

# 基于神经网络库存融合控制技术

陈承贵, 罗克露

(怀化职业技术学院, 湖南 怀化 418000)

**摘要:** 神经网络控制系统通常会面临多种选择, 如样本的训练方式、神经网络的算法等, 不好的选择会降低预测率。BP(Back Propagation)神经网络库存控制系统融合多种库存控制技术, 利用BP算法对学习的精度和收敛的速度进行改进, 能比较精确地预测库存。讨论了有关BP神经网络的算法及算法改进等问题, 以品牌服装库存控制为例, 提出用神经网络的多层感知器实现库存融合控制。

**关键词:** 神经网络; 预测; 多层感知器; BP算法; 库存

中图分类号: TP301.6

文献标识码: A

## Neural network-based inventory control technology integration

CHEN Cheng Gui, LUO Ke Lu

(Huaihua Vocational and Technical College, Huaihua 418000, China)

**Abstract:** There are a number of choices for neural network control system, such as the training method of the sample, the algorithm of the neural network. It will reduce the forecast rate if you make a bad choice. BP(Back Propagation) neural network inventory control system integrates a variety of inventory control techniques, it can use BP algorithm to improve the accuracy of the studies and the speed of the convergence, it can also calculate inventory more accurately. This paper discusses the algorithm of the neural network and the improvement of the algorithm. Take the case of branded clothing inventory control, realize the control of inventory integrating by using the multilayered perceptron of neural network.

**Key words:** neural network; forecast; multilayer perceptron; BP algorithm; stock

在库存管理中体现库存的典型指标有需求量、库存控制量、销售周期、期初库存量、阶段批量订货等。传统的商业库存控制方法如ABC、EOQ和季节控制管理等都因为单一控制而无法实现对数据的精准预测。基于BP神经网络技术可以解决传统商业库存控制方式的不足。神经网络NN(Neural Networks)在数据挖掘中的应用近年来已成为研究热点。其应用涉及商业、安全和环境等多方面领域, 可用于库存与销售、访问控制、地学分析与预测、目标识别、模糊控制、故障诊断及基于BP网络的医疗保健管理系统等。

基于任何一种神经网络的库存控制都要受到多种限制, 如训练样本的依次学习, 前面学习的知识容易被后面的学习经验掩盖, 从而利用部分样本的知识对全局网络的推广应用, 降低数据的精确度等。企业库存控制量影响因素很多, 有供应商的, 也有企业本身的, 还有客户的, 同时跟经济和气候的变化也有密切的关系。神经网络算法在典型算法的基础上有很多变种。而算法的改进对库存的控

制又显得至关重要, 这也是目前研究预测库存控制的重点。神经网络对库存应用已经实现了库存灰色预测、动态预测的研究。然而, 由于样本的依次训练方式, 库存管理的单一, 无法保证数据预测的准确。如何改变样本的学习方法, 提高库存输出算法和系统的性能, 是神经网络改进算法的库存控制问题。本文首先讨论BP神经网络结构和算法, 并以品牌服装的库存控制为例, 讨论BP神经网络的改进算法及系统结构。

### 1 BP神经网络

神经网络对分类或预测是一种很好的数据挖掘技术, 但是, 在实际应用中, 怎样对数据预测产生更好的精度和更高的效率, 成为神经网络研究的重点。

1986年Rumelhart D E等<sup>[1]</sup>提出了后向传播模型BP算法, 该算法通过迭代处理一组选定的训练样本, 将每个样本的网络预测与实际知道的类标号进行比较, 然后进行网络学习。针对每个训练样本, 修改权重值, 使得网络预测

值与实际类之间的均方差最小。BP算法分为2个阶段：计算学习阶段和修改阶段。计算学习阶段，输入信息由输入层经每个隐层到输出层，计算每个单元的实际输出值，也称为正向传播；修改阶段是BP算法的核心，由输出层到每个隐层，计算实际输出与期望输出之差，即误差，从而根据误差调整每个样本的权重值，以使其最终收敛结束。

