基于深度极限学习机的危险源识别算法 HIELM

李诗瑶 周 良 刘 虎
(南京航空航天大学计算机科学与技术学院 南京 210016)

摘 要 危险源识别是民用航空管理的重要环节之一,危险源识别结果必须高度准确才能确保飞行的安全。为此,提出了一种基于深度极限学习机的危险源识别算法 HIELM(Hazard Identification Algorithm Based on Extreme Learning Machine),设计了一种由多个深层栈式极限学习机(S-ELM)和一个单隐藏层极限学习机(ELM)构成的深层网络结构。算法中,多个深层 S-ELM 使用平行结构,各自可以拥有不同的隐藏结点个数,按照危险源领域分类接受危险源状态信息完成预学习,并结合识别特征改进网络输入权重的产生方式。在单隐藏层 ELM 中,深层 ELM 的预学习结果作为其输入,改进了反向传播算法,提高了网络识别的精确度。同时,分别训练各深层 S-ELM,缓解了高维数据训练的内存压力和节点过多产生的过拟合现象。

关键词 危险源识别,深度学习,极限学习机(ELM),分类
中图法分类号 TP183 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.05.016

Hazard Identification Algorithm Based on Deep Extreme Learning Machine

LI Shi-yao ZHOU Liang LIU Hu
(College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

Abstract Hazard identification plays an important role in aviation safety management. The results of hazard identification must be highly accurate to ensure the safety of the flight. To this end, a hazard identification algorithm based on deep extreme learning machine (HIELM) was proposed, which consists of multiple deep stacked ELMs and a single ELM. There are a parallel structure and different number of hidden nodes among these deep ELMs, and the hazard information is gotten to produce deep features according to the hazard area. In addition, the way of generating input weights has been enhanced with recognition features. The single ELM receives the results as its input. With the help of the improved back propagation algorithm, the network can achieve much better accuracy. The thought that deep ELMs are trained respectively alleviates the memory pressure and the over fitting phenomenon when facing the high-dimensional datasets.

Keywords Hazards identification, Deep learning, Extreme learning machine (ELM), Classification

1 引言

在民用航空管理体系中,安全是一个亘古不变的主题,风险管理是航空管理的重要组成部分。风险管理分为3个重要组成部分:危险源识别、风险评估和风险控制。危险源识别是风险管理中最基础和重要的环节,通过正确地识别危险源,能够准确对危险源进行控制,保证飞行过程的安全性和可靠性。在民航系统中,危险源被定义为可能导致人员伤害或财物损失事故的、潜在的不安全因素;危险源识别(辨别)就是识别危险源存在并确定其特性的过程。

随着科学技术的发展,危险源识别技术大体分为3种类型。1)经验法,即人工分析法,将领域相关标准和专家经验相结合,通过标准的评价过程来对危险源进行分析。Smith B E[2]以结构化的头脑分析为基础,提出了一种综合性方法,对航空运输中潜在的危险源进行识别,但该方法需要消耗大量的人力、物力资源,并且不能充分地利用人的领域知识和经验。2)计算机辅助的方法,该方法通过计算机辅助的方式建立系统的模型或完成人的分析过程,然后通过模型分析对危险源进行识别。Katrina Groth 等人[3]提出了一个集成的架构和软件平台,该平台通过三层混合模型,即事件树、故障树和事件序列图,结合建模的方法和算法实现了对概率风险的评估,并利用贝叶斯网络实现了非决定性各元素之间的依赖关系;Cui 等人[4]建立了结合 HAZOP 分析法、保护层分析法和安全完整性水平的验证等方法的平台,利用编程语言实现了以上方法并使不同方法间的数据实现共享。该方法虽然部分解放了人力,但是仍然不能充分利用现有的经验知识。3)以专家系统为代表的智能化危险源识别,这类方法在分析的过程中运用机器学习方法解放了人力,基本不需要人类的

到稿日期:2016-04-15 返修日期:2016-08-19 本文受江苏省产学研联合创新资金项目(SBY201320423)资助。
李诗瑶(1991—),女,硕士生,主要研究方向为信息系统及集成、机器学习等;周 良(1966—),男,博士,副教授,硕士生导师,主要研究方向为信息系统、知识工程;刘 虎(1974—),男,博士,高级工程师,硕士生导师,主要研究方向为物联网和云计算。

参与。Olawande D 等人[6]针对安全性分析提出了一个概念性的框架，在危险源识别的过程中运用基于案例推理的方法进行分析，复用了已有的知识，在该框架中还包括自然语言处理技术，使得专家知识能够通过机器直接处理与获得。该方法虽然利用了已有的经验知识，但是随着系统的发展，其暴露出经验数据库膨胀和适应能力差的问题；算法由于采用最邻近方法来求解最邻近问题，在数据和维度较少时表现出较优越的性能，但数据量增多时，就降低了效率与准确率。

