连续时延耦合系统的混沌同步及其在保密通信中的应用*

张 俊，周尚波
（重庆大学 计算机学院，重庆 400044）

摘 要：研究了具有连续时延双神经元系统的双向耦合混沌同步问题及在扩展频谱保密通信中的应用。利用 Krasovskii-Lyapunov 理论，给出了系统同步的一个充分条件，通过选择合适的耦合参数可以保证全局混沌同步。给出了使用混沌掩码技术在扩展频谱保密通信中的应用实例。

关键词：混沌同步 神经元 保密通信 连续时延

Synchronization of coupled continuous time-delay chaotic system and its application to secure communications

ZHANG Jun, ZHOU Shang Bo
(College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: The chaotic synchronization between two time delayed neuron chaotic systems with linearly bi-directional coupling and to its application of spread spectrum secure communications are studied. Some generic criterion is developed for choosing the appropriate coupling parameters to ensure global chaotic synchronization based on Krasovskii-Lyapunov theory. Finally, an application example is given, which uses the proposed chaotic system to realize spread spectrum secure communications based on the chaotic masking strategy.

Key words: choatic synchronization, neuron, secure communications, continuous time-delay

自从 Pecora 和 Carroll[1-2]在 1990 年实现了混沌系统的完全同步化以来，对同步的研究在通信、控制、神经科学等许多领域引起了学者们的广泛兴趣[3-6]，同步的概念也被加以推广，如广义同步、相位同步、延迟同步、反向同步等。近年来，混沌系统的控制和同步研究[7]及在保密通信中的应用[8]成为新的热点。但人们发现，由低维动力学系统产生的混沌而构造的保密通信系统其保密性是脆弱的[9]，例如使用非线性动力学预测或回归映射方法[10]，以及使用神经网络方法[11]等，都可以重构混沌系统，以对信息进行解密。由此使人们想到利用高维动力学系统产生超混沌，使正的 Lyapunov 指数个数大于 1，以提高保密性能。

混沌是人脑和人工神经网络的一个基本运行模式，它在神经网络的记忆、模式识别等过程中起着重要的作用。但是一个值得注意的事实是：混沌对初始条件非常敏感，即使两个神经元的初始条件非常接近，它们的状态很快会变的毫不相干，并且发现在生物系统中，两个神经元之间发生的短暂时延是很正常的，对神经元之间的信息传递也是至关重要的。因此，时延在混沌系统中的影响和作用引起了人们的广泛注意。研究表明[12-13]，带时延的混沌系统能表现出很好的超混沌特性，被认为是一种有效的加密工具。

本文研究的是具有连续时延双神经元耦合系统的混沌同步问题。

1 系统描述

考察如下的时延神经元方程[14]：

$$\frac{dy(t)}{dt}=-y(t)+a\tanh[y(t)-by(t-\tau)+c] \tag{1}$$

设 $c=0, x(t)=y(t)-by(t-\tau)$，且用任一函数 $f(\cdot)$ 代替 $\tanh(\cdot)$，有如下方程：

$$\dot{x}(t)=-x(t)+a(f(x(t))-bf(x(t-\tau))) \tag{2}$$

实际上，这是个单时延的神经元方程式，它的动力学行为和分岔现象已经被仔细研究过[15]。本文主要考虑的是具有连续时间延时的双神经元方程：

* 中国博士后科学基金资助项目（2004035524）

$$\begin{cases}\dot{x}_1(t)=-x_1(t)+a_1f(x_2(t))-a_1b_1f(x_2(t-\tau(t)))\\ \dot{x}_2(t)=-x_2(t)+a_2f(x_1(t))-a_2b_2f(x_1(t-\tau(t)))\end{cases}\quad(3)$$

接下来，考虑系统(3)式的双向耦合同步问题。

$$\begin{cases}\dot{x}_1(t)=-x_1(t)+a_1f(x_2(t))-a_1b_1f(x_2(t-\tau(t)))-k_1(x_1(t)-y_1(t)) & \text{(a1)}\\ \dot{x}_2(t)=-x_2(t)+a_2f(x_1(t))-a_2b_2f(x_1(t-\tau(t)))-k_2(x_2(t)-y_2(t)) & \text{(a2)}\end{cases}\quad(4a)$$

$$\begin{cases}\dot{y}_1(t)=-y_1(t)+a_1f(y_2(t))-a_1b_1f(y_2(t-\tau(t)))-k_1(y_1(t)-x_1(t)) & \text{(b1)}\\ \dot{y}_2(t)=-y_2(t)+a_2f(y_1(t))-a_2b_2f(y_1(t-\tau(t)))-k_2(y_2(t)-x_2(t)) & \text{(b2)}\end{cases}\quad(4b)$$

