第 54 卷 第 9 期 2005 年 9 月
1000-3290/2005/54(09)/4012-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.9,September,2005

混沌神经网络逆控制的同步及其在保密通信系统中的应用*

于灵慧　房建成

(北京航空航天大学第五研究室,北京　100083)

(2004 年 9 月 30 日收到;2004 年 12 月 17 日收到修改稿)

利用神经网络的学习、逼近能力构造混沌神经网络,提出逆控制混沌同步方法来同步两个混沌神经网络,并基于逆控制和混沌神经网络的同步给出一种新的混沌保密通信系统.理论分析和数值实验结果表明,新系统能够有效地克服信道噪声对信息传输的不良影响,具有较强通用性和柔韧性,且有同步速度快,信号恢复精度高和密钥量大的优点.

关键词:混沌同步,自适应逆控制,混沌神经网络,保密通信

PACC:0545

1. 引　　言

混沌在信息处理中的作用是一个非常值得研究的课题,这一方面是由于混沌这种奇异现象的丰富的工程内涵,另一方面因受到 Freeman 等[1—4]对人脑和动物大脑中动态混沌作用及丰富的实验结果使人们认识到利用混沌实现信息处理的坚强的生物学背景.混沌信号最本质的特性是对初始条件极为敏感,并由此导致了混沌信号的类随机特性.用它作为载波调制出来的信号当然也具有类随机特性.因而,调制混沌信号即使被敌方截获,也很难破译,这就为混沌应用于保密通信提供了有利条件.由于混沌信号又具有整体稳定性,当用同一个混沌信号去驱动两个相同的系统时,两个系统的某些部分将产生同步化的行为,这就为混沌应用于通信(特别是保密通信)提供了可行性.

混沌同步在各个领域,特别是在保密通信中具有潜在的巨大应用前景已引起了人们广泛的研究兴趣[5—10].1983 年 Tang 将同步与混沌联系起来,1993 年 Cuomo 和 Oppenheim 用电阻、电容和运算放大器 Opamp 综合出一个鲁棒性很强的同步混沌电路[5],并进行了信息隐蔽调制—解调(加减调制—解调)的计算机仿真,10 多年来,同步混沌的研究取得了突飞猛进的发展,使得混沌通信走向了应用研究的前沿.

本文利用神经网络的学习,逼近能力构造混沌神经网络,基于逆控制原理提出了混沌神经网络逆控制混沌同步方法来同步两个混沌神经网络,采用数字保密通信方式,给出了一种新的混沌保密通信系统.新系统具有较强的通用性和柔韧性,且同步速度快,信号恢复精度高和密钥量大等优点.

2. 混沌神经网络的构造

网络中每个神经元的动力学行为可由下列方程描述:

$$y(t+1) = ky(t) - \alpha g[f(y(t))] + \theta(t), \quad (1)$$

$y(t+1)$为神经元在 $t+1$ 时刻的状态,k 为衰减因子,α 为正的参数,f 为输出函数,其表达式为具有陡度参数 ε 的 Logistic 的函数 $f(y) = 1/(1+e^{-y/\varepsilon})$,$\theta(t)$为与外部输入有关的阈值.神经元的输出 $x(t+1)$可通过 $y(t+1)$计算得到 $x(t+1) = f(y(t+1))$.方程(1)当 $k = 0.5$,$\alpha = 1.0$,$\varepsilon = 0.015$,$a = 0.32$ 时呈现混沌解,其 Lyapunov 指数是 0.13.

本文采用循环神经网络对 Hénon 离散混沌系统进行建模.特别的选用 Elman[11] 提出的一种神经网络,因为它对噪声有较强的抑制能力,结果简单且性能良好[12],结构如图 1 所示,它包含一个隐层,其中

* 国家自然科学基金(批准号:60174031)资助的课题.

隐层的输出经过延迟再反馈到输入，构成了循环网络. 网络的结构取输入层的节点数为 2，对应于 Hénon 映射的两个变量，隐层结点数为 10，输出层的节点数为 2. 为了确定 Elman 网络的权值和阈值，首先由 Hénon 混沌系统产生时间序列，去除暂态点，用 1000 点来训练 Elman 网络，训练算法为误差反向传播(BP)算法. 一旦训练完毕，把网络的输出引入到输入，随机选取初值，让神经网络迭代，便可以得到 Hénon 混沌神经网络. 训练好的网络就是 Hénon 系统很好的逼近.

