文章编号:1001 - 893X(2002)05 - 0141 - 07

混沌神经网络及其在保密通信中的应用*

刘年生　郭东辉　吴伯僖

(厦门大学技术物理研究所,福建 厦门 361005)

摘　要:具有高度复杂非线性动力学特性的混沌神经网络系统已成为近年来进行加密通信应用研究的热点课题。本文首先概括了混沌神经网络的一些主要理论模型及其非线性动力学系统的特点和复杂性,并分析人们如何利用混沌神经网络系统的这些复杂非线性特点,如混沌同步和混沌吸引子等,进行加密通信的基本算法原理,最后总结有关混沌神经网络及其加密通信应用中所需要进一步研究的一些课题。

关键词:保密通信;混沌神经网络;混沌同步;混沌吸引子
中图分类号:TN918.2;O415.5　　**文献标识码**:A

Chaotic Neural Network and its Application in Secure Communications

LIU Nian - sheng, GUO Dong - hui, WU Bo - xi

(Institute of Technical Physics, Xiamen University, Xiamen 361005, China)

Abstract: The chaotic neural networks with the characteristics of very complicated nonlinear dynamics have been a hot project of application to secure communications in recent years. This paper firstly deals with some main theoretic models, the characteristics and complexities of nonlinear dynamics of them. It analyzes the basic principles which chaotic neural networks are applied to secure communications using the complex property of nonlinear dynamics of them such as chaotic synchronization and chaotic attractors. It finally summarize the projects of chaotic neural network and its application to secure communications that needs to be further researched.

Key words: Secure communication; Chaotic neural network; Chaotic synchronization; Chaotic attractor

一、引　　言

1990 年 K. Aihara、T. Takabe 和 M. Toyoda 等人[1]根据生物神经元的混沌特性首次提出混沌神经网络模型,将混沌学引入神经网络中,使得人工神经网络具有混沌行为,更加接近实际的人脑神经网络,因而混沌神经网络被认为是可实现其真实世界计算的智能信息处理系统之一,成为神经网络的主要研究方向之一,它在许多领域中具有广泛的应用前景,如在网络通信、组合优化和人工智能等领域[2~9],尤其是在保密通信方面[10~15],因此吸引了国内外许多人对它进行多方面的深入研究,取得了许多理论研究成果和技术应用成果,值得去总结和分析,以明确混沌神经网络进一步发展的方向。因为随着社会和科技的不断发展,在军事、金融或商业等部门以及个人通信中,信息加密应用越来显得越重要,人们总是希望追求那种能够完全保密的加密系统,而根 C. E. Shannon 信息论原理,唯一能够达到完全保密的加密算法只有一次一密的序列加密方法,但是由于其存在着难以克服的分配大量随机参数流的困难,因此,

* 收稿日期:2002 - 05 - 16
基金项目:国家自然科学基金(No. 69886002, 60076015)和福建省自然科学基金(No. A0010019)资助

在现代密码学的实际应用中,人们一直致力于寻找那些依赖 NP 问题的复杂性或只须少量的随机参数就能够产生具有密码学意义的大量伪随机序列的加密方法。理论研究已证明混沌神经网络具有非常丰富和复杂的非线性动力学特性,特别是它的混沌动力学特性[1,2,15,17,18],它不仅是一个非常复杂难解的 NP 问题,而且能产生无法预测的序列轨迹;若以根据神经网络混沌分类特性来实现加密算法,与 DES 相比,其加密与解密的算法是非对称的,安全性更好;若以神经网络的混沌序列轨迹来实现加密算法,与以移位寄存器为基础的序列加密法相比,在序列周期、随机统计性以及线性复杂度方面均有优势,我们已从理论上证明这种混沌加密方法具有相当的安全性[11]。此外,由于神经网络是一种高速并行运算的网络,只要用集成电路来直接兑现它的并行运算方式,其加密算法就可实现实时加密通信,可以满足现代 网络实时通信的要求。然而,在加密通信工程实际中很少见到是基于混沌神经网络技术的,理论研究与实际应用之间存在着较大的差异,这也就是混沌神经网络需要进一步研究和改进的方向。为此本文首先对概括了混沌神经网络的一些主要的理论模型和其非线性动力学特点,接着总结和分析利用混沌神经网络混沌同步和混沌吸引子等特性进行加密通信的基本算法原理和存在的问题,最后总结了有关混沌神经网络及其加密通信应用中需要进一步研究的课题。