针对危险源识别算法中存在的自适应能力差等问题，本文提出了一种基于深度学习的危险源识别算法 HIELM，该算法用深层极限学习机学习危险源数据的深层特征，用训练网络记忆危险源的潜在特征，并结合标准化方法和深层极限学习机算法，提高了网络的鲁棒性和识别的准确性，同时结合分类处理方法，改善了网络训练时内存受限导致的不能获得最优网络结构的问题。

2 HIELM 算法的总体思路

从民航管理中危险源识别的定义和方法上可以看出，对危险源的识别就是根据危险源的评估标准，利用一定的技术手段和标准化过程对危险源进行分析。在危险源分析中，国际民航组织安全管理手册针对危险源提出 SHEL 模型，将危险源信息分为人件、软件、硬件和环境，国内依据民航空中交通管理安全管理体系(SMS)建设指导手册从人员、设备、环境和管理 4 个方面对危险源进行分析，并遵循国际民航组织提供的 3 个步骤：1)识别一般危险源；2)将一般危险源分解成一组特定危险源或一般危险源的构成要素，每个特定危险源可能具有一组不同或独特的诱发因素，从而使得每个特定危险源在本质上各不相同，而且独特；3)将特定的危险与潜在的特定后果联系起来。

综上所述，危险源识别的过程可看作一个危险源分类的过程。由于危险源识别过程处理的数据量较大，危险源深层特征较多及特征关联性较强，并且识别处理要求在具有较高准确率的基础上进行，识别处理速度能够满足在线实时处理要求，而深层极限学习机只需要设置网络的隐层节点个数，在算法执行过程中不需要调整网络的输入权值以及隐元的偏置，并且产生唯一的最优解，具有训练错误率低、处理速度快和内存要求低的特征，因此本文利用深层极限学习机实现危险源深层特征提取。为了使网络模型能够达到结构最优，算法首先利用领域知识将危险源状态信息进行类别划分，针对每一个类别构建一个深层 ELM 网络，然后将各个子 ELM 网络的识别结果输入一个单隐藏层极限学习机进行再学习，得到最终的识别结果。这样减轻了网络训练时的内存压力，同时也符合人类大脑分区域处理信息的要求，使网络获得更优的识别效果。

HIELM 算法流程图如图 1 所示，算法分为两个阶段：预学习阶段和再学习阶段。在预学习阶段利用深层 ELM 对危险源特征进行学习，得到各领域的危险源识别结果；在再学习阶段，利用单隐藏层极限学习机对预学习结果进行再学习，得到最终危险源的识别结果。

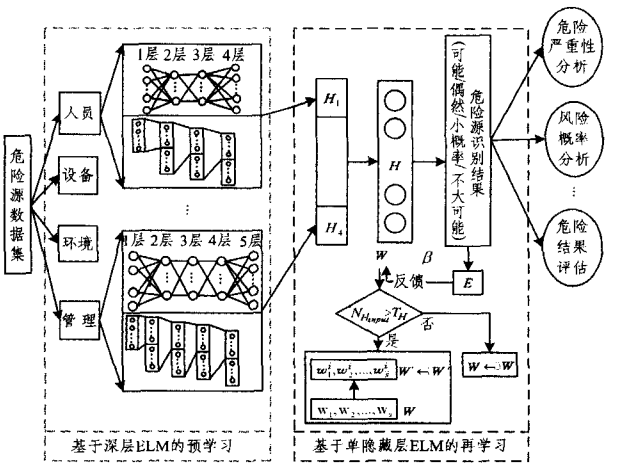

图 1 HIELM 算法流程

2.1 基于深层 ELM 的预学习

随着机器学习的发展，利用深层神经网络不断学习事物深层特征能够提高网络的准确率，这对于民航危险源识别非常重要。在深层学习阶段，引入深层神经网络机制，不断学习危险源状态的深层特征，获得有较高准确率的识别结果；同时，为了达到网络的最优结构，提出按照人员、设备、环境及管理 4 个领域分模块地对危险源状态信息进行学习，在实际应用中，如果各领域状态信息过多则可以继续细分。

为了提高各模块中深层网络的学习效率，引入栈式极限学习机(Stacked Extreme Learning Machine，S-ELM)作为网络的训练方法，其流程如图 2 所示。

