基于径向基神经网络的混沌加密方案

王 喆，陈 玲，朱双鹤
(空军工程大学 电讯工程学院，陕西 西安 710077)

摘 要：提出了一种基于径向基(RBF)网络的混沌序列产生方法，并基于这种模型提出了一种新的混沌加密方案。计算机仿真证明利用RBF网络良好的逼近任意非线性映射和处理系统内在的难以解析表达的规律性的能力，及快速的收敛速度，在统一的系统结构下通过权值的切换方式(即用不同的混沌映射)可产生比单一混沌映射更多的、性能更接近理论值的混沌序列，同时基于该模型的混沌加密方案具有高度的保密性和灵敏性。

关键词：径向基(RBF)网络；混沌序列；加密
中图分类号：TN914　　**文献标识码**：A　　**文章编号**：1009-3516(2003)03-0055-03

目前许多文献中讨论和给出的混沌保密通信方案都是基于单一的混沌映射模型进行设计和分析[1]。由于计算精度的限制，实际中只能产生有限长的混沌序列，有限长的混沌序列的统计性能与理论值(无限长时)存在很大差异[2]，这就限制了基于单一混沌映射产生的、能够同时满足自相关和互相关性能的混沌序列的数量。解决此问题的可能方案是采用多个混沌系统来进行设计，但不同的混沌系统均需要单独设计，且一旦完成设计，其系统结构和参数的变更就难以实现，而且映射关系可以用显式给出，具有一定的被破译风险。利用神经网络产生混沌序列，只需充分利用神经网络的灵活性，在统一的系统结构下，通过变更网络的连接权值就可实现不同混沌系统产生的各种混沌序列[3]，同时将混沌映射关系变为隐式形式，使其更具隐蔽性。本文提出了一种基于径向基(RBF)网络的混沌序列产生方法，利用RBF网络良好的逼近任意非线性映射和处理系统内在的难以解析表达的规律性的能力，及快速的收敛速度，在统一的系统结构下通过权值的切换方式(即用不同的混沌映射)来产生比单一混沌映射更多的、性能更接近理论值的混沌序列，最后在此基础上提出了一种新的混沌加密方案。

1 建立具有混沌性态的RBF网络

1.1 RBF网络模型

RBF网络结构如图1所示。RBF网络完成映射$f:R^n \to R^m$，其数学表达式为

$$f_i(x)=\theta_0+\sum_{j=1}^{h}\theta_{ij}\Phi(\|x-c_j\|) \qquad i=1,2,\cdots,m \quad (1)$$

式中，$x\in R^n$为网络的输入向量，c_j为网络的隐层中心点，其值可用N-MEANS法确定，$\|\cdot\|$表示范数，这里取欧几里德范数，$\Phi(\cdot)$称为径向基函数，完成从$R^n \to R^m$的非线性变换，这里取高斯函数，其形式为

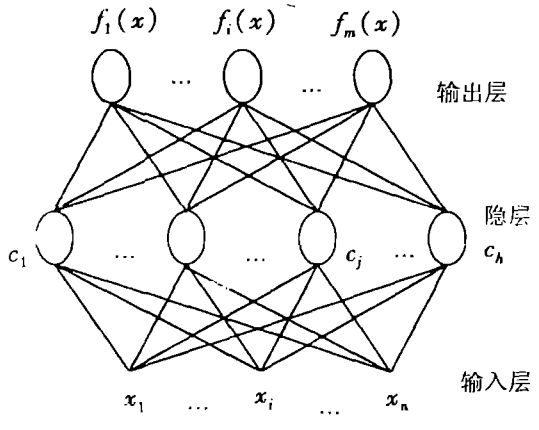


图1 RBF网络结构

收稿日期：2002-10-11
基金项目：陕西省自然科学基金资助项目(2001X32)
作者简介：王 喆(1973-)，女，陕西西安人，硕士生，主要从事混沌通信技术研究；
朱双鹤(1940-)，男，河南清丰人，教授，主要从事混沌理论及智能信息处理研究.

$$\Phi(\|x-c_j\|)=\exp\left(\frac{-\|x-c_j\|^2}{\beta^2}\right) \tag{2}$$

式中,β 为宽度值,一般为常数,这里取 $\beta=1.2$。$\theta_{ij}(1\leqslant i\leqslant m,1\leqslant j\leqslant h)$ 为网络的各层之间的连接权值,θ_0为网络的偏置。