二、混沌神经网络的模型与特性

混沌神经网络与以前的常规神经网络如离散型 Hopfield 模型[16]相比,在模型结构和动力学特性等方面均不同,增加了混沌特性,包括混沌同步和奇异吸引子等。

1. 混沌神经网络模型

混沌神经网络的研究就起源于和基于混沌神经元的研究,至今已报道的混沌神经元模型有许多种,其中有 2 类最为人们所关注,一类是 K. Aihara 等人根据生物神经元的特性而提出的混沌神经元,另一类是 M. Inoue 等人依据 Logistic 映射将混沌振荡子作为混沌神经元。

(1) Aihara 混沌神经网络模型

K. Aihara、T. Takabe 和 M. Toyoda 等人[1]吸收了前人对生物神经元和人工神经元的研究成果,提出了一种混沌神经元模型,在常规神经元模型如离散型 Hopfield 模型基础上嵌入了脑神经元的特性,包括递级反应、相对不应性和输入时空综合等。单个的 Aihara 混沌神经元示意图如图 1 所示,它带有

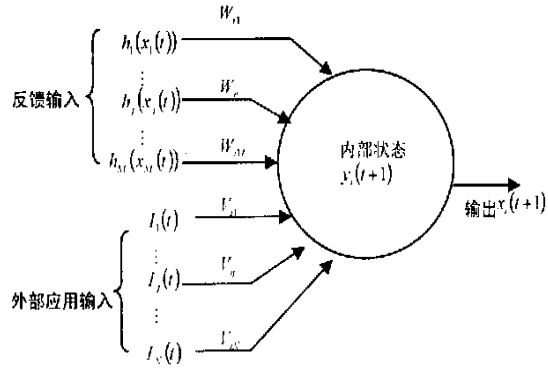


图 1 Aihara 混沌神经元模型

来自内部神经元的反馈项和外部输入项,以及来自神经元本身的不应性项和阈值,并假定这种不应性项随时间按指数方式衰减。这样由个混沌神经元所组成的混沌神经网络的第个混沌神经元的动力模型描述如下:

$$x_i(t+1) = f_i\Big(\sum_{j=1}^{M} W_{ij}\sum_{r=0}^{t} k^r h_j(x_j(t-r)) + \sum_{j=1}^{M} V_{ij}\sum_{r=0}^{t} k^r I_j(t-r) - \alpha\sum_{r=0}^{t} k^r g_i(x_i(t-r)) - \theta_i\Big) \quad (1)$$

式中 $x_i(t+1)$ 为第 i 个混沌神经元在离散时刻 $(t+1)$ 的输出;

f_i 为第 i 个混沌神经元的连续输出函数;

M 为混沌神经元的个数;

W_{ij} 为第 j 个混沌神经元与第 i 个混沌神经元之间的联结权值;

h_j 为第 j 个混沌神经元的轴突变换传输函数;

N 为外部输入的个数;

V_{ij} 为第 j 个输入与第 i 个混沌神经元之间的联结权值;

$I_j(t-r)$ 为离散时刻 $(t-r)$ 第 j 个外部输入的强度;

g_i 为第 i 个混沌神经元的不应性函数;

k 为不应性衰减系数;

α 为自反馈系数,一般为一正数;

θ_i 为第 i 个混沌神经元的全或无激发阈值。

若 $y_i(t+1)$ 代表离散时刻 $(t+1)$ 时第 i 个混沌神经元的内部状态,则公式(1)可表示为

$$y_i(t+1) = \sum_{j=1}^{M} W_{ij} \sum_{r=0}^{t} k^r h_j(x_j(t-r)) + \sum_{j=1}^{N} V_{ij} \sum_{r=0}^{t} k^r I_j(t-r) - \alpha \sum_{r=0}^{t} k^r g_j(x_i(t-r)) - \theta_i \quad (2)$$

$$x_i(t+1) = f_i(y_i(t+1)) \quad (3)$$

该模型具有十分丰富而又复杂的非线性动力学特性[17],如采用混沌模拟退火算法[18]则可进行全局组合优化计算。

(2) Inoue 神经网络模型

1991 年 Inoue 等人[19]提出了另外一种混沌神经网模型,以耦合的混沌振荡子作为单个神经元,每个耦合混沌振荡子的同步和异步分别对应于神经元的激发和抑制这两种状态,其中耦合混沌振荡子的同步来自于混沌中的规则性,而混沌的不规则性则可产生随机搜索能力。对于离散时间,耦合混沌振荡子的运动方程由 f(x) 和 g(x) 描述如下:

$$x_i(t+1) = f(x_i(t)) + D_i(t)[y_i(t+1) - x_i(t+1)] \quad (4)$$

$$y_i(t+1) = g(y_i(t)) + D_i(t)[x_i(t+1) - y_i(t+1)] \quad (5)$$

公式中 $D_i(t)$ 是离散时刻 t 第 i 个神经元的耦合系数,$x_i(t)$ 和 $y_i(t)$ 分别是离散时刻 t 第 i 个神经元第一和第二个振荡子变量。而 f(x) 和 g(y) 可为最基本混沌 Logistic 映射,即:

$$f(x) = ax(1-x),\ 0 < a \le 4 \quad (6)$$

$$g(x) = by(1-y),\ 0 < b \le 4 \quad (7)$$

离散时刻 t 第 i 个神经元的状态定义为

$$u_i(t) = \begin{cases} 1(\text{激活}) & |x_i(t) - y_i(t)| < \varepsilon \\ 0(\text{抑制}) & \text{其它} \end{cases} \quad (8)$$

ε 为同步的临界参数。

设第 i 个神经元和第 j 个神经元由耦合常数 W_{ji} 联结,W_{ji} 与 $D_i(t)$ 的关系可定义为

$$DD_i(t) = \sum_j W_{ij} u_j(t) + s_j + \theta_i \quad (9)$$

$$D_i(t) = \begin{cases} DD_i(t), & DD_i(t) > 0 \\ 0 & \text{其它} \end{cases} \quad (10)$$

式中 s_i 是外部输入;

θ_i 是第 i 个神经元的阈值。

在此基础上,1992 年 Inoue 等人[20]用一个混沌振荡子实现了 Hopfield 的联想记忆和求 TSP 解的功能,通过对其运动方程的分析研究又将其推广到模拟态,运动方程为

$$\begin{bmatrix} x_i(t+1) \\ y_i(t+1) \end{bmatrix} = \frac{1}{2+2D_i(t)} \begin{bmatrix} 1+D_i(t) & D_i(t) \\ D_i(t) & 1+D_i(t) \end{bmatrix} \begin{bmatrix} f[x_i(t)] \\ g[y_i(t)] \end{bmatrix} \quad (11)$$

式中 $0 \le x_i(t) < 1$;

$0 \le y_i(t) < 1$;

$u_i(t) = \dfrac{1}{1+\exp(-z_i/z_0)}$;

$z_i \equiv \dfrac{\varepsilon}{\nabla_i(t)} - 1$;

$\nabla_i(t) = |x_i(t) - x_i(t+3)|$。

除了以上两种混沌神经网路模型外,还有许多其它混沌神经网络模型,例如经改进后具有混沌特性的 Hopfield 模型[21]和细胞神经网络模型[22]。

2. 混沌神经网络的特性

与常规的离散型 Hopfield 神经网络相比较[16],混沌神经网络具有更丰富的非线性动力特性,主要包括如下:

(1) 在神经网络中引入混沌动力行为

在 Aihara 混沌神经网络模型公式(2)和(3)中,不妨假设 $x_i(t) = 1/(1+e^{-y_i(t)/\varepsilon})$ 为 S 形连续有界函数,且输出函数和不应性函数为 $f(x) = g(x) = x$ 时,则它的 *Lyapunov* 指数为

$$\lambda_1 = \lim_{m\to\infty} \frac{1}{m} \sum_{t=0}^{m-1} \ln \left| \frac{dy_i(t+1)}{dy_i(t)} \right| = \lim_{m\to\infty} \frac{1}{m} \sum_{t=0}^{m-1} \ln \left| k + \frac{1}{\varepsilon} \sum_{j=1}^{M} W_{ij} x_i(t)(1-x_i(t)) - \frac{\alpha}{\varepsilon} x_i(t)(1-x_i(t)) \right|$$

仿真计算结果表明,在许多不同的取值区域内存在 Lyapunov 指数为正的情况[1,17,18],即混沌态,而在 Inoue 神经网络模型中,根据公式(6)、(7)和(8)的非线性映射,选择适当的参数 a 和 b,采用频谱分析方法或相关函数法[23]来来判断网络状态是否为混沌态。