S-ELM 算法的主要思想是前一层节点能够有选择地传递其中的重要节点给上一层，然后上层节点利用接收的节点与随机产生的节点构成自己的隐层输出。算法本质就是网络的第 $L-1$ 层中的 N 维隐层特征空间通过维度约减产生最重要的 N' 维隐层特征空间，并将这 N' 维隐层特征空间传递给上一层，上一层只需要产生 $N-N'$ 个随机节点，这 $N-N'$ 个节点产生的隐层输出与接收到的 N' 个节点作为第 L 层的隐层特征空间。考虑到一般危险源的构成要素对于危险源的识别具有一定的指导作用，本文对 S-ELM 算法进行了改进。在算法中，构建一张存放一般危险源构成要素的表 T，在初始化权重时，查找表 T，如果状态信息在 T 中，从一个较大的数域中随机产生相应的权重值；否则，从较小的数域中产生权重。

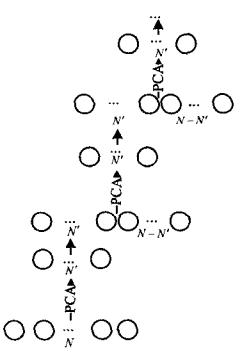

图 2 S-ELM 算法流程

在 S-ELM 中，重要节点通常通过主成分分析算法(Principal Components Algorithm，PCA)来产生。它的主要思想是

利用数据集协方差矩阵的特征值分解或数据集矩阵的奇异值分解将数据集中相关的变量转换为非线性相关的变量。具体方法是将相关数据标准化，求出标准化后矩阵 B 的协方差矩阵 C，利用特征值分解求出 C 的特征向量 D 和特征值 V，将特征值和相应的特征向量按特征值递减排列得到排序后特征向量 D'，将矩阵 B 与 D' 的前 m 行相乘，得到非线性相关的变量 $Y=BD'$。

在深层学习阶段，假设一组危险源状态信息集为 $R=\{R_1,R_2,\cdots,R_n\}$，其中，一个危险源的状态信息为 $R_k=\{r_{k1},r_{k2},\cdots,r_{kM_k}\}^T$，$k=1,\cdots,n$，对应的识别结果为 $O=\{O_1,\cdots,O_n\}$，按照领域分类将深层网络划分为 4 个模块。为了确定状态信息 r_{kj} $(k=1,\cdots,n,j=1,\cdots,M_k)$ 所属的领域分类即网络的模块，利用处理非线性数据具有优越性的支持向量机(Support Vector Machine，SVM)对状态信息进行分类。设分类后的结果为 $R_k=\{C_1,C_2,C_3,C_4\}^T$，其中，$C_i=\{c_{i1},c_{i2},\cdots,c_{im_i}\}^T$ $(i=1,\cdots,4)$，将分类后的结果输入相应模块中。接着对各子网络使用 S-ELM 算法，在使用 S-ELM 算法之前，设各模块隐藏节点的个数为 H_i，深层网络的层数为 L_i。根据危险源构成要素表 T，从不同数域随机产生各模块的权重 $W_i=\{W_{i1},\cdots,W_{im_i}\}$ 和隐藏节点偏移量 $b_i=\{b_{i1},\cdots,b_{im_1}\}$，并选择 S 型函数：

$$g(x)=\frac{1}{1-\exp^{(-x)}} \tag{1}$$

作为激励函数，计算各模块首层的隐层特征空间 H_{i1}：

$$H_{i1}=\frac{1}{1-\exp^{(-C_iW_i+b_i)}}=\begin{pmatrix} h_{11} & \cdots & h_{1H_{i1}} \\ \vdots & \ddots & \vdots \\ h_{m_i1} & \cdots & h_{m_iH_{i1}} \end{pmatrix} \tag{2}$$

使用维度约减算法 PCA 对各模块首层产生的隐层特征空间进行约减得到 H'_{i1}，并把 H'_{i1} 传递给第二层。在第二层，随机产生 $H-H'_{i1}$ 个隐层节点，它们的输出与 H'_{i1} 相结合构成第二层隐层特征空间 H_{i2}，重复上述步骤，直到产生第 L 层的隐层特征空间 H_{iL_i}，网络的隐层特征空间 $H_i=H_{iL_i}$。

以上就完成了一个模块的深层学习过程，具体步骤如算法 1 所示，该过程需要记录各模块的预识别结果 H_i。

算法 1　基于深层 ELM 的预学习

输入：危险源的状态信息集 $R=\{R_k\mid k=1,\cdots,n\}$，其中，$R_k=\{r_{k1},r_{k2},\cdots,r_{kM_k}\}^T$；危险源构成要素表 T 和激励函数 g(x)

