基于神经网络混沌扩频序列的研究 [1]

刘联会 石 军 李白萍 王建新

(西安科技大学 通信与信息工程学院 西安 710054)

摘 要: 应用神经网络的强大学习能力和具有全局最优的 BP 改进算法，提出了通过训练学习建立的具有混沌性态的优化神经网络模型；利用网络权值调整的灵活性来产生混沌序列，该模型序列更换容易并且数量巨大。实验与分析结果表明该模型产生的混沌扩频序列具有良好的相关特性、平衡特性以及理想的线性复杂度，是最优加密密钥及扩频码的优选码型之一。

关键词: 混沌扩频序列，神经网络模型，相关函数，线性复杂度

中图分类号: TN914.5, TN-052 **文献标识码**: A **文章编号**: 1009-5896(2004)01-0137-05

Study of Chaotic Spread-Spectrum Sequences Based on Neural Networks

Liu Lian-hui Shi Jun Li Bai-ping Wang Jian-xin

(*School of Comm. and info. Eng., Xi'an Univ. of Sci. & Tech., Xi'an* 710054, *China*)

Abstract The chaos generation neural network based on the excellent learning ability and synaptic weight database are built to generate many chaotic spread-spectrum sequences trained by the modified back-propagation algorithm with various discrete chaotic time series. The chaotic sequences are very easily generated by changing weights of neural network model, and their number is large. The computer simulation results show that the output chaotic sequences have good correlation property, balance property and linear complexity, therefore they are good candidates for the optimal encrypting code and the spread spectrum code.

Key words Chaotic spread-spectrum sequences, Neural networks model, Correlation function, Linear complexity

1 引言

近几年来，各种文献中所讨论的或给出的混沌序列设计方案大都是基于单一的混沌映射模型来进行设计和分析的[1]，由于受微处理器字长的限制，有限长混沌序列的统计特性与理论值存在很大的差异，因此，局限性很大。有鉴于此，本文提出一种基于 BP 算法神经网络的混沌序列产生方法，此种方法可在统一的系统结构模型下，通过对权值的不同调用来产生比单一混沌映射更多的、符合扩频通信要求的扩频信号。采用 BP 算法的优点在于它的半行结构，即输入数据流从输入层流向输出层，而误差信号从输出层流向输入层。同时，模型的建立也改善了通信系统的保密性能。

2 神经网络混沌序列产生的系统模型

一般地，单层单个神经元感知器常用的激励函数有 S 型函数、双曲函数以及阈值函数等，取其输出层的神经元为线性元，则输出可表示为下式：

$$y=\sum_{i=0}^{n}\omega_i\frac{1}{1+e^{-(u_ix+\theta_i)}}+\theta \tag{1}$$

[1] 2002-07-22 收到，2003-03-06 改回

式中 ω_i 和 θ_i 分别为权系数和阈值，u_i 和 θ 为常数。其展开基函数为 $f(x_i)=1/[1+e^{-(u_i x+\theta_i)}]$，由于 u_i 是任意函数，所以 $f(x_i)$ 是一无穷函数的集合。显然，当 u_i 取不同的值时，它是一个非正交但却是线性独立的函数集合，可以证明任一线性独立函数均可以通过 Schimidt 正交变换使之正交化，故可用它来展开任意函数，因此，神经网络具有强大的学习能力以及能够以任意精度逼近非线性函数的能力，通过对混沌序列的学习和建模是可以具有混沌性态的。

基于神经网络的混沌扩频序列产生的系统模型如图 1 所示。

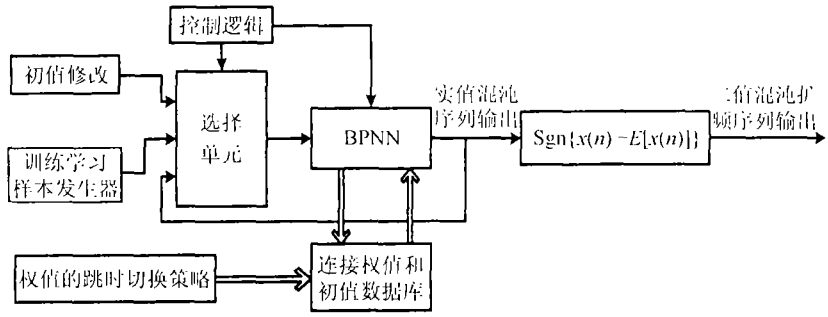

图 1 基于神经网络的混沌扩频序列的产生系统模型

3 BP 算法的改进

对 BP 算法 [2,3] 改进之一是步长 η 的修正，为了克服选择步长的困难，提出步长的修正公式为

$$\eta(n)=(1+\varepsilon\lambda)\eta(n-1) \tag{2}$$

式中 ε 为小于 1 的正常数，$\lambda=\mathrm{sgn}[\partial E/\partial\omega(n)\cdot\partial E/\partial\omega(n-1)]$。