(2) 混沌神经网络的同步特性

1990 年 Pecora 和 Carroll[24]发现了混沌同步现象,并认为它是混沌现象的一个基本属性。依照同样的原理,当 2 个混沌神经网络系统相耦合时,其中一个神经网络为激励系统,通过连接参数的驱动或

耦合来激励另一个神经网络,该响应神经网络运用自反馈方法缩小两者之间的同步误差,最终实现两者之间的混沌同步[10]。

(3) 混沌神经网络的吸引子

吸引子描述了神经网络运动的收敛类型,是神经网络行为的最终决定者,尤其为非整数维的奇异吸引子时,它就是神经网络产生混沌现象的内在推动力。在混沌神经网络系统中共存着多种吸引子,包括单点式、周期环和奇异吸引子,其中 Luonan Chen 和 Kazuyuki Aihara 等[17]在 1999 年从理论上证明暂态混沌神经网络中存在着奇异吸引子,它是由单点式吸引子通过同源同宿分形演化而来的,比在离散 Hopfield 神经网络系统中[25]根据 Lyapunov 能量函数经过迭代而得到的吸引子要复杂得多。

三、混沌神经网络在保密通信中的应用

混沌神经网络系统中丰富的非线性动力学特性为其在保密通信中的应用提供了坚实的理论基础,目前主要是根据它的混沌同步特性和混沌吸引子特性来进行信息加密与解密的。

1. 混沌同步在保密通信中的应用

由于混沌系统对初始条件和参数十分敏感,所以在 20 世纪 90 年代初,混沌同步就开始用于保密通信,至今已经历了 4 次大的改进与发展[13,26],其主要的方法和特点如表 1 所示。

表 1 混沌同步保密通信的发展主要历程

发展阶段	主要方法	主要特点
第一代 (从 1993 年起)	附加混沌遮盖 混沌键控	前者电路实现简单,用于模拟通信;但抗噪声和参数失配的能力较弱,且保密性差。后者虽抗噪声和参数失配的能力较强,可用于数字通信,但保密性差。
第二代 (1993～1995 年)	混沌参数调制 混沌非自治调制	这两种方法理论上可使得同步误差接近零,甚至不存在同步误差,保密性较第一代有所增强,但还不令人满意。
第三代 (自 1997 年起)	混沌密码系统	将经典的密码技术与混沌同步结合起来,进一步增强了系统的保密性,至今还没有被破译过,但带宽利用率较低。
第四代 (自 1999 年起)	混沌脉冲同步	带宽利用率较高,抗噪声和参数失配的能力较强,并可与常规的密码技术结合在一起,提高系统的保密性。

以最近的第四代混沌脉冲同步保密通信为例进行说明,Tao Yang 和 Leon O. Chua 等人[27,28]于 1997 年根据脉冲微分方程理论利用蔡氏振荡子(Chua's oscillator)来实现混沌脉冲同步保密通信。

蔡氏振荡电路方程一般表示为

$$\begin{cases} \dot{x} = a[y - x - f(x)] \\ \dot{y} = x - y + z \\ \dot{z} = -by - cz \end{cases} \tag{12}$$

其中 a、b 和 c 为常数,f(x)为蔡氏二极管的分段线性函数,一般表示为

$$f(x) = dx + \frac{1}{2}(g - d)(|x + 1| - |x - 1|)$$

(其中 d 和 g 为常数)

方程(12)也可改写为一般的非线性动力学方程,即:

$$\dot{X} = AX + \Phi(X) \tag{13}$$

其中:

$$X = \begin{bmatrix} x \\ y \\ z \end{bmatrix} \quad A = \begin{bmatrix} -a & a & 0 \\ 1 & -1 & 1 \\ 0 & -b & -c \end{bmatrix} \quad \Phi(x) = \begin{bmatrix} -af(x) \\ 0 \\ 0 \end{bmatrix}$$