输出：各模块预识别结果 H_i，即各模块的最后一个隐藏层的隐层特征空间

步骤 1　利用 SVM 将危险源状态信息 R_k 按照人员、设备、环境和管理进行分类得 $R_k=\{C_1,C_2,C_3,C_4\}^T$，并将 C_i 作为对应深层模块的输入；

步骤 2　根据危险源要素表 T 产生各模块权重，并计算各模块隐层特征空间 H_i：

For i=1 to 4

(1)判断状态信息是否符合危险源要素表 T 中的数据，若符合，则从较大的数域[0.5,1]随机产生输入层权重 W_i；否则，从较小的数域[0,0.5]随机产生输入权重 W_i；

(2)随机产生隐藏节点偏移量 b_i；

(3)根据式(2)，计算模块 i 的首层隐层特征空间 H_{i1}；

(4)根据 S-ELM 算法，计算各模块的最后一层隐层特征空间 H_{iL_i}：

For k=2 to L_i

1)依照 S-ELM 得到第 k 层的隐层特征空间 H_{ik}；

2)IF k=L_i

记录第 i 个模块的隐层特征空间

H_i 即 H_{iL_i}；

End IF

End For

End for

输出：各模块的隐层特征空间 H_i

2.2　基于单隐藏层 ELM 的再学习

在预学习阶段，仅仅完成了在各领域中的危险源状态识别过程。在这一阶段，算法使用一个单隐藏层极限学习机网络学习各模块的识别结果，并得出危险源最终的识别结果。

假设第 i 个模块的识别结果为 H_i，将 4 个模块的识别结果连接，形成再学习阶段的输入向量 $H_{input}=\{H_1,\cdots,H_4\}$，将向量 H_{input} 输入单隐藏层神经网络来计算网络的隐藏层特征空间 H。在单隐藏层 ELM 中网络的输出权重 $\beta=H^TO$。为了提高网络的鲁棒性，本文使用标准化的 ELM，引入对实验危险性和结构危险性的平衡参数 C，由于训练样本的数量常常小于隐藏层节点的数量，RELM 的输出权重 β 为：

$$\beta=H^T\left(\frac{1}{C}+HH^T\right)^{-1}O \tag{3}$$

网络的输出为：

$$\Gamma_o=H\beta \tag{4}$$

为了提高网络的准确性，引入反向传播算法对网络的权重进行微调。设训练过程中的输入为 X_{train}，输出结果为 Y_{label}，激励函数为 $g(x)$。在单隐藏层极限学习机中，反向传播算法的基本思路是向输入权重传递网络误差，不断更新权重，使网络达到较优的结构。为了提高网络的收敛效率，算法选择性地更新网络权重，具体步骤如下。

(1)根据基本 ELM 算法随机产生 ELM 的输入权重 W，根据式(3)计算网络的输出权重 β；

(2)根据实际输出结果 Γ_o 与训练集结果 Y_{label}，计算网络误差 E：

$$E=Y_{label}-\Gamma_o \tag{5}$$

(3)根据网络误差 E，计算网络的权重更新 ΔW：

$$\Delta W=\zeta\beta^TE\Gamma_o(1-\Gamma_o)X_{train}^T \tag{6}$$

(4)更新网络权重：如果网络中输入数据量大于一个阈值 T_H，利用 PCA，求出选择权重 W' 和特征向量 D'，网络权重为 $W'=W'-\Delta WD'$；如果网络中输入数据量小于一个阈值 T_H，网络权重为 $W=W-\Delta W$；

(5)利用新的输入权重重新计算新的输出权重 β 和 Γ_o；

(6)如果 $Y_{label}=\Gamma_o$，则算法停止；否则，返回步骤(2)继续进行计算，直到达到一个足够大的迭代次数或算法收敛。

在危险源识别过程中，只需要利用 SVM 算法将危险源状态信息进行分类，将状态信息按照类别输入相应模型，经过预学习阶段和再学习阶段，得到输出结果，即完成了一次危险源识别。算法具体步骤如算法 2 所示。

在算法 2 中，步骤 1 和步骤 2 实现了预学习阶段。在步骤 2 中，各领域识别可以并行进行也可以按顺序依次进行。步骤 4 和步骤 5 完成了算法的再学习阶段，该阶段的输出结果就是算法最终的危险源识别结果。

算法 2 HIELM

输入：危险源状态信息集 $R=\{(R_k,O_k)|k=1,2,\cdots,n\}$，其中，$R_k=\{r_{k1},r_{k2},\cdots,r_{kM_k}\}^T$；危险源激励函数 $g(x)$，标准化参数 C 和危险源构成要素表 T