式中，x_i 和 $y_i(i=1,2)$ 是状态变量，$k_i(i=1,2)$ 是耦合系数。

记 $e_1(t)=x_1(t)-y_1(t)$，$e_2(t)=x_2(t)-y_2(t)$。由(4a)及(4b)得到如下双神经元的双向耦合混沌同步系统：

$$\begin{cases}\dot{e}_1(t)=-(1+2k_1)e_1(t)+a_1(f(x_2(t))-f(y_2(t)))\\ \qquad -a_1b_1(f(x_2(t-\tau(t)))-f(y_2(t-\tau(t))))\\ \dot{e}_2(t)=-(1+2k_2)e_2(t)+a_1(f(x_1(t))-f(y_1(t)))\\ \qquad -a_2b_2(f(x_1(t-\tau(t)))-f(y_1(t-\tau(t))))\end{cases}\quad(5)$$

为了方便，设

$$e=\begin{bmatrix}e_1(t)\\ e_2(t)\end{bmatrix},\ F(t)=\begin{bmatrix}a_2(f(x_2(t))-f(y_2(t)))\\ a_1(f(x_1(t))-f(y_1(t)))\end{bmatrix},$$

$$F(t-\tau(t))=\begin{bmatrix}-a_1b_1(f(x_2(t-\tau(t)))-f(y_2(t-\tau(t))))\\ -a_2b_2(f(x_1(t-\tau(t)))-f(y_1(t-\tau(t))))\end{bmatrix},$$

$$A=\begin{bmatrix}-(1+2k_1) & 0\\ 0 & -(1+2k_2)\end{bmatrix}$$

则(5)式，可写成：

$$\dot{e}=Ae+F(t)+F(t-\tau(t))\quad(6)$$

于是，耦合同步问题就转化为(6)式的稳定性问题。

2 同步控制理论研究

如果误差系统式(6)全局稳定，则系统式(4a)和式(4b)同步。以下将根据 Krasovskii-Lyapunov 理论求出误差系统式(6)的全局稳定性条件。

定理 1 设 $\boldsymbol{P}$ 是一个对称正定矩阵，$|f'(\cdot)|<M$ $(M<\infty)$，且 $|\dot{\tau}(t)|\le\tau_m<1$，如果存在一个常数 $\beta>0$，使得：

$$Q_1=\boldsymbol{P}A+\beta\boldsymbol{P}+\frac{1}{2}I+M\boldsymbol{P}^{\mathrm{T}}\boldsymbol{P}<0,\ Q_2=I-2\beta\boldsymbol{P}(1-\tau_m)\le 0$$

则误差系统式(6)是全局稳定的，即耦合系统式(4a)与式(4b)同步。

证明：定义 Lyapunov 函数如下：

$$V(t)=\frac{1}{2}e^{\mathrm{T}}\boldsymbol{P}e+\beta\int_{-\tau}^{0}e^{\mathrm{T}}(t+\theta)\boldsymbol{P}e(t+\theta)d\theta$$

对函数 $V(t)$ 求导数，并结合(6)式，得到：

$$\dot{V}(t)=\frac{1}{2}\dot{e}^{\mathrm{T}}\boldsymbol{P}e+\frac{1}{2}e^{\mathrm{T}}\boldsymbol{P}\dot{e}+\beta(e^{\mathrm{T}}\boldsymbol{P}e-e^{\mathrm{T}}(t-\tau(\tau))\boldsymbol{P}e(t-\tau(\tau))(1-\dot{\tau}(t)))$$

$$=\frac{1}{2}e^{\mathrm{T}}A^{\mathrm{T}}\boldsymbol{P}e+\frac{1}{2}e^{\mathrm{T}}\boldsymbol{P}Ae+[F^{\mathrm{T}}(t)+F^{\mathrm{T}}(t-\tau(t))]\boldsymbol{P}e+\beta e^{\mathrm{T}}\boldsymbol{P}e$$

$$-\beta e^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e(t-\tau(t))(1-\dot{\tau}(t))$$