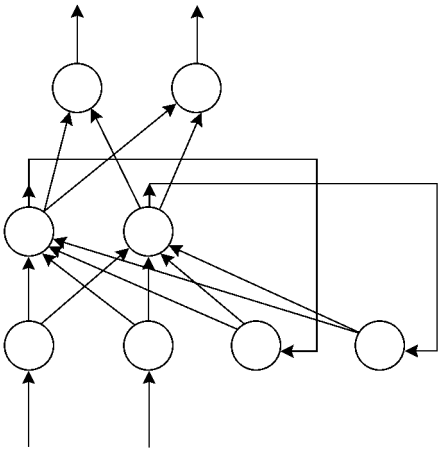

图 1　Elman 神经网络结构

图 1 所示为 Hénon 映射及神经网络逼近 Hénon 映射得到的 Hénon 混沌神经网络的吸引子(Hénon 混沌神经网络). 由图 2 可知，混沌神经网络吸引子与原系统非常相似. 为了从量上进一步揭示混沌神经网络的动力学行为，本文在前面给出了其 Lyapunov 指数. Lyapunov 指数是衡量动力学系统相邻轨道平均分散的一个物理量，正的 Lyapunov 指数意味着系统处在混沌状态. 经计算，Hénon 混沌神经网络的 Lyapunov 指数为 0.30 与原混沌系统的 Lyapunov 指数相同. Hénon 混沌系统与它的神经网络吸引子如图 2.

3. 离散混沌神经网络的同步

本文构造的混沌神经网络属于离散混沌系统，就目前来说，有关离散混沌同步的研究不如连续系统那么深入. 从文献报道看，大部分同步方法需要把整个系统分解成几个子系统或几个部分(稳定的和不稳定的)，如基于压缩映射的混沌同步方法，有源无源分解(APD)混沌同步法等[13]. 这类同步方法要求系统必须是易分解的.

鉴于此，本文基于自适应逆控制原理[14,15]提出一种新的离散系统混沌同步的方法来实现混沌神经网络的同步，考虑 m 维离散混沌系统 A(发射系统)：

$$X_{n+1}^{(1)} = \breve{F}(X_n^{(1)}), \tag{2}$$

则接收系统 B 可描述为

$$X_{n+1}^{(2)} = \breve{F}(F^{-1}(r'_n)), \tag{3}$$

$$X_n^{(2)} = F^{-1}(r'_n), \tag{4}$$

式中 $X_n^{(1)}, X_n^{(2)}, r'_n \in R^m$；$F^{-1}(r'_n)$为逆控制项，$\breve{F}$ 为时变的混沌神经网络结构模型，r'_n 为带有噪声的接收信号，对许多离散混沌系统，如 Logistic 方程、Hénon 映射等，反馈控制方法不能使两个系统同步. 针对这种情况，本文引入逆控制，即逆控制项 $F^{-1}(r'_n)$是变量 $X_n^{(1)}, X_n^{(2)}$ 的非线性函数，取包含噪声的 Hénon 逆映射的混沌建模 $\breve{F}^{-1}(r'_n)$为逆控制项，把以上描述的混沌方法称为逆控制混沌同步方法. 逆控制混沌系统同步方法不改变原系统的混沌特性，不需要分解系统，而且它的适用面很广，不仅