输出：危险源识别结果

步骤 1 利用 SVM 将危险源信息 R_k 划分到人员、设备、环境、管理 4 个不同的领域中得到 $R_k=\{C_1,C_2,C_3,C_4\}^T$，并将不同的领域分类集输入到相应的模块中；

步骤 2 对每个子网络使用 S-ELM 算法：

For i=1 to 4

使用 S-ELM 算法得到各深层网络的预识别结果 H_i；

End For

步骤 3 将深层网络预识别结果组合作为顶层神经网络的输入 $H_{input}=\{H_1,\cdots,H_4\}$；

步骤 4 根据 ELM 算法和激励函数 $g(x)$，计算单隐藏层 ELM 的初始输入权重 W_t、隐层输出 H_t 和输出权重 β_t；

步骤 5 通过反向传播算法，确定网络的最终输入权重 W、隐层输出 H 和输出权重 β；

步骤 6 危险源识别结果：

$\Gamma_o=H\beta$

与 S-ELM 算法相比，HIELM 算法将一个多隐藏节点多维度的 S-ELM 网络划分为多个具有较少隐藏节点、层数的网络和一个单隐藏神经网络。已知在文中 HIELM 算法共有 4 个模块，假设每个模块有 L_i 层，每一层有 H_i 个隐藏节点，其中 $i=\{1,\cdots,4\}$，那么网络的单隐藏层具有 $\sum_{i=1}^{4}H_i$ 个隐藏节点。一个 HIELM 网络可以模拟一个具有 $(\sum_{i=1}^{4}L_i+1)$ 个隐藏层、每层有 $\sum_{i=1}^{4}H_i$ 个隐藏节点的 S-ELM 网络。由文献[8]可知，对于一个含有 H 个隐藏节点的神经网络来说，其涉及 2 个 $H\times H$ 的矩阵运算，分别是 H^TH 和 $(H^TH)^{-1}$ 或 $(\frac{1}{C}+H^TH)^{-1}$。所以，S-ELM 算法的复杂度如下：

$$comp(S\text{-}ELM)=(\sum_{i=1}^{4}L_i+1)(\sum_{i=1}^{4}H_i)^2 \tag{7}$$

而在 HIELM 算法中，算法的复杂度为：

$$comp(HIELM)=\sum_{i=1}^{4}L_iH_i^2+(\sum_{i=1}^{4}H_i)^2<(\sum_{i=1}^{4}L_i)(\sum_{i=1}^{4}H_i)^2+(\sum_{i=1}^{4}H_i)^2=comp(S\text{-}ELM) \tag{8}$$

显然，HIELM 算法具有较低的算法复杂度。

3 实验结果和分析

本文从准确性和训练时间两个方面对算法进行评估，并将该算法与传统的 ELM 算法、S-ELM 算法、支持向量机(SVM)、深信度网络(DBN)以及基于案例推理的算法进行比较，说明了本算法的泛化特性和可行性。

由于目前没有公开的危险源数据库，本实验将某民航行政管理系统的数据库作为实验数据库。通过对上述数据库中的危险源状态进行分析，获得危险源的风险概率类别。在民航领域中，风险概率类别大概可以分为 4 种：很可能、偶然、小概率和不大可能。

实验在 Intel core i7 2.6GHz Window7 的环境下使用 Matlab 2014Ra 进行。在实验中，标准化系数 C 依据文献[20]从 $\{2^{-24},\cdots,2^{24},2^{25}\}$ 中选取，通过实验的方法选择使得算法结果最优的值作为参数 C 的值。图 3 为算法精确度与 C 的关系，选取曲线由上升趋势变平缓的拐点作为参数 C 的取值，由此得到 $C=2^{-2}$。实验按领域将危险源状态信息分为 4 类：人员、设备、环境、管理，如表 1 所列，用到的一般危险源构成要素如表 2 所列。