### 1.1 算法的结构

神经网络模型由输入层、隐层和输出层组成，网络拓扑结构如图1所示。

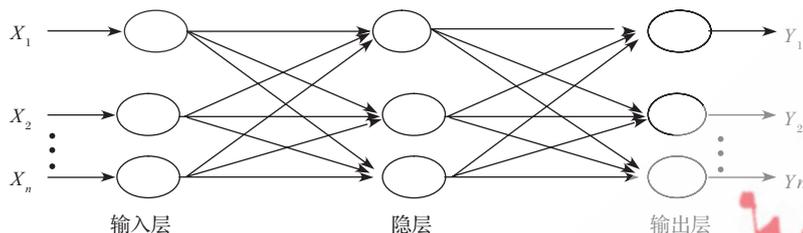


图1 BP神经网络拓扑结构

根据BP神经网络拓扑结构所示，BP网络有 \$n\$ 层，隐层用 \$L\_n\$ 表示，输入向量 \$\mathbf{X}=(X\_1, X\_2, \dots, X\_n)\$ 表示，期望输出用 \$\mathbf{Y}=(Y\_1, Y\_2, \dots, Y\_m)\$ 表示，而对应的实际输出 \$\mathbf{O}=(O\_1, O\_2, \dots, O\_m)\$。

BP网络参数结构可用以下参数描述：激活函数为 \$F\_n\$；网络输入样本集 \$\mathbf{S}=(\mathbf{X}, \mathbf{Y})\$；神经元的联接值 \$\mathbf{W}=(W\_1, W\_2, \dots, W\_n)\$；神经元网络输入函数 \$net = x\_1 w\_1 + x\_2 w\_2 + \dots + x\_n w\_n\$；BP神经元这里选用的S形激活函数 \$o=f(net)=\frac{1}{1+e^{-net}}\$；BP神经网络实际输出对输入求导，得到 \$f'(net)=o(1-o)\$。

BP神经网络在样本学习过程中，利用精度控制参数 \$\varepsilon\$，取误差测度 \$E = \sum E\_p < \varepsilon\$ 对权值 \$w\$ 的调整，若 \$E < \varepsilon\$，BP网络中的权重不会有显著的变化，误差也不再减小，网络将趋于稳定，即收敛了。

传统的BP神经网络输出层连接权值 \$w\_{ij}\$ 的调整<sup>[2]</sup>：

$$w_{ij} = w_{ij} + \Delta w_{ij} = w_{ij} + \alpha \delta_j O_i = w_{ij} + \alpha (y_j - O_j) (1 - O_j) O_j O_i \quad (1)$$

式中，\$\alpha\$ 为学习率；\$w\_{ij}\$ 为前层 \$AN\_i\$ 第 \$i\$ 个神经元到输出层 \$AN\_j\$ 的联接权值；\$O\_j\$ 为前层的实际输出；\$y\_j\$ 为输出层的理想(期望)输出；\$O\_i\$ 为输出层的实际输出。BP神经网络隐层 \$AN\_i\$ 的连接权值 \$v\_{ij}\$：

$$v_{ij} = v_{ij} + \Delta v_{ij} = v_{ij} + \alpha \sum_{k=1}^{H_h} (\delta_k \cdot v_{jk}) \cdot (1 - O_j) O_j \quad (2)$$

### 1.2 改进算法

在前面的数据挖掘研究中，对于神经网络的基本BP算法，前层和后层权值关系是：

$$w_{ij}(k+1) = w_{ij}(k) + \Delta w_{ij}(k) = w_{ij}(k) + \alpha \delta_j O_i \quad (3)$$

其中，\$w\_{ij}(k+1)\$ 为后层连接权值，而 \$w\_{ij}(k)\$、\$\Delta w\_{ij}(k)\$ 则是前层的连接权值和修改权值。在整个网络中，连接权值的修改是决定BP网络收敛速度和收敛精度的重要因素。由于BP网

络的收敛是基于无穷小的权修改量，也就意味着网络训练有可能陷入无穷的时间。所以，步长的选取是关键因素。步长取值过小，收敛速度很慢；步长取值太大，有可能跳过最优值，甚至，整个BP网络可能处于瘫痪和不稳定状态。

认真地研究神经网络学习算法存在的问题及对策，针对库存控制系统的BP算法，对BP算法的权修改量加以改进，在 \$\Delta w\_{ij}(k)\$ 前层的权修改量中，增加一个自适应因子 \$(1-\beta)\$，即：\$(1-\beta)\Delta w\_{ij}(k)\$。因此，后层的连接权值修改量 \$\Delta w\_{ij}(k+1)\$ 为：

$$\Delta w_{ij}(k+1) = (1-\beta)\Delta w_{ij}(k) + \alpha \delta_j O_i \quad (4)$$