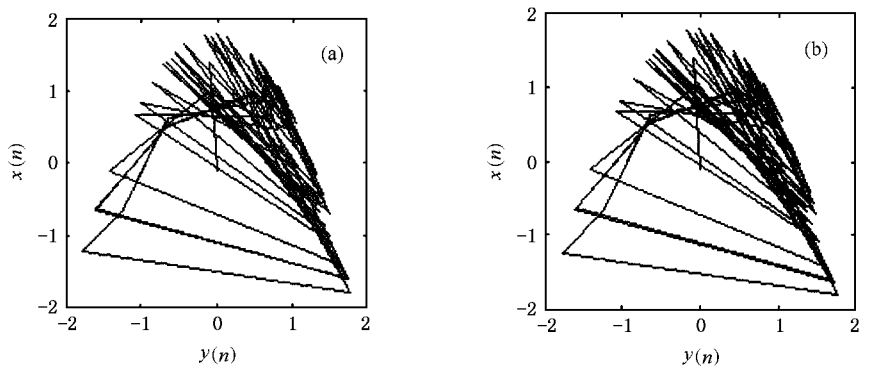

图 2　混沌系统与它的神经网络逼近的吸引子　(a) Hénon 映射；(b) Hénon 混沌神经网络

适用于简单的混沌系统,同样也适用于复杂结构的混沌系统(如图 3 所示布鲁塞尔振子的混沌神经网络),所以它是线性逆控制方法的自然推广,而且它的同步速度很快,鲁棒性强.

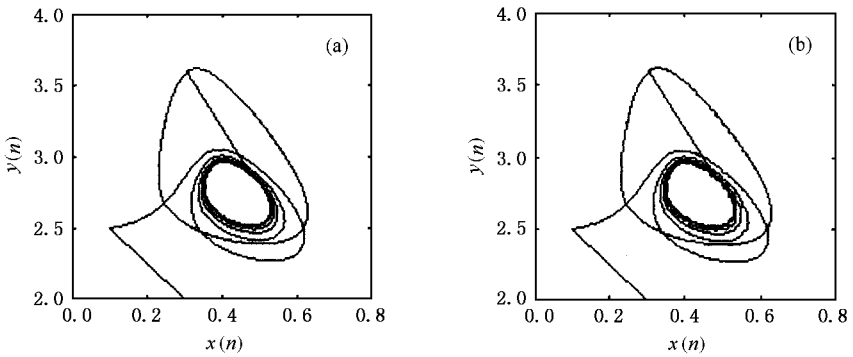

图 3 布鲁塞尔混沌系统与它的混沌神经网络吸引子 (a)布鲁塞尔振子;(b)布鲁塞尔振子混沌神经网络

下面把非线性逆控制混沌同步问题应用于 Hénon 混沌神经网络的同步问题.设 Hénon 混沌神经网络的动力学方程为

$$\begin{bmatrix} X_{n+1} \\ Y_{n+1} \end{bmatrix} = F\begin{bmatrix} X_n \\ Y_n \end{bmatrix}, \tag{5}$$

则混沌神经网络的同步可描述为具有不同初始值的两个相同的网络 CNNC,

$$\begin{bmatrix} X_{n+1}^{(1)} \\ Y_{n+1}^{(1)} \end{bmatrix} = F\begin{bmatrix} X_n^{(1)} \\ Y_n^{(1)} \end{bmatrix}, \begin{bmatrix} X_{n+1}^{(2)} \\ Y_{n+1}^{(2)} \end{bmatrix} = F\begin{bmatrix} X_n^{(2)} \\ Y_n^{(2)} \end{bmatrix} \tag{6}$$

的同步.非线性逆控制混沌同步系统结构如图 4 所示.

CNNC 和 CNNB′ 的运算如图 4 所示.$[X_n^{(1)}, Y_n^{(1)}]^{\mathrm{T}}$ 经过网络控制器 CNNC 的迭代得到 $[X_{n+1}^{(1)}, Y_{n+1}^{(1)}]^{\mathrm{T}}$,在受到噪声污染后经过 CNNB 得到的 $[X_n^{(2)}, Y_n^{(2)}]^{\mathrm{T}}$ 正好与 $[X_n^{(1)}, Y_n^{(1)}]^{\mathrm{T}}$ 达到同步,所以在 $[X_n^{(2)}, Y_n^{(2)}]^{\mathrm{T}}$ 驱动网络 CNNC 后得到的 $[X_{n+1}^{(2)}, Y_{n+1}^{(2)}]^{\mathrm{T}}$ 也与 $[X_{n+1}^{(1)}, Y_{n+1}^{(1)}]^{\mathrm{T}}$ 同步.有效的去除了噪声的污染.图 5 给出了当两个 Hénon 混沌神经网络初值分别为 $(0.1, 1.0)^{\mathrm{T}}$ 和 $(0, 0.1)^{\mathrm{T}}$,噪声 $n_k = -1/3\sin 0.8n + 0.1/3(y_{n+1}^{(1)})^2$ 时的同步结果.

