Circuits Syst.* **46** 1144

[7] Wu C J and Lee Y C 2000 *Electron. Lett.* **36** 1842

[8] Terry J R and VanWiggeren G D 2001 *Chaos, Solitons Fractals* **12** 145

[9] Jiang Z P 2002 *IEEE Trans. Circuits Syst.* **49** 92

[10] Angeli A D, Genesio R and Tesi A 1995 *IEEE Trans. Circuits Syst.* **42** 54

[11] Leuciuc A 2000 *IEEE Trans. Circuits Syst.* **47** 82

[12] Huijberts H J C, Lilge T and Nijmeijer H 2001 *Int. J. Bifur. Chaos* **11** 1997

[13] Chen C T 1984 *Linear System Theory and Design* (New York: Holt, Rinehart and Winston)

[14] Goodwin G C and Sin K S 1984 *Adaptive Filtering, Prediction, and Control* (Englewood Cliffs, NJ: Prentice-Hall)

[15] Pecora L M, Carroll T L, Johson G and Mar D 1997 *Phys. Rev.* E **56** 5090