1.2 产生混沌序列的 RBF 网络模型

RBF 网络具有良好的逼近任意非线性映射的能力,因此该网络通过对混沌序列的学习和建模可具有混沌性态。基于 RBF 神经网络的混沌序列产生模型系统结构如图 2 所示。网络连接权值和初值数据库用来存储由学习样本训练好的网络权值和相应的初值。由网络的输出至输入端的反馈形成闭环结构,使输出的混沌序列反馈至输入端,作为下次输出序列的初始值,从而可以源源不断的输出混沌序列。最后将网络产生的模拟混沌序列按式(3)转化成二进制混沌序列。

$$a_n=\begin{cases}1 & x_n\geqslant c\\ -1 & x<c\end{cases} \tag{3}$$

式中 c 表示采用非线性量化法的分点。

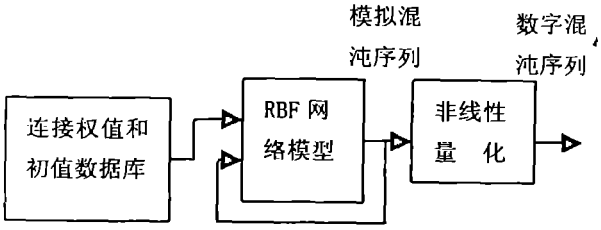
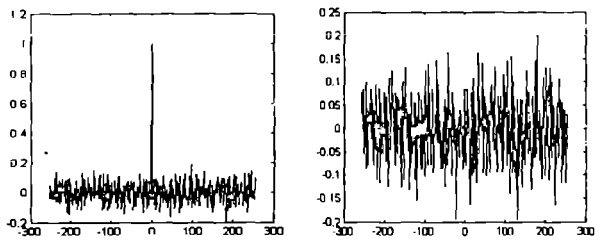


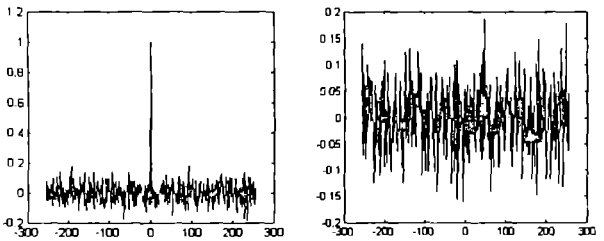
图2 产生混沌序列的 RBF 网络模型系统结构

利用以上模型我们对被广泛研究且具有良好相关性能的 Full - Logistic 映射和 Henon 映射进行了实验仿真,RBF 网络采用 3 层结构:输入、隐含、输出,每层节点数比例为 1:8:1,序列长度取为 $N=1\,024$,相关间隔范围 $M=1\,000$。图 3 和图 4 分别给出了用这种算法产生的 2 种有限长混沌序列的自相关函数和互相关函数,由图可见,利用这种算法产生的混沌序列的自相关和互相关特性良好。



(a) 自相关函数 (b) 互相关函数

图3 Full - Logistic 映射的自相关和互相关函数



(a) 自相关函数 (b) 互相关函数

图4 Henon 映射的自相关和互相关函数

2 基于 RBF 网络混沌序列产生模型的混沌加密方案

基于 RBF 网络的混沌序列产生模型可以由统一的系统结构通过切换权值来产生不同的混沌映射,可以很方便地在同一系统中将多个混沌映射级联起来,以生成周期更长的、性能更接近于理论值的混沌序列,从而克服了有限精度对混沌序列性能的影响(原理如图 5 所示)。另一方面,只需对该模型的连接权值和初值数据库中的数据分组号进行编码,就可采用一次一秘密码体制[4]进行信息加密,密钥 K 是连接权值和初值数据库中的数据分组号,用户只需按分组号产生相同的密钥流进行解码就可实现保密通信,由于密钥流 L 为隐式形式,又采用了一次一秘密码体制,因而这种加密体制保密度极高。

