Vol 11 No 11, November 2002
1009-1963/2002/11(11)/1124-04

Chinese Physics

© 2002 Chin. Phys. Soc.
and IOP Publishing Ltd

A secure communication method for a high-power information signal based on chaotic masking

Li Jian-Fen(李建芬) and Li Nong(李 农)

The Engineering Institute of the Air Force Engineering University, Xi'an 710038, *China*

(Received 14 March 2002; revised manuscript received 10 May 2002)

In this paper, we present a secure communication method for a high-power information signal based on chaotic masking. In the transmitter, an adaptive controller is adopted to pick up the change of the information signal, and to inject the controller's error into the transmitting system. At the same time, the information is directly added to the chaotic signal in transmission to drive the receiving system. In the receiver, another adaptive controller is used to maintain chaotic synchronization of the transmitting and receiving systems and to recover the information signal. Since the synchronization error is independent from the information signal, the power of the information signal can be equivalent to that of the chaotic signal, and the frequency of the information signal can be set within the range of the principal frequencies of the chaotic signal. The results of theoretical analysis and numerical simulation show that the presented method not only enhances the degree of security of low-dimensional chaotic systems but also significantly improves the signal-to-noise ratio at the receiving end.

Keywords: chaotic masking, secure communications, adaptive controllers, Chua's circuits
PACC: 0545

1. Introduction

Based on the drive-response synchronization method of Pecora and Carroll,[1,2] Cuono *et al*[3] have proposed a chaos masking secure communication scheme. In order to maintain synchronization between the transmitter and receiver, the ratio of the power of the chaotic carrier to the information signal should be greater than approximately 30dB to guarantee a fairly small distortion on the chaotic attractor. However, this leads to a poor signal-to-noise ratio (SNR) of the recovered information signal and enables the interceptor to discover the information easily by the return map method[4] and the nonlinear forecasting method.[5] By giving one of the variables in a low-dimensional chaotic system, we can properly construct a return map where the dynamics are attracted to an almost one-dimensional (1D) set. In a conventional chaos masking scheme, the power of the information signal is required to be sufficiently lower than that of the chaotic carrier. The added small information can be considered as a kind of distortion on the chaotic trajectory, which results in the deviation of the map point from the original silent attractor, i.e., the segments are broadened into diffuse stripes. The information can be extracted by measuring the distance between the present positions of the points in the attractor and the places they should have appeared in the absence of a message, and by taking into account to which side of it the point has moved.

There are many methods[6−10] to improve the security of chaotic communication. The chaos masking method based on unidirectional-coupled synchronization in Refs.[6] and [7], to some extent, enhances the degree of security,[11] as the message is not only just added to the chaotic carrier signal to drive the receiver but is also injected into the transmitter to modulate the carrier. To maintain the chaotic state of the transmitter when this method is applied, the power of the information signal is much lower than that of the chaotic carrier, so the SNR of the received signal is still poor. Thereby a chaos masking method for a high-amplitude information signal has been shown in Ref.[12], in which an adaptive controller maintains the synchronization of transmitting and receiving systems and recovers the information signal. However, this is only suitable to a much lower frequency of information signal with respect to the chaotic carrier, due to the synchronization error relating to the rate of change of the information signal.

We have developed a chaotic masking method for secure communication based on Ref.[12], in which an additional adaptive controller is used in the transmitter to trace the variation of the information signal,

and the controller's error is injected into the transmitting system. Hence, the power of the information signal can be equivalent to that of the chaotic signal and the frequency of the information signal can be set within the principal frequencies of the chaotic oscillation. Chua's circuit is considered as an illustrative example to demonstrate the effectiveness of this method. The results of theoretical analysis and numerical simulation show that this method improves efficiently the security of low-dimensional chaotic systems.

2.Secure communication scheme based on chaotic masking

The dimensionless equations of state for Chua's circuit[13] are given by

$$\dot{\boldsymbol{x}} = A\boldsymbol{x} + Df(x_1)$$

$$= \begin{bmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{bmatrix} \boldsymbol{x} + \begin{bmatrix} -\alpha \\ 0 \\ 0 \end{bmatrix} f(x_1),$$

where $\boldsymbol{x} \in R^3$ is the state vector, $A \in R^{3\times 3}$ and $D \in R^{3\times 1}$ are coefficient matrices, and $f(*)$ is a nonlinear function defined by

$$f(x_1) = bx + 0.5(a-b)[|x_1+1| - |x_1-1|],$$

where a and b are normalized slopes of a piecewise linear function.