在脉冲同步通信系统中有 2 个蔡氏振荡子,其中一个为激励子系统,即方程(13)所示,另一个为响应子系统,方程表示如下:

$$\dot{\tilde{X}} = A\tilde{X} + \Phi(\tilde{X}) \tag{14}$$

其中 $\tilde{X}^T = (\tilde{x}, \tilde{y}, \tilde{z})$ 为响应子系统的状态变量。

在离散时刻 τ_i (i = 1,2,…) 时激励子系统的状态变量传送到响应子系统,响应子系统的脉冲微分方程为

$$\begin{cases} \dot{\tilde{X}} = A\tilde{X} + \Phi(\tilde{X}) \\ \Delta\tilde{X}|_{t=\tau_i} = -Be \end{cases} \tag{15}$$

其中 $e^T = (e_x, e_y, e_z) = (x - \tilde{x}, y - \tilde{y}, z - \tilde{z})$ 为同步误差,B 为一个 3 ×3 阶矩阵,该矩阵表示两子系统的耦合程度。

令

$$\Phi(X,\tilde{X}) = \Phi(X) - \Phi(\tilde{X}) = \begin{bmatrix} -af(x) + af(\tilde{x}) \\ 0 \\ 0 \end{bmatrix}$$

则脉冲同步误差系统可表示为

$$\begin{cases} \dot{e} = Ae + \Phi(X,\tilde{X}), \ t \neq \tau_i \\ \Delta|_{t=\tau_i} = Be, \ i = 1,2,\cdots \end{cases} \tag{16}$$

Tao Yang 利用脉冲微分方程理论证明方程组(16)是渐近稳定的[27],因而脉冲同步系统也是渐近稳定的。这种脉冲同步系统可与常规的加密算法相结合来获得一个复合的传送信号,提高混沌保密通信的实用安全,其典型的加密流程框图如图 2 所示。该基于脉冲混沌同步保密通信系统的主要特点见前表 1 所示。

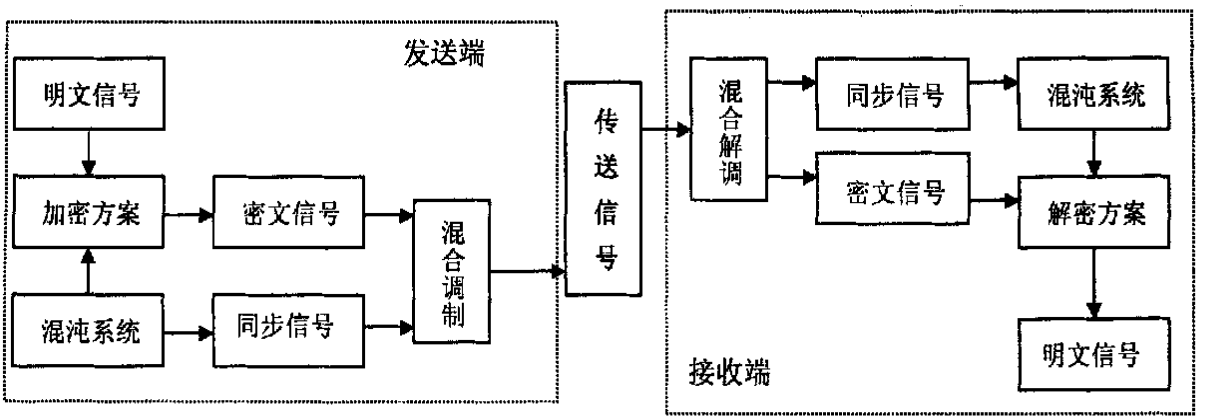


图 2 基于混沌神经网络保密通信系统框图

目前,对这四代混沌同步保密通信的研究与开发仍在继续,今后可能主要如下几方面进行改进:

(1) 通过对混沌系统运动方程和混沌电路的改进,进一步提高混沌同步保密通信系统抗信道噪声干扰的能力,适当放宽混沌同步的发送机和接收机之间的特性参数失配允许程度,便于混沌保密通信系统从有线通信发展到无线通信,并有利于工程上的实现。首先,目前的混沌同步保密系统多为混沌信号在理想的信道中进行传输来仿真评估的,而在实际传输信道中存在着噪声、信号衰减和信道时变性等,混沌信号抗噪声干扰等的性能还比较差,信号失真度较高,明文恢复的失真度也相应较大;其次,混沌同步误差只有在 2 %以内,系统才具有较好的鲁棒性,这就要求混沌发射(激励系统)与接收(响应系统)两系统之间特性参数要高度匹配,而在工程实际中难以达到。这些问题均需通过对混沌神经网络及其相应的混沌电路的改进来解决。