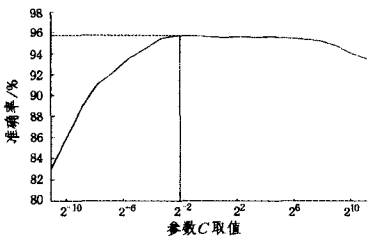

图 3 算法精确度与参数 C 的关系

表 1 危险源信息示例

领域	子领域	状态类别
人员	知识水平	理论知识
		专业操作技能
		工作经验和技术
	生理和心理因素	抗压能力
		身体健康水平
		心理健康水平
		飞行时限
		工作强度等
	意识和态度	风险感知能力
		安全意识和态度
		安全目标认知
	操作	非法操作
		飞行指令准确性
		移交问题
		突发问题处理能力
	机组资源	机组搭配
设备	机场设施	设备故障率
		设备维护错误
		设备软件工作不正常
		网络安全
	飞机	飞机维护错误
		飞机日常使用
		飞机系统安全性
		警告系统安全性
环境	自然环境	天气因素(温度/湿度/风力)
		天气预报有效性
		鸟击意外
		非法干扰
		升空物体
		特殊地理环境
		电磁干扰
	工作环境	工作环境满意度
管理	规章	制度不适用
		空域划设不合理
		运维管理有效性
	机构	交流信息真实度
		资源配置

表 2 危险源要素列表

序号	危险源要素
1	小于最小飞行间隔
2	低于最低安全高度
3	空管雷达出现低高度告警或飞行冲突告警
4	非法入侵跑道
5	陆空通信失效
6	无线电干扰
7	影响空管运行安全的设备故障

在实验 1 中，比较基本 ELM 算法、S-ELM 算法和 RHELM 算法的准确度，设置 S-ELM 和 RHELM 的层数都为 5($S=5$)；在实验 2 中，比较 S-ELM 算法和 RHELM 算法的准确度随网络层数的变化，设置网络隐藏层有 500 个节点($N=500$)；实验 3 中，比较了 5 种算法的训练时间，设置 ELM 算法中隐藏层节点为 12000 个，S-ELM 的隐藏层节点为 1000 个($N=1000$)，共 100 层($S=100$)，RHELM 隐藏层节点为 500 个($N=500$)，共 50 层($S=50$)，SVM 的参数 C 和 γ 通过排列组合的方式分别从$\{10^{-3},\cdots,10^{6}\}$和$\{10^{-5},\cdots,10^{4}\}$中确定，DBN 的网络结构为 956-1000-1500-500。

通过实验可以得出如下结论：如图 4 所示，RHELM 算法要优于其他两种算法，并且随着隐藏节点数的增加，准确率具有显著的提高，算法隐藏层节点达到 800 个后增加少量节点对于精度的提高不明显，需要大幅度提高隐藏节点的数据或增加隐藏层数量；由图 5 可以看出，相对于 S-ELM 而言，在隐藏层节点个数一定时，RHELM 具有较高的识别精度，从图像的趋势可以看到，增加隐藏层数量对于 HIELM 的识别精确度有一定帮助；通过实验 3 可以看出(见表 3)，HIELM 算法的训练时间仅仅优于 DBN 网络。虽然 HIELM 具有较高的精确度，并且只需较少的隐藏节点个数，但是由于 RHELM 算法需要分别对各领域建立深层模型并对各网络进行训练，往往具有较长的训练时间，因此 HIELM 只适用于精度要求较高、但对训练速度要求不高的识别工作。

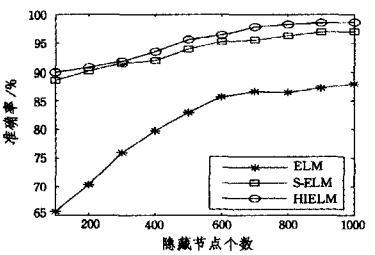

图 4　隐藏节点个数与准确率的关系图

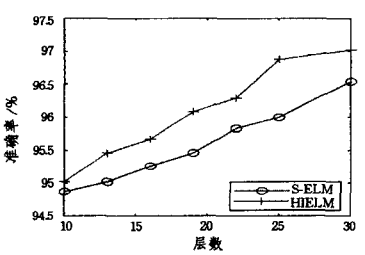

图 5　网络层数与准确率的关系图

最后，将 HIELM 算法与基于案例推理的算法进行比较，由图 6 可知，HIELM 具有较高的识别精度，随着引入数据量的增加，文中提到的算法仍然具有较高的识别准确率。

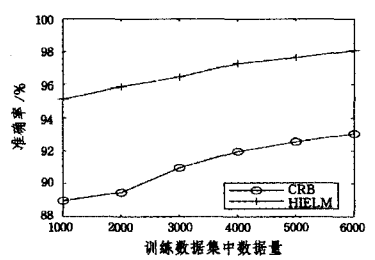

图 6　数据量与准确率的关系图

表 3　不同算法的训练时间与准确度比较

算法	训练时间/s	准确度/%	隐藏节点个数
ELM	203.04	96.95	12000
S-ELM	770	98.20	1000
SVM	723.05	98.23	5000
DBN	2856.03	97.98	1500
HIELM	1015	98.64	500