A secure communication scheme presented based on Chua's circuit is shown in Fig.1. The equations of state are

$$\begin{cases} \dot{\boldsymbol{x}} = A\boldsymbol{x} + Df(x_1) + K(s(t) - k_{d1}), \\ \dot{k}_{d1} = \mu(s(t) - k_{d1}), \quad \text{for transmitter, and} \\ y = x_1 + s(t); \end{cases} \tag{1}$$

$$\begin{cases} \dot{\boldsymbol{x}}' = A\boldsymbol{x}' + Df(x_1') + K(y - y'), \\ \dot{y}' = x_1' + k_{d2}, \quad \text{for receiver,} \\ \dot{k}_{d2} = \mu(y - y'), \end{cases} \tag{2}$$

where $s(t)$ is the information signal, x_1 and x_1' are the first components of $\boldsymbol{x}$ and $\boldsymbol{x}'$ respectively, $K = [k\ 0\ 0]^{\mathrm{T}}$ is a feedback coefficient matrix, k_{d1} and k_{d2} are the gain of adaptive controllers connected with the transmitter and receiver respectively, which are similar to the LMS adaptive controller, and μ is a constant for controlling speed and stability.

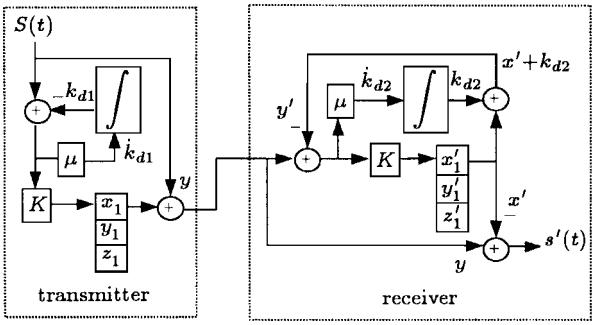

Fig.1. Block diagram of the secure communication scheme.

Equations (1) and Fig.1 show that the signal injected into the transmitter is the error of $s(t)$ and $k_{d1}(t)$ instead of $s(t)$. So, if the amplitude of $s(t) - k_{d1}(t)$ is much lower than that of the chaotic signal, the transmitter will remain in a chaotic state. We assume

$$\boldsymbol{e}(t) = \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix} = \begin{bmatrix} x_1 - x_1' \\ x_2 - x_2' \\ x_3 - x_3' \\ k_{d1} - k_{d2} \end{bmatrix}.$$

From Eqs.(1) and (2), the synchronization error equations are given by

$$\dot{\boldsymbol{e}}(t) = \begin{bmatrix} -\alpha - k & \alpha & 0 & -k \\ 1 & -1 & 1 & 0 \\ 0 & -\beta & -\gamma & 0 \\ -\mu & 0 & 0 & -\mu \end{bmatrix} \boldsymbol{e}$$

$$+ \begin{bmatrix} -\alpha \\ 0 \\ 0 \\ 0 \end{bmatrix} (f(x_1) - f(x_1'))$$

$$= A_f\boldsymbol{e} + B(f(x_1) - f(x_1')).$$

Because $f(*)$ is a piecewise linear continuous function, whose slopes are a and b ($a < b < 0$), then $a(x_1 - x_1') \le f(x_1) - f(x_1') \le b(x_1 - x_1')$.

If $f(x_1) - f(x_1') = \delta(t)(x_1 - x_1')$ ($\delta(t)$ is a time-varying parameter, and $a < \delta < b$), then $\dot{\boldsymbol{e}}(t)$ may be written as

$$\dot{\boldsymbol{e}}(t) = \begin{bmatrix} -\alpha(1+\delta) - k & \alpha & 0 & -k \\ 1 & -1 & 1 & 0 \\ 0 & -\beta & -\gamma & 0 \\ -\mu & 0 & 0 & -\mu \end{bmatrix} \boldsymbol{e} = A(t)\boldsymbol{e}. \tag{3}$$

Equations (3) are time-varying homogeneous linear equations, in which δ can be approximated as a constant since the oscillating trajectory of Chua's circuit

lies in the range of $|x_1| > 1$ most of the time (as shown in Fig.2). Then, Eqs.(3) can be approximated as homogeneous linear equations with constant coefficients, and the eigenvalues of matrix A will be negative real parts when k and μ are properly selected. By numerical calculation, the chaotic synchronization, i.e. $\boldsymbol{e}(t) \to 0$, can be achieved when the values of k and μ satisfy the condition of $k > 5$, $\mu > 5$ and $k/\mu \in (0.5\text{–}1)$. The information signal $s(t)$ can be recovered by inverse transformation $s'(t) = y - x_1'$.