改进之二是对 (隐层) 误差反传因子乘以一个小于 1 的正常数因子 β，以提高建模精度。

改进的 BP 算法训练神经网络得到网络权值和阈值的基本公式为

对输出层：

$$\omega_{jk}(k+1)=\omega_{jk}(k)+\eta_1(k)\delta_k\beta_1 O_j+\alpha_1[\omega_{jk}(k)-\omega_{jk}(k-1)] \tag{3}$$

$$\theta_k(k+1)=\theta_k(k)+\eta_2(k)\delta_k+\alpha_2[\theta_k(k)-\theta_k(k-1)] \tag{4}$$

对隐层：

$$\omega_{ij}(k+1)=\omega_{ij}(k)+\eta_3(k)\delta_j\beta_2 O_i+\alpha_3[\omega_{ij}(k)-\omega_{ij}(k-1)] \tag{5}$$

$$\theta_j(k+1)=\theta_j(k)+\eta_4(k)\delta_j+\alpha_4[\theta_j(k)-\theta_j(k-1)] \tag{6}$$

式中 δ_k,θ_k 分别是输出层的反传误差因子和阈值；δ_j，θ_j 分别是隐层的反传误差因子和阈值；ω_{ij} 是输入层和隐层节点之间的连接权值；ω_{jk} 是隐层和输出层节点之间的连接权值；在式 (3)–(6) 中，η_1,η_2,η_3 和 η_4 的取值按式 (2) 变化，可以不同，也可以相同，这也适用于 $\alpha_1,\alpha_2,\alpha_3$ 和 α_4 的取值；O_i,O_j 分别是隐层和输出层节点 (神经元) 的输出。

由于 BP 网络中隐层节点使用的是 sigmoid 函数，其值在输入空间中无限大的范围内为非零值，因而是一种全局逼近的神经网络。

4 BP 算法对混沌序列的学习策略

神经网络利用 BP 算法学习某一非线性映射关系时，由于训练序列是混沌序列，不具有重复性，因此，BP 网络学习及权值调整采用的是同步工作方式。

本文选择 ICMIC(Iterative Chaotic Map with Infinite Collapses) 映射 [4]$y = \sin(a/x)$，$a \in (0, +\infty)$ 作为训练样本，BP 神经网络采用 3: 8: 1 结构. 图 2 和图 3 分别给出了 ICMIC 映射的分岔图和 Lyapunov 指数分布图.

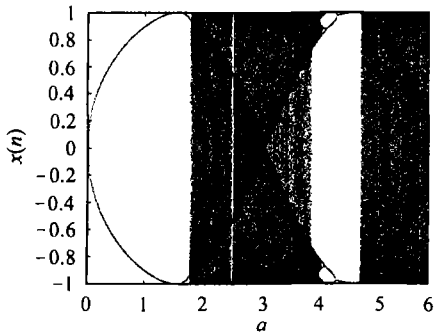

图 2　ICMIC 混沌映射参数 a 在 [0,6] 区间内分岔图

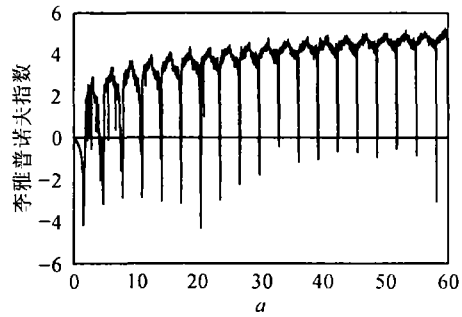

图 3　ICMIC 映射参数 a 在 [0,60] 区间的 Lyapunov 指数分布图

图 4 给出了 ICMIC 映射及神经网络逼近 ICMIC 映射得到 ICMIC 混沌神经网络的吸引子. 由图 4 可知，混沌神经网络的吸引子与原系统的非常相似. 经计算，ICMIC 混沌神经网络的 Lyapunov 指数 [5] 为 8.3704，而 ICMIC 混沌映射的为 8.3736，这说明神经网络很适合混沌系统的建模.