同时，为了验证算法具有良好的可行性，分别从数据库中抽取 25 条人员信息、20 条设备状态信息、10 条环境信息和 2 条管理信息，通过排列组合的方式形成 10000 条危险源状态信息来对算法进行验证，其中，很可能发生的危险源有 5321 个，偶然发生的危险源有 2604 个，很少发生的危险源有 1260 个，不大可能发生的危险源有 815 个，通过计算识别的准确率为 98.32%，从表 4 可以看出算法能够对危险源进行识别，并且具有较高的识别查准率。

表 4　算法识别结果与查准率

状态	测试数据	算法识别结果	查准率/%
很可能	5321	5399	98.33
偶然	2604	2524	98.45
很少	1260	1265	98.18
不大可能	815	812	98.28

结束语　本文针对危险源识别算法中存在的适应性差和学习高维度数据时 ELM 网络训练内存受限的问题，提出了一个基于深层 ELM 算法的危险源识别算法 HIELM。通过建立深层神经网络对不同状态信息进行识别时，为了提高深层 ELM 网络的训练效率，本文引入 S-ELM 训练方法，有选择地传递网络的隐层特征空间，减少了各层的权重数量，并对 S-ELM 算法进行了改进，引入一般危险源列表对输入权重的产生进行指导。为了得到系统危险源的识别结果，将各领域危险源识别结果作为一个单隐藏层 ELM 网络的输入。算法中引入反向传播算法作为单隐藏层 ELM 网络的训练方法，通过传播网络的输出误差不断调整输入权重，直到网络到达收敛状态。仿真实验表明本文算法对危险源具有很高的识别准确率，并且采用按领域分类分模块识别的方法解决了网络在训练时内存受限以及识别过程受到数据库样本限制的问题。

然而，在各领域模块中对深层 ELM 的训练降低了算法的速度，并且算法对噪音较敏感。在未来，为了增加 HIELM 的鲁棒性，将会把降噪的自动卷积网络应用于 HIELM 中，并研究深层降噪自动卷积网络。同时，将继续研究深层 ELM 的理论，以加快深层 ELM 和 HIELM 的训练速度，争取使 HIELM 实现联机处理。

参 考 文 献

[1] HUANG G B, WANG D H, LAN Y. Extreme Learning Machines: a Survey[J]. International Journal of Machine Learning and Cybernetics, 2011, 2(2): 107-122.

[2] SMITH B E, DE-JONG H H, EVERDIJ M H C. A Prognostic Method to Identify Hazards for Future Aviation Concepts[C]// ICAS Secretariat-26th Congress of International Council of the Aeronautical Sciences. ICAS Secretariat, 2008: 3950-3965.

[3] GROTH K, WANG C D, MOOSLEH A. Hybrid Causal Metho-

dology And Software Platform For Probabilistic Risk Assessment And Safety Monitoring Of Socio-Technical Systems[J]. Reliability Engineering & System Safety, 2010, 95(12): 1276-1285.

[4] CUI L, SHU Y D, WANG Z H, et al. HASILT: An Intelligent Software Platform for HAZOP, LOPA, SRS and SIL Verification[J]. Reliability Engineering & System Safety, 2012, 108: 56-64.

[5] XU X Z, WANG G Y, DING S F, et al. A New Method For Constructing Granular Neural Networks Based On Rule Extraction And Extreme Learning Machine[J]. Pattern Recognition Letters, 2015, 67: 138-144.

[6] DARAAMOLA O, STALHANE T, MOSER T, et al. A Conceptual Framework for Semantic Case-based Safety Analysis[C]// Emerging Technologies & Factory Automation (ETFA). IEEE, 2011: 1-8.

[7] ZHANG Y J, SUN Y C. Safety Risk Assessment of Human-machine Interaction Behavior in Cockpit[C]// Computational Intelligence and Design (ISCID). IEEE, 2014: 39-42.

[8] ZHOU H M, HUANG G B, LIN Z P, et al. Stacked Extreme Learning Machines [J]. IEEE Transactions on Cybernetics, 2015, 45(9): 2013-2025.

[9] LIANG N Y, HUANG G B, SARATCHADRAN P, et al. A Fast and Accurate Online Sequential Learning Algorithm for Feedforward Networks[J]. IEEE Transactions on Neural Networks, 2006, 17(6): 1411-1423.

[10] JAVED K, GOURIVEAU R, ZERHOUNI N. A New Multivariate Approach for Prognostics Based on Extreme Learning Machine and Fuzzy Clustering[J]. IEEE Transactions on Cybernetics, 2015, 45(12): 2626-2639.