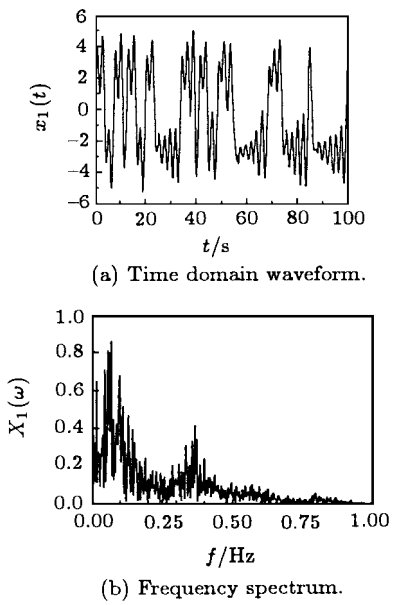

Fig.2. Time domain waveform and frequency spectrum of the chaotic signal.

The parameters chosen for numerical simulation are α=10, β=14.31, γ=0.12, a=–1.39, b=–0.75, μ=10, k=20; with these parameters we obtain Chua's double scroll strange attractor. The information $s(t)$ is a square waveform signal. Figures 2–4 show the results of numerical simulation with MATLAB. Obviously, the fundamental frequency of the information signal is within the centre frequency band of the chaotic signal.

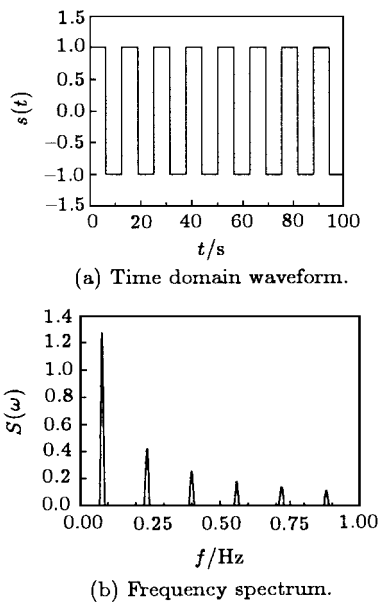

Fig.3. Time domain waveform and frequency spectrum of the information signal.

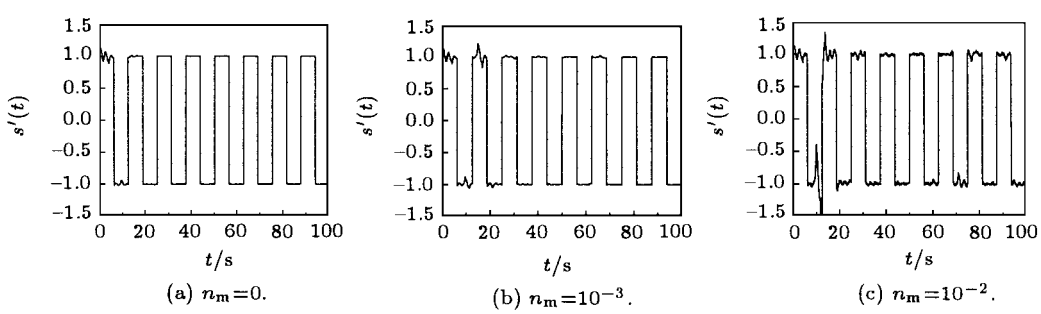

Fig.4. Information signal recovered at different noise amplitude n_{m}.

3. Noise resistance analysis

The transmitted signal through a noisy channel corrupted with an additive Gaussian white noise $n(t)$ is represented as $y = x_1 + s(t) + n(t)$. Then the synchronization error equations should be written as

$$\dot{\boldsymbol{e}}(t) = \begin{bmatrix} -\alpha(1+\delta) - k & \alpha & 0 & -k \\ 1 & -1 & 1 & 0 \\ 0 & -\beta & -\gamma & 0 \\ -\mu & 0 & 0 & -\mu \end{bmatrix} \boldsymbol{e} + \begin{bmatrix} -k \\ 0 \\ 0 \\ -\mu \end{bmatrix} n(t) = A(t)\boldsymbol{e} + C^{\mathrm{T}} n(t). \tag{4}$$

The equations are non-homogeneous linear equations with constant coefficients, whose solution can be written in the following form

$$\boldsymbol{e}(t) = \boldsymbol{e}^{At}\boldsymbol{e}(o) + \int_0^{\tau} \boldsymbol{e}^{A(t-\tau)} C^{\mathrm{T}} n(\tau) \mathrm{d}\tau. \qquad (5)$$

It is obvious that the first term in Eq.(5) converges exponentially towards zero at $t \to \infty$, so the synchronization error is determined by the second term in Eq.(5). If the construction of chaotic systems is given, the synchronization error can only be reduced with noise reduction. Figure 4 shows the information signal recovered at the receiving end at different noise amplitudes (n_{m}).