4. 离散混沌神经网络在保密通信中的应用

利用混沌遮掩方式[5,6],把前面提出的混沌神经网络同步应用于数字保密通信.混沌遮掩是广泛使用的保密通信方式,已由许多模拟电路实现[5,6].但传统的混沌遮掩方法有一个很大的缺点,那就是发射端和接收端的驱动信号不同,发射端是混沌信号,而接受端是混沌信号加有用信息,因此导致发射端与接收端不可能达到完全同步,恢复出来的信息存在误差.为此,本文提出一种改进的混沌遮掩方法,其核心思想是用有用信息既驱动接收端也反馈到发射端,即发射端的方程变为

$$\begin{bmatrix} X_{n+1}^{(1)} \\ Y_{n+1}^{(1)} \end{bmatrix} = \breve{F}\begin{bmatrix} X_n^{(1)} \\ Y_n^{(1)} \end{bmatrix} + \begin{bmatrix} s_n \\ 0 \end{bmatrix}, \tag{7}$$

使用二维的发射信号

$$\begin{aligned} r_n &= L[X_{n+1}^{(1)}, Y_{n+1}^{(1)}, s_n] \\ &= \begin{bmatrix} k & 0 \\ 0 & 1 \end{bmatrix}\breve{F}\begin{bmatrix} X_n^{(1)} \\ Y_n^{(1)} \end{bmatrix} + \begin{bmatrix} s_n \\ 0 \end{bmatrix}, \end{aligned} \tag{8}$$

其中,$L(\cdot)$为一个线性函数,接收端的方程为

$$\begin{aligned} \begin{bmatrix} X_{n+1}^{(2)} \\ Y_{n+1}^{(2)} \end{bmatrix} &= \breve{F}(F^{-1}(r_n')) \\ &= \breve{F}\begin{bmatrix} X_n^{(2)} \\ Y_n^{(2)} \end{bmatrix} + \begin{bmatrix} s_n \\ 0 \end{bmatrix}, \end{aligned} \tag{9}$$

很显然,因为在发射端也加了驱动信号 s_n,所以能保证发射端与接收端完全同步,同步后信息可以完全恢复,恢复的信息为

$$\begin{aligned} s_n' &= L^{-1}[X_{n+1}^{(2)}, Y_{n+1}^{(2)}, r_n] \\ &= L^{-1}[X_{n+1}^{(1)}, Y_{n+1}^{(1)}, r_n] \\ &= s_n. \end{aligned} \tag{10}$$

图 6 给出了基于混沌神经网络逆控制保密通信系统的原理框图.