[11] ZHANG N, DING S F, SHI Z Z. Denoising Laplacian Multi-Layer Extreme Learning Machine[J]. Neurocomputing, 2016, 171: 1066-1074.

[12] MCDONNELL M D, TISSERA M D, VLADUSICH T, et al. Fast, Simple and Accurate Handwritten Digit Classification by Training Shallow Neural Network Classifiers with the 'Extreme Learning Machine' Algorithm[J]. Plos One, 2015, 10(8).

[13] DENG W Y, ZHENG Q H, CHEN L, et al. Research On Extreme Learning of Neural Networks [J]. Chinese Journal of Computers, 2010, 33(2): 279-287. (in Chinese)
邓万宇, 郑庆华, 陈琳, 等. 神经网络急速学习方法研究[J]. 计算机学报, 2010, 33(2): 279-287.

[14] BUENO-CRESPO A, GARCIA-LAENCINA P J, SANCHO-GOMEZ J L, et al. Neural Architecture Design Based On Extreme Learning Machine[J]. Neural Networks, 2013, 48: 19-24.

[15] JOLLIFFE I T. Principal Component Analysis[M]. New York: Wiley Online Library, 2010.

[16] MOZAFFARI A, LASHGARIAN A N, FATHI A. Regularized Machine Learning Through Constraint Swarm And Evolutionary Computation Applied To Regression Problems[J]. International Journal of Intelligent Computing and Cybernetics, 2014, 7(4): 346-381.

[17] ZHU W T, MIAO J, QING L Y. Constrained Extreme Learning Machine: a Novel Highly Discriminative Random Feedforward Neural Network[C] // Proceedings of The 2014 International Joint Conference On Neural Networks. IEEE, 2014: 800-807.

[18] ZHAO R, MAO K Z. Semi-Random Projection for Dimensionality Reduction and Extreme Learning Machine in High-Dimensional Space [J]. IEEE Computational Intelligence Magazine, 2015, 10(3): 30-41.

[19] LI C, RENE-VINICIO S, ZURITA G, et al. Multimodal Deep Support Vector Classification With Homologous Features And Its Application To Gearbox Fault Diagnosis[J]. Neurocomputing, 2015, 168: 119-27.

[20] LIU B, XIA S X, MENG F R, et al. Manifold regularized extreme learning machine [J]. Neural Computing and Applications, 2016, 27(2): 255-269.

(上接第 88 页)

[14] LIU Z Q, WANG Y X, SMOLA, et al. Fast Differentially Private Matrix Factorization[C] // Proceedings of the 9th ACM Conference on Recommender Systems. Vienna, Austria, 2015: 171-178.

[15] HUA J Y, XIA C, ZHONG S. Differentially private matrix factorization[C]// Proceedings of the 24th International Conference on Artificial Intelligence. Buenos Aires, Argentina, 2015: 1763-1770.

[16] SWEENEY L. K-anonymity: A model of for protecting privacy [J]. International Journal of Uncertainty, Fuzziness and Knowledge Based System, 2002, 10(5): 557-570.

[17] LI Y, ZHANG X Z. Survey of Research on Differential Privacy [J]. Journal of Application Research of Computers, 2012, 29 (9): 3201-3211. (in Chinese)
李杨, 张新政. 差分隐私保护综述[J]. 计算机应用研究, 2012, 29 (9): 3201-3211.

[18] ZHANG X J, MENG X F. A Survey of Differential Privacy in Data Publication and Analysis[J]. Chinese Journal of Computers, 2014, 37(4): 929-949. (in Chinese)
张啸剑, 孟小峰. 面向数据发布和分析的差分隐私保护研究[J]. 计算机学报, 2014, 37(4): 929-949.

[19] DWORK C. Differential Privacy: A Survey of Results[C]// Theory and Applications of Models of Computation (TAMC2008). Berlin, 2008: 1-9.

[20] NISSIM K, RASKHODNIKOVA S, SMITH A. Smooth sensitivity and sampling in private data analysis[C]// Proceedings of the 39th Annual ACM Symposium on Theroy of Computing. San Diego, USA, 2007: 75-84.

[21] DWORK C, MCSHERRY F, NISSIMK, et al. Calibrating Noise to Sensitivity in Private Data Analysis[C]// Proceedings of the 3th Theory of Cryptography Conference (TCC). New York, USA, 2006: 363-385.

[22] MCSHERRY F. Privacy Int egrated Queries: An Extensible Platform for Privacy-Preserving Data Analysis[C]// Proceedings of the ACM SIGMOD International Conference on Management of Data (SIGMOD). Providence, Rhode Island, USA, 2009: 19-30.