(2) 高维混沌系统同步的物理机制和方法的深入探讨。目前,所发表文章中的有关混沌同步保密系统大多数是为低维的时间混沌系统,而对空间混沌、时空混沌和功能混沌等高维超混沌系统尚处于萌芽阶段[29],其物理机制和实现方法有待于进一步研究发现,其结果有可能会提高混沌同步保密系统的保密性与信号的保真度。

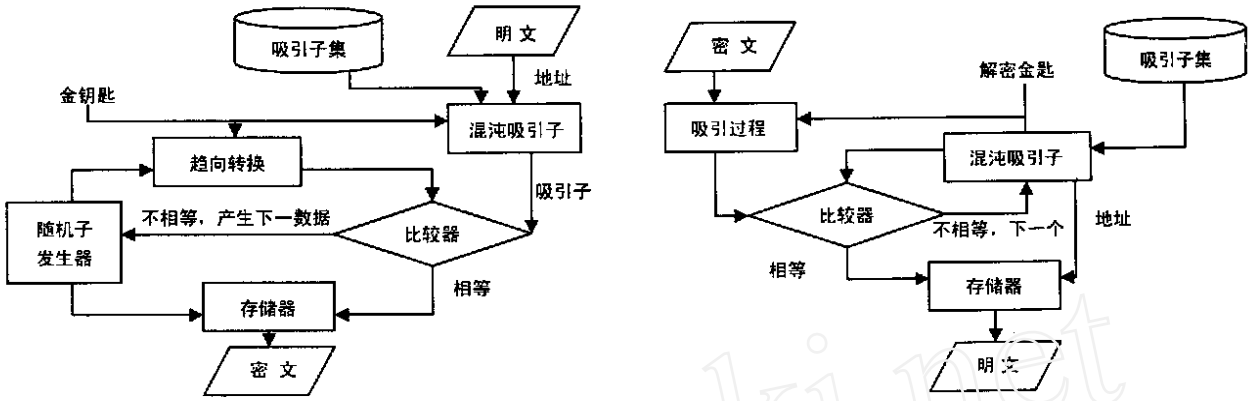
(3) 发射端和接收端之间达到同步所需的时间还未能从理论上计算出来,需要进一步深入探讨。

2. 混沌吸引子在保密通信中的应用

除了上述基于混沌同步的保密通信外,还可以基于混沌吸引子来进行保密通信,它避免了同步混沌通信系统中必须要求收发两端严格同步的诸多麻烦和不便。目前,它主要有 2 种类型,一类是基于神经网络的混沌吸引子几率式对称加密[30],另一类是基于混沌吸引子不稳定周期轨道的加密通信[31]。

基于神经网络的混沌吸引子几率式加密系统主要是依据改进后的 Hopfield 神经网络中吸引子的混沌特性,以置换矩阵 H 和编码矩阵 M 为密钥(即金钥匙)进行几率式对称分组加密,其加密和解密系统框图如图 3 所示。

这种保密通信方式如果采用较多的神经元则具有较强的实际安全性,例如采用穷举攻击法,当神经元个数 N = 32,计算机的处理能力为 10^9 条指令/秒时,找到一个正确的 H 需时 1 017 年,又由于吸引子的混沌性分布和吸引域的混沌性,所以它抗差分攻击能力较强。



(a) 加密框图　　(b) 解密框图

图 3　神经网络混沌加密算法的原理框图

而基于混沌吸引子不稳定周期轨道的加密通信则主要是根据“一个混沌吸引子是由无穷多个不稳定的周期轨道所组成的”,通过对不稳定周期轨道的幅度或相位进行调制,则可实现对信息的保密传输。例如当细胞神经元的运动方程采用最简单的伊依映射(Henon Map)时,即

$$\begin{cases} x_{n+1} = 1.4 + 0.3y_n - x_n^2 \\ y_{n+1} = x_n \end{cases} \quad (17)$$