式中，\$1-\beta\$ 为自适应因子，取值在0和1之间，\$\Delta w\_{ij}(k+1)\$ 为后层的权值修改量。因此，自适应因子 \$(1-\beta)\$ 与网络学习误差 \$\delta\$ 相关联，当 \$\delta\_j(k+1) < \delta\_j(k)\$ 时，说明网络学习误差减小，实际输出值与期望值很近，增加权值 \$(1-\beta)\Delta w\_{ij}(k)\$ 的修正量，即 \$\beta\$ 为冲量系数取较小值，从而自适应因子 \$(1-\beta)\$ 取较大值；反之，\$\delta\_j(k+1) > \delta\_j(k)\$ 时，则说明网络学习误差变大了，实际输出值正远离期望值，此时，需减小权值 \$(1-\beta)\Delta w\_{ij}(k)\$ 的修正量，即 \$\beta\$ 为冲量系数取较大值，从而自适应因子 \$(1-\beta)\$ 取较小值。根据Rumelhart对权值修改量中的冲量系数的研究，冲量系数为 \$[-0.9, +0.9]\$。现设 \$\beta\$ 为 \$0 \sim 0.9\$，因此，自适应因子 \$(1-\beta)\$ 的取值如下：

$$1-\beta = \begin{cases} 0.9 & \delta_j(k+1) < \delta_j(k) \quad (\beta = 0.1) \\ 0.1 & \delta_j(k+1) > \delta_j(k) \quad (\beta = 0.9) \end{cases} \quad (5)$$

总之，通过算法的研究，利用自适应因子 \$(1-\beta)\$，式(4)，对权修改量按需进行弹性的变化，实现了数据挖掘BP网络的学习收敛速度。

样本在训练过程中，依次对样本在网络中学习，前面学习的知识容易被后面的学习经验掩盖，从而利用部分样本的知识对全局网络的学习知识的概括，这将是严重的偏见。BP神经网络算法在样本的学习方式中也加以改进，以发现正确的知识。

改进算法对样本学习的设计，通过样本的“集中”式学习。将样本 \$\mathbf{S}(X\_p, Y\_p)\$ 一次性投入网络中进行整体学习，用它对所有权值 \$\Delta w\_{ij}\$ 的修改。即

$$\Delta w_{ij}^{(m)} = \sum \Delta_p w_{ij}^{(m)} \quad (6)$$

$$\Delta w_{ij}^{(m)} = (1-\beta)\Delta w_{ij}^{(m)} + \sum \Delta_p w_{ij}^{(m)}$$

$$\Delta v_{ij}^{(h)} = \sum \Delta_p v_{ij}^{(h)} \quad (7)$$

#### 1.2.1 算法的过程

根据自适应因子 \$(1-\beta)\$ 对权值修改量的调整和样本的“集中”式的学习，改进的BP算法过程如下：

For \$h=1\$ to \$m\$ do

初始化 \$W^{(h)}\$；

初始化精度控制参数 \$\varepsilon\$；

\$E = \varepsilon + 1\$；

While \$E > \varepsilon\$ do

$E=0$ ;

对所有的 $i, j, h$ :  $\Delta w_{ij}^{(h)}=0$ ;

对样本集 $s$ 中的每个样本:  $(X_p, Y_p)$

计算出 $X_p$ 对应的实际输出 $O_p$ ;

计算出误差测度 $E_s$ ;

$E_s=E_s+E_p$

对所有的 $i, j$ , 根据式(6), 计算 $\sum \Delta_p w_{ij}^{(m)}$ ;

对所有的 $i, j$ ,

$\Delta_p w_{ij}^{(m)}=(1-\beta)\Delta_p w_{ij}^{(m)}+\alpha\delta_j^{(m)}O_i^{(m)}$

$h=m-1$ ;

while  $h \neq 0$  do

对所有的 $i, j$ , 激活

对所有的 $i, j$ , 根据式(7)计算 $\sum \Delta_p v_{ij}^{(h)}$ ;

对所有的 $i, j$ :  $\Delta v_{ij}^{(h)}=(1-\beta)\Delta_p v_{ij}^{(h)}+\alpha\delta_j^{(h)}O_i^{(h)}$

$h=h-1$ ;