$$=e^{\mathrm{T}}[\boldsymbol{P}A+\beta\boldsymbol{P}]e+F^{\mathrm{T}}(t)\boldsymbol{P}e+F^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e-\beta e^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e(t-\tau(t))(1-\dot{\tau}(t))$$

$$\le e^{\mathrm{T}}[\boldsymbol{P}A+\beta\boldsymbol{P}]e+M\|e\|\|\boldsymbol{P}e\|+M\|e(t-\tau(t))\|\boldsymbol{P}e-\beta e^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e(t-\tau(t))(1-\dot{\tau}(t))$$

$$\le e^{\mathrm{T}}[\boldsymbol{P}A+\beta\boldsymbol{P}]e+\frac{1}{2}(\|e\|^2+M\|\boldsymbol{P}e\|^2)+\frac{1}{2}[\|e(t-\tau(t))\|^2+M\|\boldsymbol{P}e\|^2]-\beta e^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e(t-\tau(t))(1-\dot{\tau}(t))$$

$$\le e^{\mathrm{T}}[\boldsymbol{P}A+\beta\boldsymbol{P}]e+\frac{1}{2}(\|e\|^2+M\|\boldsymbol{P}e\|^2)+\frac{1}{2}[\|e(t-\tau(t))\|^2+M\|\boldsymbol{P}e\|^2]-\beta e^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e(t-\tau(t))(1-\tau_m)$$

$$=e^{\mathrm{T}}[\boldsymbol{P}A+\beta\boldsymbol{P}]e+\frac{1}{2}e^{\mathrm{T}}e+\frac{1}{2}Me^{\mathrm{T}}\boldsymbol{P}^{\mathrm{T}}\boldsymbol{P}e+\frac{1}{2}Me^{\mathrm{T}}\boldsymbol{P}^{\mathrm{T}}\boldsymbol{P}e+\frac{1}{2}e^{\mathrm{T}}(t-\tau(t))e(t-\tau(t))-\beta e^{\mathrm{T}}(t-\tau(t))\boldsymbol{P}e(t-\tau(t))(1-\tau_m)$$

$$=e^{\mathrm{T}}[\boldsymbol{P}A+\beta\boldsymbol{P}+\frac{1}{2}I+M\boldsymbol{P}^{\mathrm{T}}\boldsymbol{P}]e+e^{\mathrm{T}}(t-\tau(t))[\frac{1}{2}I-\beta P(1-\tau_m)]e(t-\tau(t))$$

$$=e^{\mathrm{T}}Q_1e+e^{\mathrm{T}}(t-\tau(t))Q_2e(t-\tau(t))<0$$

这里，$e=\begin{bmatrix}e_1(t)\\ e_2(t)\end{bmatrix}$，$e(t-\tau(t))=\begin{bmatrix}e_1(t-\tau(t))\\ e_2(t-\tau(t))\end{bmatrix}$，$\|e\|^2=e^{\mathrm{T}}e$

为了便于使用，设 $P=I$，然后得出如下推论。

推论 1 如果存在一个常数 $\beta\ge\frac{1}{2(1-\tau_m)}$，并且令 $|f'(\cdot)|<M(M<\infty)$，则 $A<-(\beta+\frac{1}{2}+M)I$，于是系统式(6)是全局稳定的，也就是说耦合系统式(4a)与式(4b)是同步的。

3 计算机仿真实验

对系统式(4a)和式(4b)进行同步仿真实验，以验证理论的正确性。

设 $\tau(t)=(2+0.5\sin(4.7t))/5$，$\tau_m=0.5$，$f(t)=\tanh(1.7t)$，$a_1=2.6$，$b_1=3.8$，$a_2=1.71$，$b_2=0.61$。当耦合强度 $k_1=k_2=0$ 时，系统处于非耦合状态。系统式(4)取初值 $x_1(t)=0.5$，$x_2(t)=-0.71$，$y_1(t)=-2.16$，$y_2(t)=-1.13$，驱动系统的状态变量演化曲线见图 1，系统的状态相图见图 2，系统表现出混沌特性。

根据推论 1，$M=1.7$，取 $\beta\ge\frac{1}{2(1-\tau_m)}=1$，则有：

$$A=\begin{bmatrix}-(1+2k_1) & 0\\ 0 & -(1+2k_2)\end{bmatrix}<-(1+\frac{1}{2}+1.7)I$$