在某个计算精度范围内通过迭代方程(17)可发现存在一条不稳定周期 4 的轨道,即:(0.305,0.893) →(1.575,0.305) →(-0.989,1.571) →(0.893,-0.989) →(0.305,0.893) →…并称二维平面上的这些点分别为 A、B、C 和 D。从任一初始点出发都将经历该不稳定周期轨道,但该不稳定周期轨道出现的频率和初次出现所需的迭代次数均与初始值有关,以此可以进行信息编码,如以 A 状态作为编码的起点,D 状态作为校验位,通过取舍 B、C 两状态来记录信息 00、01、10 和 11,于是一个不稳定周期 4 的序列就可以编码为两位二进制信息。对于这种保密通信方式有 2 个主要问题还未解决好,一个是通过伊依映射的不稳定周期轨道 P4 传输信息的效率太低,如当初始值为(0.303000,0.893000)时,只有在迭代次数为 23222、26174、30249 和 73405…时才经历不稳定周期轨道 P4,在迭代 526353 次中只有 32 次出现不稳定周期轨道 P4;另一个问题目前还无法定量评估这种保密通信的安全性。

四、总结与展望

经过 10 多年对混沌神经网络系统的研究,已取得了一系列的成果,包括对混沌神经元的模型、特性和学习算法的理论研究成果,以及在信息工程中的应用研究成果,尤其是在保密通信的应用方面,基于混沌神经网络的非线性动力学特性与复杂性,已提出了较完整的加密通信方案,进行较完备的理论分析与实验研究,如基于混沌同步或混沌吸引子的加密通信方案,从而为工程实际应用提供了良好的理论和实验基础,但仍存在许多问题尚未解决,例如:混沌同步保密通信中混沌系统的参数匹配问题、在基于混沌吸引子对称加密中大规模 Hopfield 神经元互联特性在器件兑现方面的问题等等,有待于今后进一步研究解决。

今后有关混沌神经网络及其在加密通信中的应用需进一步研究的主要课题有:

(1)对混沌神经网络模型及其混沌特性与复杂性的进一步研究。在这一方面既可以对已提出混沌神经元结构进行调整和改进,也对多维超混沌神经网络系统进行新的研究,从而给出更适合于加密应用的混沌神经网络的混沌吸引或混沌同步算法,尤其是在公开钥密码算法思想指导下实现基于混沌神经网络技术的加密通信;

(2)根据所提出的基于混沌神经网络密码算法方案,就具体的信息系统设计出具有混沌神经网络加密与解密功能的专用集成芯片,实现利用硬件对信息加解密,提高信息加解密速度与稳定性,实现信

息的实时加密通信;

(3)加强对基于混沌加密系统安全性的理论研究。基于混沌吸引子的几率式对称加密通信安全性理论上已有初步的证明,有待于进一步完整,而基于混沌同步的加密通信安全与否至今还没见到数学上的理论证明。

参 考 文 献

[1] K. Aihara, T. Takabe, M. Toyoda. Chaotic neural network [J]. Physics Letters A, 12 March 1990, Vol. 144 No. 6/7, pp. 333～340.

[2] 郭东辉,吕迎阳,刘瑞堂,等. 神经网络及其在网络通信中的应用研究[J]. 厦门大学学报(自然科学版),2001, 40(2):283～292.

[3] T. Kwok, K. A. Smith. Experimental analysis of chaotic neural network models for combinatorial optimization under a unifying framework [J]. Neural Networks, 13(2000), pp. 731～744.

[4] 荆涛,徐勇. 混沌神经网络编码研究 [J]. 系统工程与电子技术,1999,21,(2):32～38.

[5] 张毅锋,杨绿溪,何振亚. 混沌神经网络及其在联想记忆中的应用[J]. 电路与系统学报,1998,3(4):37～43.

[6] Wang Yong, You Xiaohu, Chen Ming, et al. Comparison of two neural networks in MC - CDMA multi - user detection [J]. Journal of Southeast University, 1999, 15(1):15～19.

[7] Z. Tan, M. K. Ali. Associative memory using synchronization in a chaotic neural network [J]. International Journal of modern physics C, 2001, 12(1): 19～29.

[8] 颜森林,伍仕宝,逄涣刚,等. 耦和负反馈超混沌系统及在编码通信中的应用[J]. 应用科学学报,2001,19(3):218～223.

[9] Han - Go Choi, Ho - Sub Lee, Sang - Hee Kim, et al. Adaptive prediction of nonstationary signals using chaotic neural networks[A]. IEEE World Congress on Computational Intelligence[C], 1998, Vol. 3, pp. 1943～1947.

[10] V. Milanovic, M. E. Zaghloul. Synchronization of chaotic neural networks and applications to communications [J]. International Journal of Bifurcation and Chaos, 1997, 7(1):28～31.