对所有的 $i, j, h$ :  $w_{ij}^{(h)}=w_{ij}^{(h)}+\Delta w_{ij}^{(h)}$

$E=E/2.0$

### 1.2.2 算法的实现

改进BP算法的实现:

用不同的小波随机数初始化 $w, v$ ;

初始化精度控制参数 $\varepsilon$ , 学习率 $\alpha$ ;

循环控制参数 $E=\varepsilon+1$ ; 循环最大次数为 $M$ ; 循环次数控

制参数 $N=0$ ;

while  $E > \varepsilon$  &  $N < M$  do

$N=N+1$ ;  $E=0$ ;

对所有的 $i, j, h$ :  $\Delta w_{ij}^{(h)}=0$ ;

对 $s$ 中的每个样本 $(X_p, Y_p)$ , 执行如下操作:

计算:  $o_1=F_1(X_p v)$ ;  $o_2=F_2(o_1 w)$ ;

计算输出误差: for  $i=1$  to  $m$

$E=E+(Y_p-O_{2i})^2$ ;

对所有的 $i, j$ , 计算输出层的权修改量: for  $i=1$  to  $m$  &  $j=1$  to  $n$

$\Delta w_{ij}=\sum \alpha(1-O_{1j})(O_{2j}-O_{1j})O_{1j}O_{2i}$ ;

对所有的 $i, j$ , 计算输出层的权矩阵修改量: for  $i=1$  to  $m$  &  $j=1$  to  $n$

$\Delta_p w_{ij}=(1-\beta)\Delta_p w_{ij}+\alpha\delta_j O_i=(1-\beta)\Delta_p w_{ij}+\Delta w_{ij}$

对所有的 $i, j$ , 计算隐层的权修改量: for  $i=1$  to  $H$

$Z=0$ ;

For  $j=1$  to  $m$ ;

$Z=Z+\sum w_{ij}\Delta o_j$ ;

$\Delta_i=Z$ ;

对所有的 $i, j$ , 计算隐层的权矩阵修改量: for  $i=1$  to  $H$  &  $j=1$  to  $m$

$\Delta_p w_{ij}=(1-\beta)\Delta_p w_{ij}+\alpha\delta_j O_i=(1-\beta)\Delta_p w_{ij}+\Delta w_{ij}$

修改输出层和隐层的权矩阵: for  $i=1$  to  $m$  &  $k=1$  to  $H$  &  $j=1$  to  $n$

$w_{ikj}=w_{ikj}\Delta w_{ikj}$

10 欢迎网上投稿 www.pcchina.com

## 2 基于神经网络的库存控制系统

典型神经网络的库存控制系统包含5个模块:

(1)神经网络的类型: 用于解决库存控制的预测问题。

例如选用多层感知器(MLP)与时间延迟神经网络(TDNN)相结合, 利用历史数据的时间顺序来预测库存控制量的控制水平。

(2)预测库存控制量: 用于获取未知的库存控制参数。

例如预测库存量、库存安全水平和季末最低库存量的参数。库存控制系统从学习样本中得到知识经验, 并从库存参数中提取转换信息。

(3)神经网络方法: 将通过历史数据训练神经网络, 提高网络的预测能力。例如传统的依次法、滚动法<sup>[3]</sup>和集中方法。用历史样本数据从不同角度进行网络训练, 提高训练质量。

(4)神经网络的记忆类型: 根据神经网络的单元层的节点储存知识。网络包括输入层、输出层以及隐层。节点决定了储存量的大小, 对于库存系统, 输入层的参数和隐层的节点数尤为重要, 从而决定了网络的建模。

(5)神经网络的评价: 用来评价神经网络库存系统的预测能力。通常的评价指标有皮尔森(P. Correlation)相关性系数、误差平方均值(NMSE)和绝对误差(AE)。

## 3 库存融合技术

### 3.1 ABC库存控制技术

ABC分析法基于“关键的少数, 次要的多数”的原则, 也就是把品种繁多的物资, 按其重要程度、消耗的数量、价值的大小、资金占用的多少等情况进行分类排队, 然后分别采用不同的管理方法, 做到抓住重点照顾一般的管理方法。其具体分类方法为: A类物资所占品种少, 占用资金大; B类物资占用品种比A类物资多一些, 占用的资金比A类物资少一点; C类物资所占品种最多, 占用的资金最少<sup>[4]</sup>。