于是，只要 $k_i>1.1(i=1,2)$，耦合系统即可同步。现取耦合强度 $k_1=k_2=1.5>1.1$。耦合系统的状态演化曲线如图 3 所示。耦合系统的同步误差曲线如图 4 所示。结果表明，误差 $e_1(t)=x_1(t)-y_1(t)$ 和 $e_2(t)=x_2(t)-y_2(t)$ 经过短暂瞬态后很快衰减到零，系统同步渐进稳定，实验与理论分析相一致。

4 在扩展频谱保密通信中的应用实例

本节将讨论耦合连续时延混沌系统在扩展频谱保

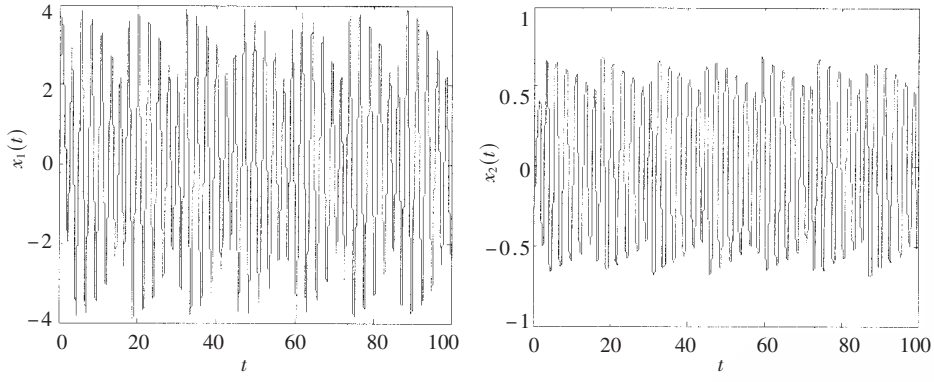


图 1 驱动系统的状态演化曲线($k_1=k_2=0$)

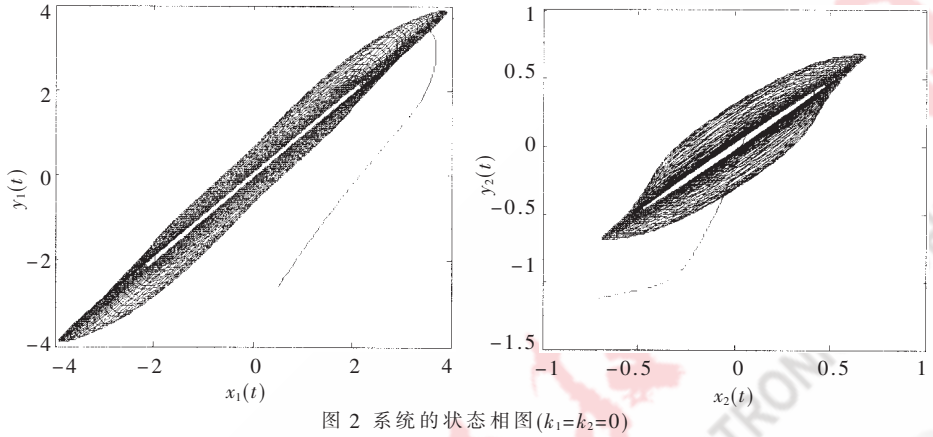


图 2 系统的状态相图($k_1=k_2=0$)

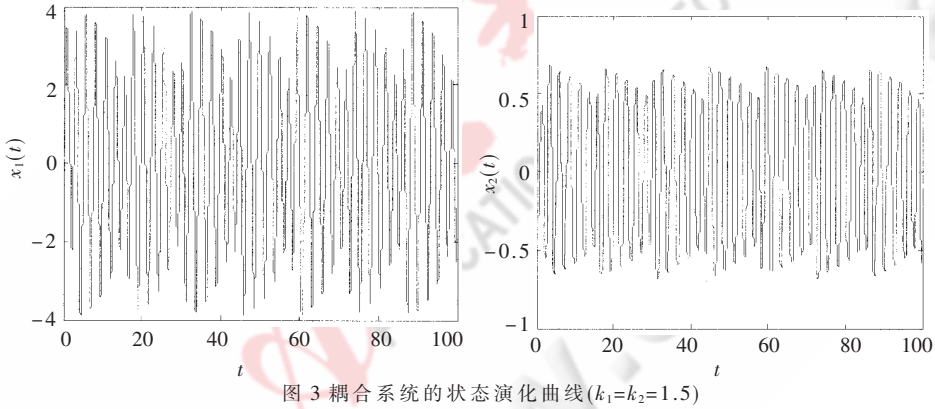


图 3 耦合系统的状态演化曲线($k_1=k_2=1.5$)