[11] Guo Donghui, L. M. Cheng, L. L. Cheng. A new symmetric probabilistic encryption scheme based on chaotic attractors of neural networks [J]. Applied Intelligence, 1999, 10(1): 71～84.

[12] T. Yang, L. B. Yang, C. M. Yang. Application of neural networks to unmasking chaotic secure communication [J]. Physica D, 1998, 124(1～3):248～257.

[13] Tao Yang. Chaotic secure communication systems: History and new results [J]. Telecommunications review, 1999, 9(4):597～634.

[14] 任晓林,胡光锐,谭政华. 混沌神经网络的同步及其在保密通信中的应用 [J]. 上海交通大学学报,2000, 34(6):744～747.

[15] S. Worlfram. Cryptography with cellular automata [A]. Proc. Crypto '85[C], 1986, pp. 524～534.

[16] J. J. Hopfield. Neural networks and physical systems with emergent collective computational abilities[A]. Proc. Natl. Acad. Sci[C]. USA, 1982, Vol. 79, pp. 2554～2558.

[17] L. Chen K. Aihara. Strange attractor in chaotic neural networks [J]. IEEE Transactions on Circuits and System - Ⅰ, 2000, Vol. 47, No. 10, pp. 1455～1468.

[18] L. Chen, K. Aihara. Chaotic simulated annealing by a neural network model with transient chaos [J]. Neural Networks, 1995, Vol. 8, No. 6, pp. 915～930.

[19] Inoue M., Nagayoshi A.. A chaos neuro - computer [J]. Physics Letter A, Vol. 158, No. 8, pp. 373～376.

[20] Inoue M., Fukushima S.. A neural network of chaotic oscillators[J]. Progress Theoretical Physics, 1992, Vol. 87, No. 3, pp. 771～774.

[21] Donghui Guo, Zhenxiang Chen, Ruitang Liu, et el. A modified Hopfield model of neural network [J]. Journal of Xiamen University (Natural), 1993, Vol. 32, No. 1, pp. 33～40.

[22] Radu Dogaru, Leon O. Chua. Universal CNN cells [J]. International Journal of Bifurcation and Chaos, 1999, Vol. 9, No. 1, pp. 1～48.

[23] Heinz Georg Schuster. Deterministic Chaos: An Introduction [M]. Deutsche Bibliothek, Cataloguing - in - Publication Data. 1984, pp. 15～30.

[24] Louis M. Pecora, Thomas L. Carroll, Synchronization in chaotic systems [J]. Physical Review Letters, 1990, Vol. 64, No. 8, pp. 821～824.

[25] 沈世镒著. 神经网络系统理论及其应用[M]. 北京:科学出版社,1998:66～92.

[26] T. Yang, C. W. Wu, L. O. Chua. Cryptography based on chaotic systems [J]. IEEE Transactions on Circuits and System - Ⅰ, 1997, Vol. 44, No. 5, pp. 469～472.

[27] Tao Yang, Leon O. Chua. Impulsive stabilization for control and synchronization of chaotic system: Theory and application to secure communication [J]. IEEE Transactions on Circuits and System - Ⅰ, 1997, Vol. 44, No. 10, pp. 976～988.

[28] Tao Yang, Leon O. Chua. Chaotic impulse radio: A novel chaotic secure communication system [J]. International Journal of Bifurcation and Chaos, 2000. Vol. 10, No. 2, pp. 345～357.

[29] 蒋国平. 基于细胞神经网络超混沌系统的扩频保密通信[J]. 南京邮电学院学报,2000,20(3):5～10.

[30] 郭东辉,何小娟,陈彩生. 基于神经网络混沌加密算法的专用芯片设计[J]. 计算机学报,2000,23(11):230～232.

[31] Henry D. I. Abarbanel, Paul S. Linsay. Secure communications and unstable periodic orbits of strange attractors[J]. IEEE Transactions on Circuits and Systems - Ⅱ, 1993, Vol. 40, No. 10, pp. 643～645.

作者简介

刘年生(1967 -),男,湖北红安人,博士,副教授,主要从事人工智能、网络通信等方面的科研与教学工作;

郭东辉(1967 -),福建莆田人,博士,教授;

吴伯僖(1926 -),福建泉州人,教授,博士生导师。