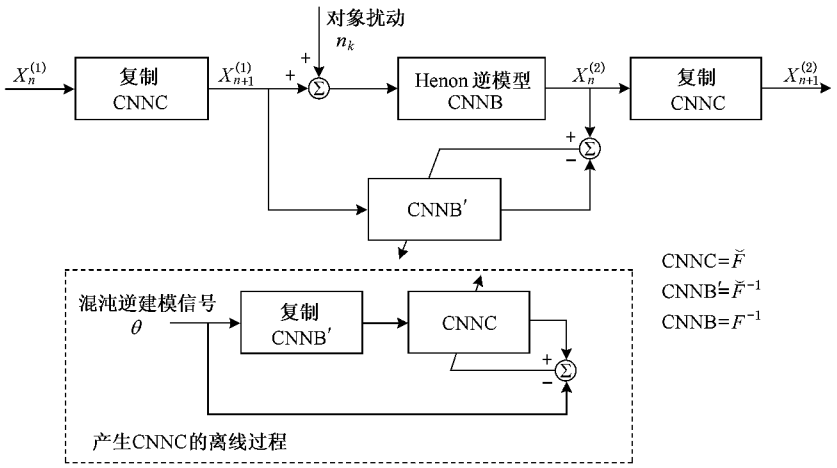

图 4　混沌神经网络同步系统结构图

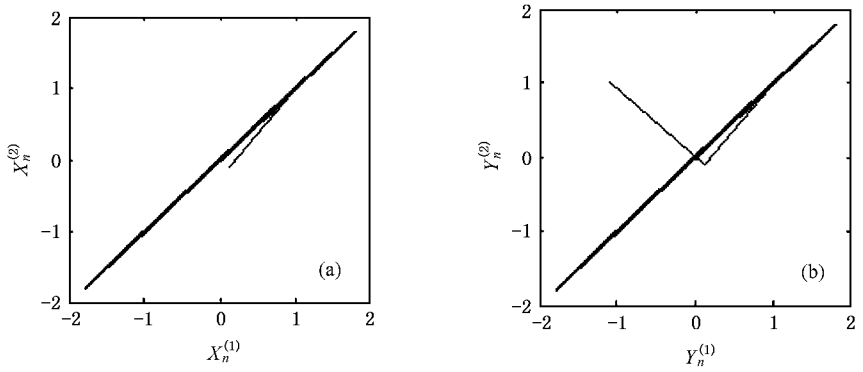

图 5　两个 Hénon 混沌神经网络同步的结果　(a)变量 $X_n^{(1)}$ 与 $X_n^{(2)}$ 的同步化行为；(b)变量 $Y_n^{(1)}$ 与 $Y_n^{(2)}$ 的同步化行为