表1 库存ABC分析法

分类	品牌数量占总品牌数量的比例/%	金额占总金额的比例/%
A类	5~15	60~80
B类	20~30	20~30
C类	60~80	5~15

如表1所示, 对于A类商品重点管理, 它库存资金占用大, 严格执行最佳库存原则, 盘活库存, 加快库存商品的周转率, 在满足客户服务水平的基础上, 寻求最佳安全库存量。而对于B类商品, 介于A类与B类商品之间, 处于库存商品的灰色管理地带, 根据B类品牌商品的销售金额, 如果销售额占B类商品的主要构成部分, 进行A类方法管理; 否则进行滞后商品管理, 周期性预测, 订货和盘存管理。C类商品, 由于占用资金不大, 根据商品的最低库存量和最大库存量, 采用批量订货原则, 寻求最大卖点和销售金额, 以适当控制库存。

《信息化纵横》2009年第8期

## 3.2 EOQ技术

在经典EOQ模型<sup>[5]</sup>中,一种典型决策参数有:

$$\text{经济订购批量: } EOQ = \sqrt{\frac{2C_3RP(C_1+C_2)}{C_1C_2(P-R)}}$$

$$\text{适当缺货量: } B_0 = \sqrt{\frac{2C_1C_2R}{C_3(C_1+C_3)}} \sqrt{\frac{P-R}{P}}$$

在经济订购批量(EOQ)经典模型中所用的符号定义如下:

$D$ 为全年需求量,  $R$ 为需求率(单位时间需求量),  $P$ 为生产速度,  $S$ 为最大存贮量,  $C_1$ 表示单位物品单位存储费用,  $C_2$ 表示每批订货成本或生产调整费用,  $Q$ 为阶段库存量,  $C_3$ 表示单位物品单位时间的缺货费用,  $EOQ$ 为经济订购批量,  $T$ 为经济订货(或生产)周期长度。

该模型的基本特征是:某种物品的全年需求量、每次订购费用成本、每件存货年保管费用或年度保管费用率都是已知常数;按一定批量供货;当存货库存量降低到零时,存货立即得到补充,即提前期为零;库存系统允许适当缺货。

## 3.3 季节库存控制技术

面向不确定需求的库存控制问题<sup>[6]</sup>研究了从市场预测出发,将预测得到的结果作为推算年需求量的参考依据并进行经济批量计算。同时,考虑到预测的误差可能导致计算出来的经济批量不经济,提出了循环预测、循环控制的方法,以使计算和操作结果向理想的状态逼近。

季节库存控制技术的实现过程:

(1)移动平均值  $M_i = (Q_i + Q_{i-1} + Q_{i-2} + Q_{i-3})/4$ ;

式中,期数  $i$  是指预测模型中的时间跨度;销售量  $Q_i$  是指预测模型中所对应的时间跨度的销售量;4个季度移动平均值  $M_i$  是指第  $i$  个、第  $i-1$  个、第  $i-2$  个和第  $i-3$  个季度销售量的平均值。

(2)中心化移动平均值(即相邻两个移动平均值的平均数);

(3)各季的季节指数;

(4)各季的季节指数平均值,并作调整;

(5)建立预测模型,计算预测值。

预测模型应为:

$$y_{i+T} = (a_i + b_i T) x^T$$

式中,  $a_i$  为某年最后一个中心化移动平均值;  $b_i$  为某年最后两个中心化移动平均值的趋势变化值;  $y_{i+T}$  表示所预测季度的预测值;  $T$  表示所预测季度与最后一个中心化移动平均值所对应季度之间的时间跨距;  $x^T$  表示所预测季度对应的调整后的季节指数。

## 3.4 库存融合控制技术

利用BP神经网络的算法工具在库存融合控制中进行实验,用来解决商品库存控制最优水平的确定问题。商品零售市场的产品销售和商品库存水平保持合理的均衡,才能

满足优质的顾客服务水平。仓库就储存待销售的商品及周边材料,这些库存商品也就占用大量资金。库存商品数量过少,顾客服务水平下降,顾客转向竞争对手,流失了顾客群,损失增加利润机会。库存商品数量过多,顾客服务水平提高,但库存资金挤压,企业资金周转缓慢。库存控制水平的数据挖掘仓库管理系统需要考虑的因素有:商品销售量和金额、商品库存量和金额、商品周转率、商品动销率、商品订货周期、商品补货量和金额,以及商品库存保本期。研究库存融合控制技术,用最优的订货量和最优的订货周期,实现最优的客服水平和最优的库存。即“四优”原则。