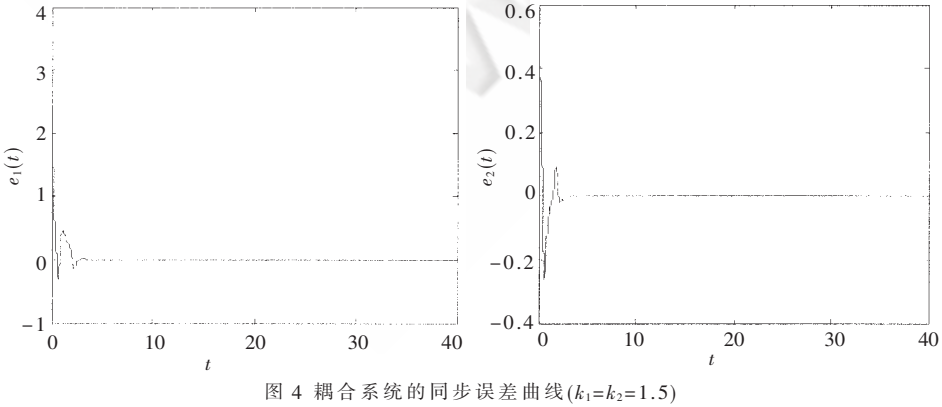


图 4 耦合系统的同步误差曲线($k_1=k_2=1.5$)

密通信中的应用。以系统式(4a)中(a1)式为发送端;以系统式(4b)中(b1)式为接受端。采用混沌掩码扩频技术,设 $s(x)$为消息信号,用 $\varepsilon s(x)$来驱动发送端:

$$\dot{x}_1(t)=-x_1(t)+a_1 f(x_2(t))-a_1 b_1 f(x_2(t-\tau(t)))-k_1(x_1(t)-y_1(t))+k_1\varepsilon s(t) \quad (7)$$

其中 ε 为一个相对较小的正数。传输信号为 $s_x(t)=x_1(t)+\varepsilon s(x)$,于是接收端方程为:

$$\dot{y}_1(t)=-(1+k)y_1(t)+a_1 f(y_2(t))-a_1 b_1 f(y_2(t-\tau(t)))+k_1 s_x(t) \quad (8)$$

收发双方经过短暂瞬态后即可达到同步,此时恢复信号为:

$$\hat{s}(t)=[s_x(t)-y_1(t)]/\varepsilon \quad (9)$$

下面以正弦信号 $s(t)=\sin(t)$为消息信号进行实验。图 5 给出了在计算机上的仿真结果。

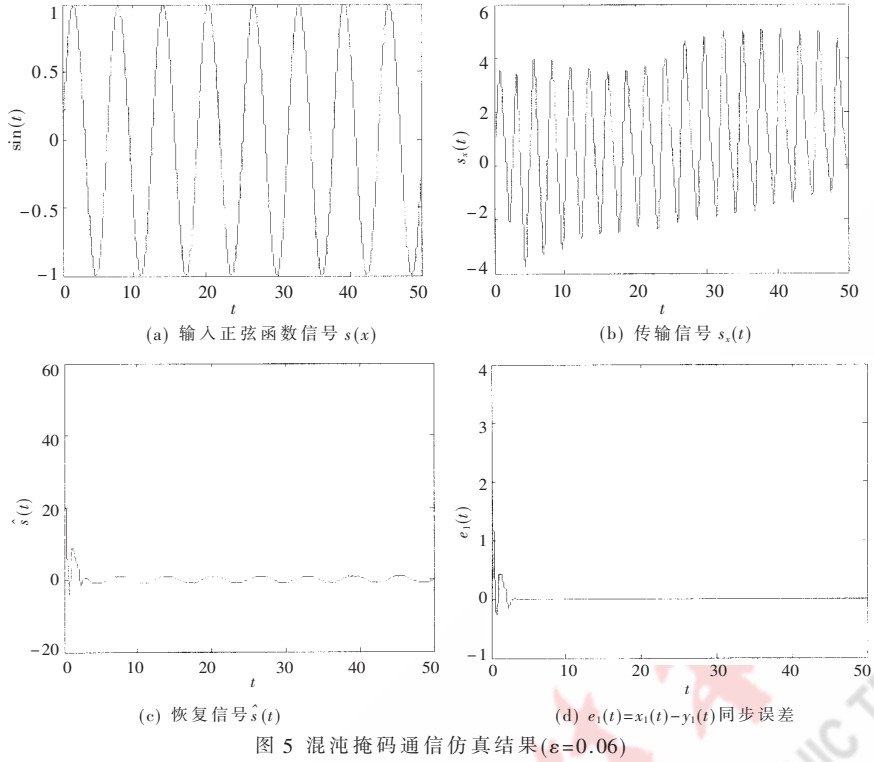
从实验结果可知,传输信号$s_x(t)$是一种类似高斯白噪声的宽频谱超混沌信号,并直接驱动接收端方程,而且由耦合同步理论知,收发双方的系统状态初值不要求相同。由图 5(c)可知,在接收端恢复的消息信号和发送端传送的消息信号精确一致,说明该方案确实可用于实际扩频保密通信系统。同时由于传输信号的超混沌特性,非法接收者难以从截获的信号中解调出消息信号,使得通信系统具有很高的保密性能。需要指出的是,发送端和接收端之间的同步只需传输一个驱动标量信号,即传输信号 $s_x(t)$,降低了通信开销,并能保证通信的安全性和可靠性。