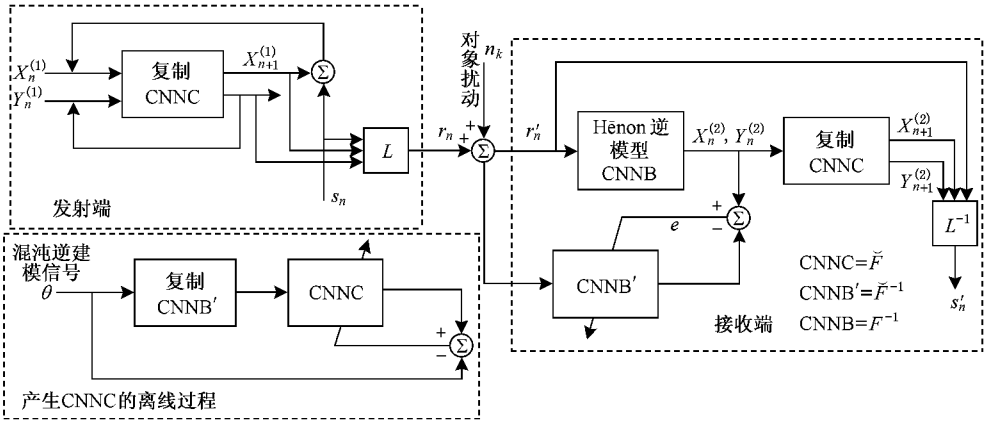

图 6　混沌神经网络逆控制的保密通信系统原理框图

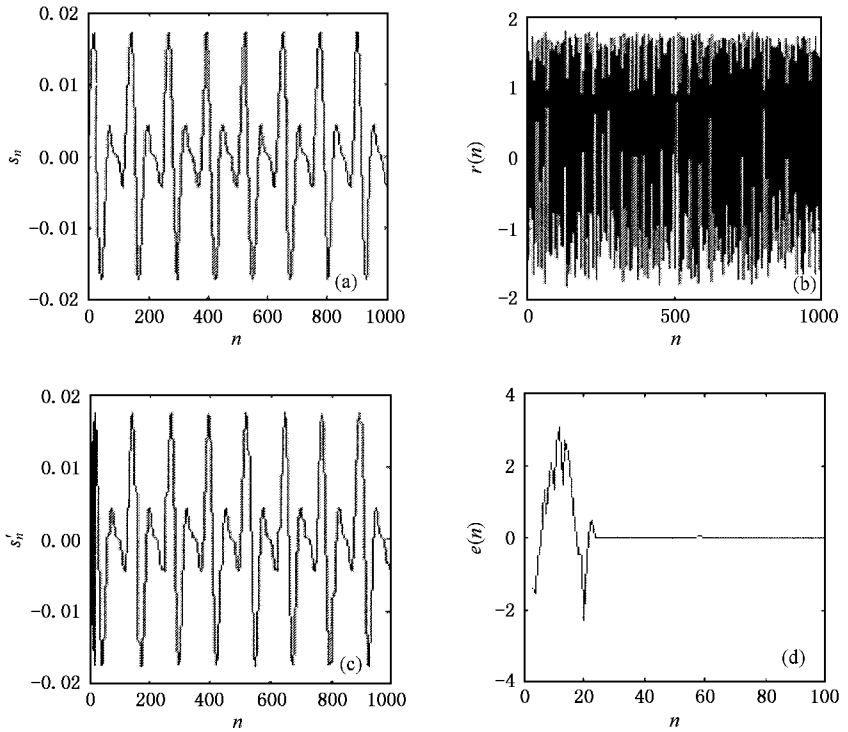

图 7 离散混沌神经网络保密通信系统传输混合正弦信号信息的结果 (a)原始信息 s_n,(b)传输的信息 $r(n)$;(c)恢复的信息 s'_n;(d) X 变量的同步行为 $e(n)$

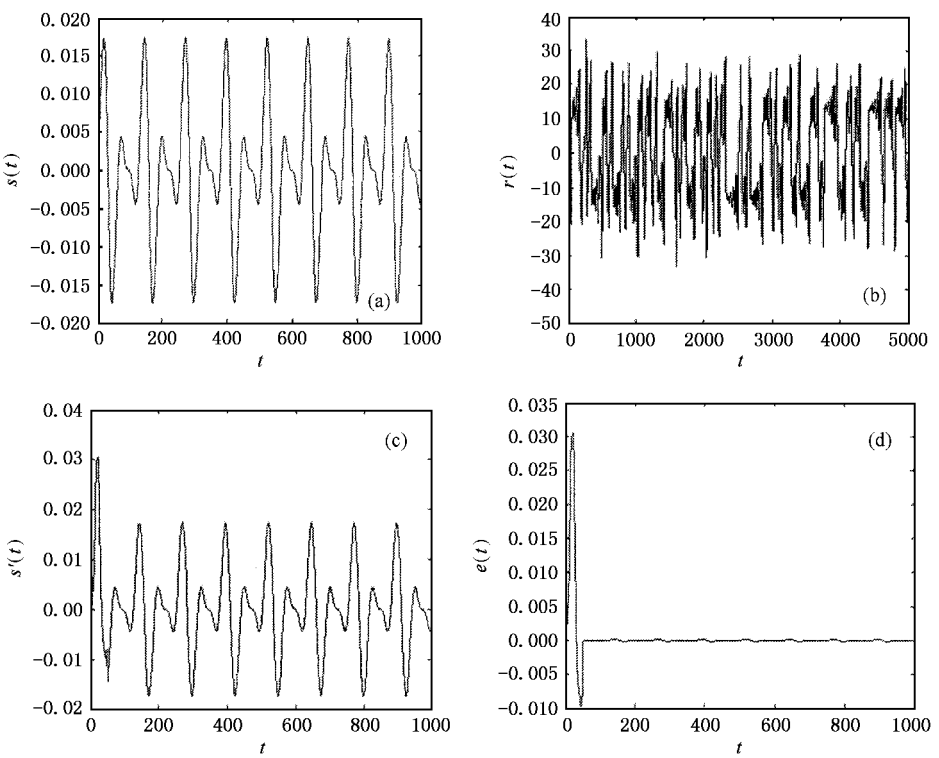

图 8 连续混沌神经网络保密通信系统传输调幅波信息的结果 (a)连续调幅波信息 $s(t)$;(b) 带有噪声的传输信号 $r(t)$;(c) 接收端恢复的信息 $s'(t)$;(d)信息恢复的误差 $e(t)$