库存控制融合技术的实现过程如图2所示。

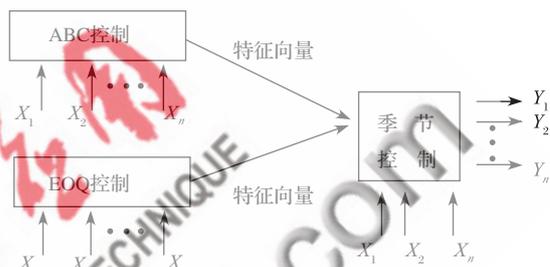


图2 多库存控制融合过程

## 3.4.1 基于BP算法库存融合控制参数

由于影响库存融合控制的参数有很多因素,在研究中全面的考虑各参数的影响,建立的库存控制模型才能是最优的。影响库存控制的参数有到货时间、供货周期、年需求量、期初库存量、阶段批量订购、搬运装卸成本、补货和需求周期、运输成本、订货费用、储存费用、缺货损失、商品调换成本、商品动销率、商品库存周转率、商品库存保本期以及影响顾客需求量的各种自然、社会参数。然而做为品牌库存融合控制的顾客需求量为随机数,订货量与价格有关,并且可以适当缺货。因此品牌库存融合控制的BP网络设置如下。

网络输入:

(1)商场

$T(n)$ 为销售周期(季);  $S(n)$ 为期初库存量(件);  $Q(n)$ 为阶段批量订货(件);  $SC(n)$ 为单位存货年储存费用(元/件年)。

(2)消费能力-价格带

$P_1(n)$ 为消费高档服装件数(件);  $P_2(n)$ 为消费中档服装件数(件);  $P_3(n)$ 为消费低档服装件数(件)。

网络输出为:  $U_2(n)$ 为阶段库存控制量(件)。

## 3.4.2 库存控制神经网络系统结构

库存控制神经网络系统采用多层感知器(MLP),多层感知机可以表示为嵌套式logsig函数,一个输出神经元可用以下公式表示:

$$F(x, w) = f\left(\sum_j w_{oj} f\left(\sum_k w_{jk} f\left(\dots f\left(\sum_i w_{ki} x_i\right)\right)\right)\right)$$

其中,  $\varphi(\cdot)$ 是sigmoid传递函数,  $w_{oj}$ 表示隐藏层神经元 $j$ 与输出神经元 $o$ 的连接权重, 其他类推。  $x_i$ 表示输入向量的第 $i$ 个分量。  $w$ 是权重向量, 其中的分量按照层号, 层中神经元的个数及神经元序号顺序排列。系统多层感知器(MLP)结构如图3所示。

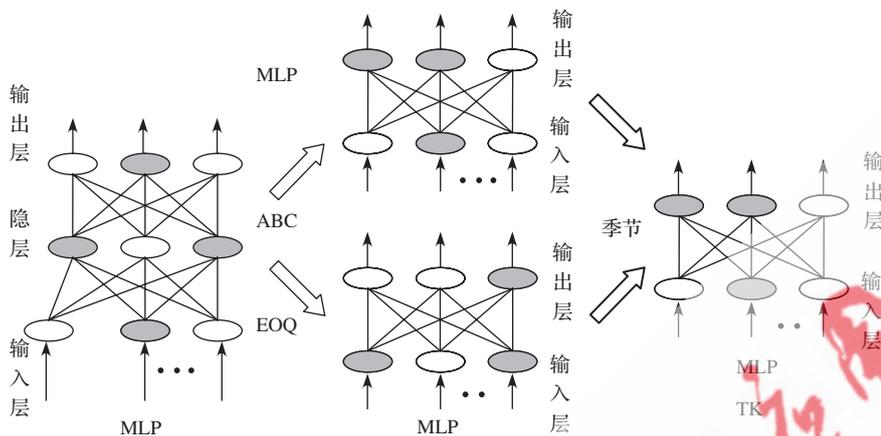


图3 库存多层感知器(MLP)