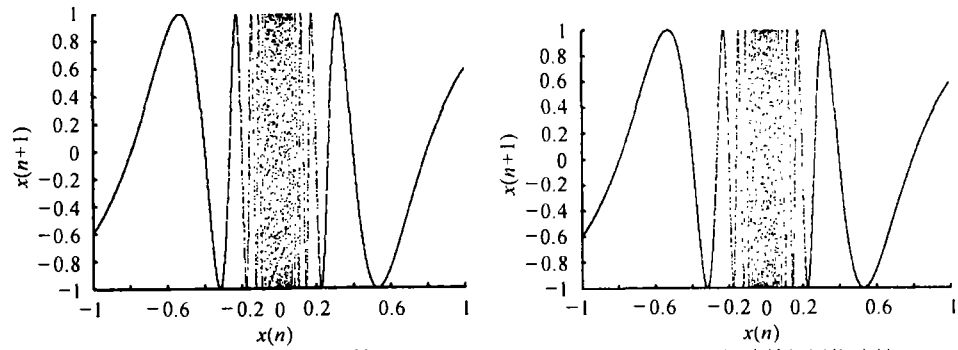

图 4　ICMIC 混沌系统与其神经网络逼近的吸引子

5 试验结果及性能分析

5.1 相关特性　设 $\{a(n)\ \ n = 1, 2, \cdots, N\}$ 为神经网络基于某一特定混沌映射所产生的某一混沌扩频序列，则它的归一化自相关函数可定义为 $c_a(m) = \frac{1}{N}\sum_{n=1}^{N} a(n)a(n+m), -M \le m \le M$. 式中 M 为相关间隔范围，其值等于 4000，下同. 图 5(a) 给出了长为 4096 的 ICMIC 映射混沌扩频序列归一化自相关函数，由图可知混沌序列 $\{a(n)\}$ 在相关间隔 0 处的自相关值近似为 1，自相关旁瓣值小于 0.1，因此此序列的自相关特性好.

设 $\{a(n), b(n)\ \ n = 1, 2, \cdots, N\}$ 为神经网络基于某一特定混沌映射所产生的两个混沌扩频序列，则它们的归一化互相关函数可定义为 $c_{a,b}(m) = \frac{1}{N}\sum_{n=1}^{N} a(n)b(n+m), -M \le m \le M$.

图 5(b) 给出了该混沌序列归一化互相关函数，由图可知混沌序列 $\{a(n),b(n)\}$ 的互相关值亦小于 0.1，因此，此序列的互相关特性也良好。

由以上可知混沌扩频序列的自相关函数具有 $\delta(t)$ 函数的特性，具有宽带特性，其互相关性很弱，因此，对它的同步和捕捉与传统扩频序列是完全一致的。

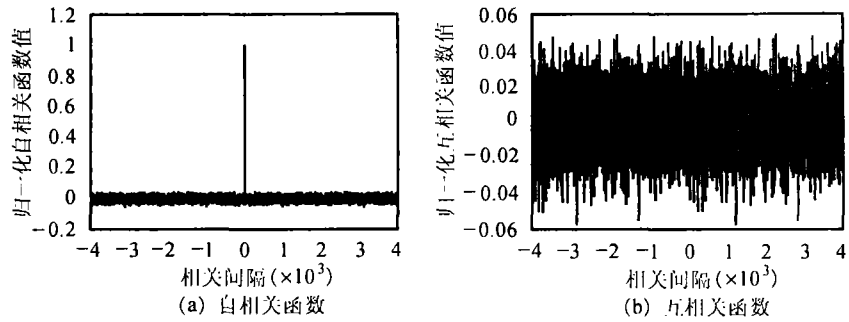

图 5 自相关函数与互相关函数特性

另外，图 6 给出了序列相关值与其周期的关系。由图 6(a) 和图 6(b) 可看出，随着周期的增大，混沌扩频序列的相关特性变好。其中：图 6(a) 是 ICMIC 映射混沌扩频序列的最大归一化自相关旁瓣绝对值与周期之间的关系，图 6(b) 是该混沌序列的最大归一化互相关绝对值与周期之间的关系。

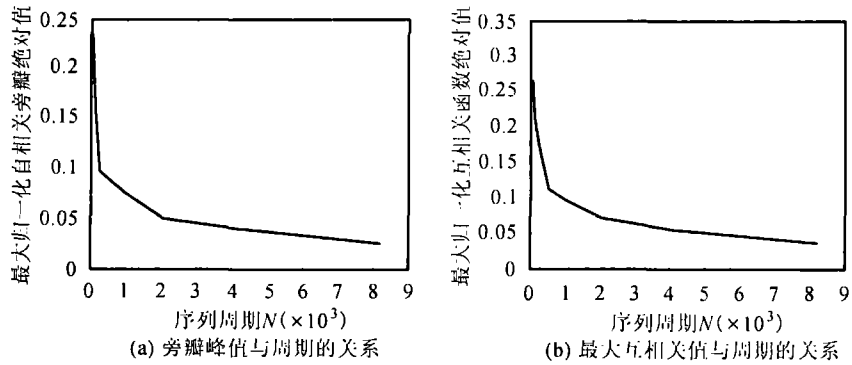

图 6 相关值与序列周期的关系

5.2 平衡性 图 7 给出了 ICMIC 映射混沌扩频序列的平衡性能分布曲线。平衡性反映了序列对载波的抑制程度。在 DS 扩频系统中，扩频码不平衡的 DS 系统载漏增大，这将破坏扩频通信系统的抗干扰以及抗侦破的能力。设混沌扩频序列 $\{a(n)\}$ 中“1”的数目与“−1”的数目之差为 L，由图 7 可知，随着周期的增大，混沌扩频序列的平衡性能逐渐得到改善。