We take $n_{\mathrm{m}} = 10^{-3}$ as an example. If the information signal can still be correctly recovered by conventional chaotic masking scheme constructed with Chua's circuit, then the SNR is less than 38dB. The reason is that the average power of chaotic signal is approximately 8dB and the power of the chaotic signal should be approximately 30dB greater than that of the information signal. By using the method presented in this paper, however, the SNR is more than 60dB.

4. Security analysis

By using the method in this paper, the signal injected into the transmitter is the error between $s(t)$ and $k_{d1}(t)$. The transmitted signal $y = x_1 + s(t)$ is modulated two times. Therefore, the hidden information signal added to the chaotic carrier at a high power makes it difficult to recover the hidden signal by the return map method.[14] Figure 5 shows the return maps of the chaotic signal $x_1(t)$ and transmitted signal $y(t)$. Clearly, the interceptor can hardly discover the hidden information from $y(t)$ by nonlinear noise reduction.

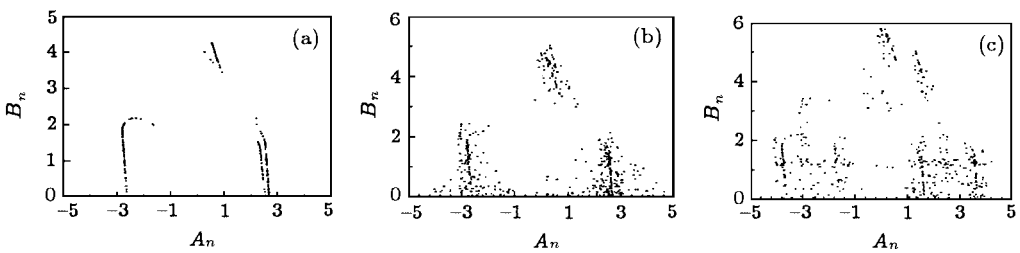

Fig.5. Return maps of chaotic signal x_1 and transmitted signal y: (a) return map of silent chaotic signal x_1; (b) return map of chaotic signal x_1 modulated by error; (c) return map of transmitted signal y.

5. Conclusion

The method presented in this paper is characterized with a high degree of security and is easily implemented in practice. Because of the high-power information signal, the SNR of the signal decoded at the receiving end is high.

References

[1] Pecora L M and Carroll T L 1990 *Phys. Rev. Lett.* **64** 821

[2] Pecora L M and Carroll T L 1991 *Phys. Rev.* A **44** 2374

[3] Cuomo K M and Oppenheim A V 1993 *Phys. Rev. Lett.* **71** 65

[4] Perez G and Cerdeira H A 1995 *Phys. Rev. Lett.* **74** 1970

[5] Short K M 1994 *Int. J. Bifurcation Chaos* **4** 959

[6] Liu F, Chen X L, Mu Zh L and Qiu Z L 2000 *Acta Electron Sin.* **28** 46 (in Chinese)

[7] Liao T L and Huang N S 1999 *IEEE Trans. CAS-I* **46** 1144

[8] Dai M, Zhang Y, Hua Y M and Ni W S 1999 *Chin. Phys.* **8** 308

[9] Kuang J Y, Deng K and Huang R H 2001 *Acta Phys. Sin.* **50** 1856 (in Chinese)

[10] Zhang J S and Xiao X C 2001 *Acta Phys. Sin.* **50** 2121 (in Chinese)

[11] Zhou C S and Lai C 1999 *Phys. Rev.* E **60** 320

[12] Li J F and Li N 2002 *Syst. Eng. Electron.* **24** (4) 41 (in Chinese)

[13] Kennedy M P 1993 *IEEE Trans. CAS-I* **40** 657

[14] He Z Y, Li K, Yang L X and Shi Y H 2000 *IEEE Trans. CAS-I* **47** 397