5. 系统仿真研究

传统的保密通信系统仅仅是对接收端进行滤波或者在接收端进行信道均衡,由于混沌对参数极端的敏感性,这样的方式在实际中往往不能得到很好的同步效果,对此,本文进行保密通信系统的改进,如图 6 所示.离线对控制器进行逆建模,将时变的逆控制器同时在接收端和发射端进行抑制噪声干扰(仿真实例加入白噪声),保证了发射端和接收端的完全同步.实例,图 7 给出了离散混沌神经网络系统传输数字信息 $s_n = 0.01\sin(n/10)[1 + \sin(n/20)]$(见图 7(a)所示)的结果,加密调制矩阵中的 $k = 0.9$ 为保密需要,信息信号应小于混沌调制信号.图 7(b)所示为离散 Hénon 混沌神经网络的发射信号 $r(n)$,它包含信息信号和混沌调制信号.经过很短的暂态过程之后,恢复信息如图 7(c)所示,发射系统与接收系统达到同步误差很好地收敛到 0(见图 7(d)),仿真结果证明信息在很短的时间后能够完全恢复.图 8(a)为连续 Lorenz 混沌神经网络系统传输调幅波($s(t) = F\sin(\omega t)[1 + f\sin(\Omega t)$,其中 $F = 0.01, f = 1.0, \Omega = 0.05$)的结果,图 8(b)为携带调幅波的 Lorenz 混沌神经网络发射信号 $r(t)$,经过同步后,信息能够准确恢复(见图 8(c)),恢复误差如图 8(d)所示.

6. 结　论

本文利用神经网络的学习和逼近能力构造混沌神经网络,提出了混沌神经网络逆控制方法来同步两个混沌神经网络系统,并对混沌保密通信系统进行了改进.研究表明该方法能够有效地抑制噪声对恢复传输信号的所造成的破坏.最后仿真结果表明了所给方法的有效性.

[1] Freeman W J 1987 *Biological Cybernetics* **56** 139

[2] Freeman W J 1992 *Int J. Bifurcation and Chaos* **2** 451

[3] Yao Y and Freeman W J 1990 *Neural Networks* **3** 153

[4] Duke D W and Pritchara W S 1991 *Phys. Lett.* **11** 494

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

[6] Kocraev L J, Halle K S and Chua L O 1992 *Int J. B if and Chaos* **2** 709

[7] Kocraev L and Parlitz U 1995 *Phys. Rev. Lett.* **74** 5028

[8] AngeliA De 1995 *IEEE Trans CAS* **42** 54

[9] Tang G N, Luo X S and Kong L J 2000 *Acta Phys. Sin.* **49** 30 (in Chinese) [唐国宁、罗晓曙、孔令江 2000 物理学报 **49** 30]

[10] Wu Z Q, Ao D and Liu K 2004 *Acta Phys. Sin.* **53** 21(in Chinese) [吴忠强、奥　顿、刘　坤 2004 物理学报 **53** 21]

[11] Elman J L 1990 *Cognitive Science* **14** 179

[12] Gencay R and Liu T 1997 *Physica* D **108** 119

[13] Luo X S and Fang J Q and Wang L H and Kong L J and Weng J Q 1999 *Acta Phys. Sin.* **48** 2022 (in Chinese) [罗晓曙、方锦清、王力虎、孔令江、翁甲强 1999 物理学报 **48** 2022]

[14] [America] B. Windrow and [Israel] E. Walach (Author), Liu S T and Han C Z (Translator). 2000 *Adaptive Inverse Control* (Xi 'an: Xi 'an Jiaotong University Press) 150 – 197 (in Chinese) [[美] 威德罗、[以色列] 瓦莱斯著,刘树堂、韩崇昭译 2000 自适应逆控制(西安 西安交通大学出版社)150—197]

[15] Lu Z G, Yu L H, Liu X J, Gao M J and Wu S C 2002 *Acta Phys. Sin.* **51** 2211 (in Chinese) [卢志刚、于灵慧、柳晓菁、高美静、吴士昌 2002 物理学报 **51** 2211]

Synchronization of chaotic neural networks based on adaptive inverse control and its applications in secure communications*

Yu Ling-Hui Fang Jian-Cheng

(*The 5th Unit, Beijing University of Aeronautics and Astronautics, Beijing*, 100083, *China*)

(Received 30 September 2004; revised manuscript received 17 December 2004)

Abstract

Based on adaptive inverse control theory, a new chaotic neural networks synchronous system and its secure communication are designed. The synchronization of chaotic neural networks system in the presence of perturbation is studied. The proposed method can overcome effectively the noise pollution of channel in transmitting information. The numerical experiments show that the proposed secure communication scheme has advantages of flexible implementation, fast synchronization, high-quality recovery of information and large amounts of secret key for information encryption.

Keywords: chaotic synchronization, adaptive inverse control, chaotic neural network, secure communications

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 60174031).