本文分别将ABC、EOQ和季节库存输入参数直接输入感知器, 感知器输入层的神经元个数对应库存参数的个数。然后, 利用S传递函数提取ABC库存参数, EOQ库存参数和季节库存参数。再将提取到的3种库存参数值合并为一个特征向量, 输入感知器的下一层进行学习, 压缩合并后的向量送入感知器。同时以数据库中保存的ABC-EOQ-季节模板为学习目标, 试图预测出该库存的库存控制量。如果预测操作失败, 回溯到特征合并前一步, 分别将ABC库存控制参数向量和EOQ库存参数向量输入到ABC库存预测感知器和EOQ库存预测感知器, 利用数据库中保存的ABC库存控制模板和EOQ库存模板进行预测, 预测的结果再次与季节库存参数送入季节库存预测感知器, 从而获得库存

控制量的预测结果。

利用BP神经网络对库存进行库存控制量预测, 可以提高系统性能。本文描述了BP神经网络算法, 并提出用集中样本训练的方法和增加自适应因子改进BP算法。神经网络在某种程度上模拟了生物的感知特性, 它是一种分布式并行处理结构的网络模型, 具有自组织和自学习能力、很强的预测能力以及对不完全信息的鲁棒性。由于对库存控制量的综合预测有许多未知条件, 神经网络方法可以通过学习获得对这些条件的隐性表达, 使它的适应性更强, 也易于实现。

下一步工作将对本文中提出的方法进行实验验证。同时, 还将研究如何利用神经网络对EOQ、ABC管理以及季节控制库存预测及其相应的算法。

## 参考文献

- [1] RUMELDE, HINTONGE, WILLIAMSR. J. Learning representations by back-propagating errors[J]. Nature, 1986, 323: 533-536.
- [2] 蒋宗礼. 人工神经网络导论[M].北京:高等教育出版社, 2001.
- [3] 何炎祥. 神经网络技术在库存管理中的应用[J]. 计算机工程与应用, 2002(15): 182-183.
- [4] 谭坚坚. ABC分析法在库存管理中的应用研究[J]. 科教文汇, 2006(4): 75-76.
- [5] 杨帅. 几类库存控制模型及其应用[D]. 重庆大学硕士学位论文, 2005(6): 7-9.
- [6] 刘振超, 黄中鼎. 面向不确定需求的库存控制问题[J]. 上海第二工业大学学报, 2005, 22(2): 32-33.

(收稿日期: 2008-12-25)

上接第7页

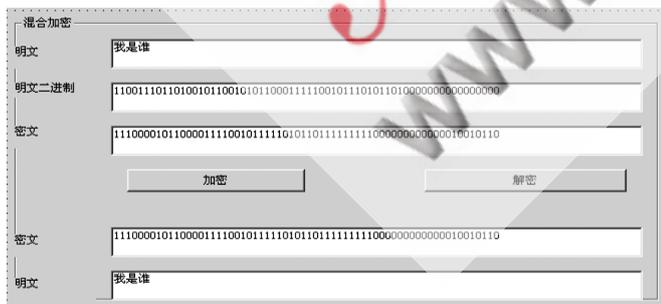


图9 加解密过程

本文详细介绍了混合加密算法各部分设计流程, 并对混合后加密算法的安全性进行了分析, 对于DES算法的密钥容易破解以及无法确定消息来源身份的缺点, 混合加密算法在其运算过程中加入了KEELOQ算法, 使DES的密钥破解的可能性大大降低, 并且通过IC卡工作之前的特定

学习步骤, 可以确定消息来源的身份, 解决了DES加密算法无法处理的问题。对于KEELOQ加密算法传输效率低以及无法用于数据加密的问题, 混合加密算法采取了不用其加密数据, 只是对加密密钥进行加密的办法, 避开了KEELOQ无法解决的问题, 很好地实现了IC卡既安全, 加密速度又快的要求。

## 参考文献

- [1] 陈鲁生, 沈世镒. 现代密码学[M]. 北京: 科学出版社, 2002.
- [2] 杨义先, 钮心忻. 应用密码学[M]. 北京: 邮电大学出版社, 2005.
- [3] 李福平, 金伟正, 邓德祥. KEELOQ技术的软件实现[J]. 电子技术应用, 2002, 28(6): 35-38.
- [4] 章照止. 现代密码学基础[M]. 北京: 邮电大学出版社, 2004.
- [5] 求是科技. 单片机通信技术与工程实践[M]. 北京: 人民邮电出版社, 2005.

(收稿日期: 2008-12-27)