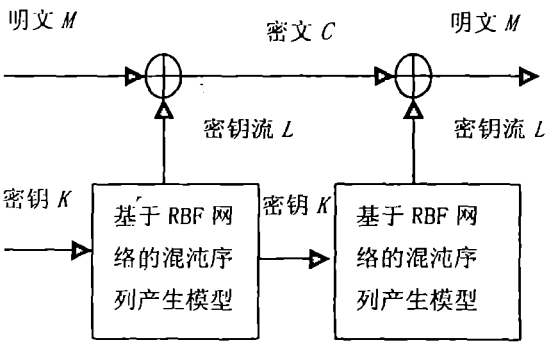
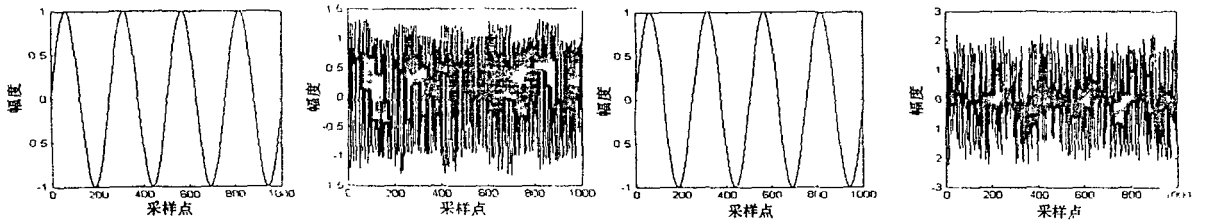


图5 RBF 网络混沌序列产生模型的混沌加密系统原理框图

下面,通过 Full - Logistic 映射和 Henon 映射进行仿真证明新的混沌加密方案的有效性和敏感性。采用高频正弦信号作为信息信号,$s(t)=0.05\sin(0.025t)$,通过对 Full - Logistic 映射和 Henon 映射的网络连接权值和初值分组号进行适当编码,再按编码索取分组号产生混沌映射对信息信号进行加密,然后按反码对信息信号进行解密,图 6 为加解密仿真图。由图可见,信息信号和恢复信号几乎完全相同。随机改变反码中的网络连接权值和初值分组号,就无法恢复出原始信息信号(如图 6(d)所示)。



(a)信息信号　(b)加密后的信号　(c)恢复信号　(d)错误恢复的信号

图6　基于 RBF 网络的混沌序列产生模型的混沌加密方案仿真

3　结束语

本文首先提出了一种基于 RBF 网络的混沌序列产生方法,然后基于这种模型提出了一种新的混沌加密方案。计算机仿真证明利用 RBF 网络良好的逼近任意非线性映射和处理系统内在的难以解析表达的规律性的能力,及快速的收敛速度,在统一的系统结构下通过权值的切换方式(即用不同的混沌映射)可产生比单一混沌映射更多的、性能更接近理论值的混沌序列,同时基于该模型的混沌加密方案具有高度的保密性和灵敏性。实际应用时只需根据需要来改变网络连接权值和初值分组号即可产生所需的混沌序列进行加密,从而不需要针对不同的混沌映射去设计相应的结构,同时系统具有高度的保密性。

参考文献:

[1] 郑会永. 混沌及混沌保密通信技术[J]. 中国图象图形学报, 1999,12:1042 - 1050.
[2] 王　亥,胡建栋. Logistic - Map 混沌扩频序列[J]. 电子学报,1997,25(1):19 - 23.
[3] 万继红. 一种新的混沌扩频序列产生方法[J]. 电讯技术 ,2000,(4):47 - 52.
[4] 李振玉. 现代通信中的编码技术[M]. 中国铁道出版社,1996.
[5] 朱双鹤,李小春,曲　毅,等. 一种新的混沌掩盖保密通信方案[J]. 空军工程大学学报(自然科学版),2002,3(6):37 - 40.

(编辑:门向生)

Chaotic Encryption Based on RBF Neural Networks

WANG Zhe,　CHEN Ling,　ZHU Shuang - he
(The Telecommunication Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710077, China)

Abstract: A new chaotic sequence generation method, based on the RBF neural network, which has the strong learning ability and nonlinear function approximation capacity and a new chaotic encryption with this method are proposed in this paper. Experimental results show that this scheme can very easily generate much more chaotic sequences with desirable statistical properties than single chaotic map by changing weights of this RBF neural network and this new chaotic encryption has higher security and sensitirity.

Key words: RBF neural network; chaotic sequence; encryption