本文研究了双向耦合的连续时延双神经元系统的混沌同步问题,并给出了混沌同步的一个充分条件。在给定的耦合强度范围内,仿真结果与理论分析是一致的,系统达到了较为满意的同步效果。扩展频谱保密通信的应用实例的仿真结果证明本文给出的耦合混沌通信系统具有高的安全性、可靠性、保密性。

参考文献

[1] PECORA L M, CARROLL T L. Synchronization in chaotic systems[J]. Phys. Rev. Lett.,1990,64(8):821-824.

[2] PECORA L M, CARROLL T L. Driving systems with



(a) 输入正弦函数信号 $s(x)$　(b) 传输信号 $s_x(t)$

(c) 恢复信号 $\hat{s}(t)$　(d) $e_1(t)=x_1(t)-y_1(t)$ 同步误差

图 5 混沌掩码通信仿真结果(ε=0.06)

chaotic signals[J]. Phys. Rev. A,1991,44(4):2374-2384.

[3] CUOMO K M, OPPENHEIM A V. Circuit implementation of synchronized chaos with applications to communications [J]. Phys. Rev. Lett.,1993,71(1):65-68.

[4] JIANWEI S, DURAND D M. Phase synchronization in two coupled neurons[J]. Phys. lett. A,1999,264(10):289-296.

[5] DAIHAI H, SHI Peng Liang, STONE L. Noise-induced synchronization in realistic models[J]. Phys. Rev. E, 2003,67(2):0272011-0272013.

[6] 关新平, 范正平, 陈彩莲,等.混沌控制及其在保密通信中的应用[M]. 北京:国防工业出版社,2002.

[7] ZHOU S B, LIAO X F, YU J B, et al. Chaos and its synchronization in two-neuron systems with discrete delays[J]. Chaos, Solitions & Fractals,2004,21(1):133-142.

[8] 彭军, 廖晓峰, 吴中福,等. 一个时延混沌系统的耦合同步及其在保密通信中的应用[J]. 计算机研究与发展,2003,40(2):263-268.

[9] 周红, 凌燮亭. 混沌保密通信原理及其保密性分析[J].电路与系统学报,1996,1(3):57-62.

[10] PEREZ G, CERDEIRA H A. Extracting messages masked by chaos[J]. Phys. Rev. Lett.,1995,74(11):1970-1973.

[11] YANG T, LIN B Y, CHUN M Y. Application of neural networks to unmasking chaotic secure communication[J]. Phys. D,1998,124(1~3):248-257.

[12] MENSOUR B, LONGTIN A. Synchronization of delaydifferential equations with application to private communication[J]. Phys. Lett. A,1998,244(1):59-70.

[13] TIAN Yu Chu, GUO Fu Rong.Adaptive control of chaotic continuous-time systems with delay[J]. Phys. D,1998,117(1):1-12.

[14] GOPALSMAY K, LEUNG K C. Conerugence under dynamical thresholds with delays[J]. IEEE Trans.on Neural Networks,1997,8(2):341-348.

[15] LIAO X F, WONG K-W, LEUNG C-S,et al. Hopf bifurcation and chaos in a single delayed neuron equation with non-monotonic activation function[J]. Chaos, Solitons & Fractals,2001,12(8):1535-1547.

(收稿日期:2007-03-26)