5.3 线性复杂度 图 8 给出了 ICMIC 映射混沌扩频序列的线性复杂度。线性复杂度即序列的等效线性长度 [6]，当序列被用作密码中的密钥流时，序列的线性复杂度就是评价该序列优劣的重要指标。由图 8 可知，序列的线性复杂度接近 $y=x/2$ 这条曲线，即混沌扩频序列的线性复杂度与序列长度的一半符合得很好，因此，混沌扩频序列有可能成为一种可实际被选用的流密码体制。本质上，混沌扩频序列是独立均匀分布的二元随机序列，其线性复杂度的数学期望约为序列长度的一半，方差约为 86/81，具有理想的复杂度特性。

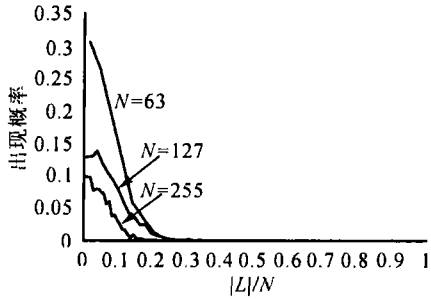

图 7　混沌扩频序列的平衡性能分布曲线

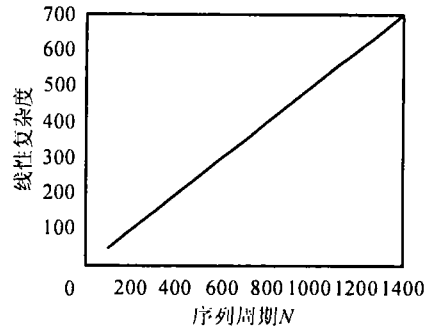

图 8　混沌扩频序列的线性复杂度

6 结论

应用具有全局最优的 BP 改进算法，提出了基于神经网络的混沌扩频序列产生方法。实验结果表明：与传统的扩频序列 (由移位寄存器产生，如 Gold 序列、 m 序列等，其主要缺点是数目有限并且复杂度低等) 相比，该模型产生的混沌扩频序列具有数量巨大、良好的自互相关特性、平衡特性及理想的线性复杂度，并且扩频序列产生容易，在适当的混沌模型参数与隔次迭代次数条件下，可产生比传统扩频序列自相关旁瓣峰值、互相关峰值更低的扩频序列，因此其抗多址和多径性能良好，同时也能提高小区的软信道容量，尤其适用于 CDMA 和保密通信系统。实际使用时，根据需要调用数据库中的相应权值和初始值，就可以在统一的网络结构下产生所需要的混沌扩频序列。因此，只需给不同的用户分配不同的初值和权值数据库中的检索号，即可进行迭代产生相应的混沌扩频序列。在一定的条件下，混沌序列的周期任意，可根据需要，以任意较长的周期截短。为了增强系统的通信保密性能，可采用复合混沌映射作为训练样本或辅以权值跳时切换策略，即在不同的时间段内调用不同的网络权值。可以断言，混沌扩频序列在 CDMA 和保密通信技术中有极其良好的应用前景。

参　考　文　献

[1] 王亥，胡健栋. 改进型 Logistic-Map 混沌扩频序列 [J]. 通信学报， 1997, 18(8): 19–23.

[2] 易继锴，侯媛彬. 智能控制技术 [M]. 北京：北京工业大学出版社， 1999: 102–108.

[3] 张家树，肖先赐. 基于神经网络的混沌信号源的设计及同步 [J]. 电子与信息学报， 2002, 24(1): 37–44 .

[4] He D, He C, Jiang L G, *et al.*. A chaotic map with infinite collapses[A]. IEEE 2000 tencon Proc., Kuala Lumpur, Malaysia, Sept. 2000, III: 95–99.

[5] Rosenstein M T, Collins J J, Luca C J. A practical method for calculating largest Lyapunov exponents from small data sets[J]. *Physica D*, 1993, 65(1/2): 117–134.

[6] Massey J L. Shift-register synthesis and BCH decoding[J]. *IEEE Trans. on Info. Theory*, 1969, 15(1): 122–127.

刘联会：　男，1946 年生，教授，陕西省电子学会信息与通信学会委员，长期从事信息与通信工程的教学与研究工作.

石　军：　男，1975 年生，硕士，研究方向为混沌在移动通信系统中的应用.

李白萍：　女，1965 年生，副教授，在职博士生.

王建新：　男，1967 年生，工程师，在职博士生.