文章编号:2095-0411(2018)02-0069-08

基于用户鼠标行为的身份认证方法

陈 功[1],朱佳俊[1,2],施 勇[1],薛 质[1]

(1. 上海交通大学 网络空间安全学院,上海 200240; 2. 上海交通大学 数学科学学院,上海 200240)

摘要:提出一种基于用户鼠标行为特征的身份认证方法,通过对用户的鼠标行为数据进行分析,归纳出两类鼠标行为特征,基于鼠标基本行为的一级特征,以及基于基本行为关系的二级特征,并采用极限学习机作为分类算法实现对用户身份的认证。通过实验表明所提出的二级特征能够有效降低认证方法的认假率,而极限学习机因其良好的泛化能力与优秀的学习速度是合适的认证算法。

关键词:鼠标行为;极限学习机;身份认证

中图分类号:TP 309 **文献标志码**:A **doi**:10.3969/j.issn.2095-0411.2018.02.010

User Authentication Method Based on Mouse Dynamics

CHEN Gong[1], ZHU Jiajun[1,2], SHI Yong[1], XUE Zhi[1]

(1. School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China; 2. School of Mathematical Science, Shanghai Jiao Tong University, Shanghai 200240, China)

Abstract: This paper presents a user authentication method based on mouse dynamics as a behavioral biometric. Two kinds of features are proposed to characterize a user's unique pattern of the interaction with mouse device. One-level features are fine-granted metrics extracted for accurate characterization of five basic mouse actions and two-level features are defined based on the relations between the basic mouse actions. Extreme Learning Machine (ELM) is utilized for quick and efficient classification. The efficacy of the proposed features and verification method are evaluated by experiments based on a publicly available dataset. The experimental results demonstrate the high efficiency of ELM in verifying users' identities based on mouse dynamics.

Key words: mouse dynamics; extreme learning machine; user authentication

随着信息技术日新月异的发展,互联网已经融入到社会生活的方方面面。一方面,信息系统使得人们的工作与生活更加高效便利;另一方面,如何保障用户的隐私与财产安全是社会信息化新阶段的重要课题。用户的身份认证,即确认用户是否具有相应的访问或操作权限,是保障信息系统内数据与资产安

收稿日期:2017-11-10。

基金项目:国家自然科学基金资助项目(51375062,514755050);江苏省重点研发计划项目(BE2015043)。

作者简介:陈功(1989—),男,江苏南通人,硕士生。通信联系人:薛质(1971—),E-mail: zxue@sjtu.edu.cn

全的第一关卡,具有举足轻重的地位。

生物认证作为一种新的身份认证技术,通过用户本身的生物特征对其身份进行识别,不仅克服了传统认证技术的缺陷,而且具有更高的可靠性[1]。根据利用信息的不同,生物认证技术可分为基于生理特征的认证与基于行为特征的认证。目前广泛使用的指纹认证、虹膜认证均属于基于生理特征的认证,然而这类认证手段不仅需要额外的硬件支持,提高了整个认证系统的成本,而且需要独立的特征采集过程,无法实现实时无干扰的认证。基于行为特征的认证技术则是利用了不同用户在人机交互过程中所采取的行为(对键盘、鼠标、触摸屏等输入设备的操作)之间的差异性,无需额外的辅助设备,具有成本低、可移植性高等优点[2]。目前,对用户行为特征的研究主要集中于击键动力学(即用户在键盘上的击键行为)方面并已有较为成熟的研究成果[3-5],但在图形交互界面(Graphical User Interface, GUI)广泛普及的时代,鼠标已成为许多用户最常用的输入设备,而鼠标动力学也逐渐成为该领域的研究热点。

文章提出了一种基于用户鼠标行为特征的身份认证技术,通过分析用户在多个连续时间段内操作鼠标的行为数据,提出了两类鼠标行为特征来描述用户的鼠标行为模式,并利用极限学习机进行准确高效地分类,最终实现对用户的身份认证。

1 研究进展

鼠标动力学的研究目的是通过对用户的鼠标行为数据进行特征的提取,实现对用户行为模式的建模与量化分析,从而达到异常行为检测、身份认证、身份识别等目的。

Ahmed 等首次提出在入侵检测中将击键动力学与鼠标动力学相结合[6],并进一步在[7]中提出了基于鼠标动力学的生物行为特征,表明不同个体的鼠标行为之间确实存在差异性。Ahmed 等尝试为每一个用户建立独有的鼠标动力学签名(Mouse Dynamics Signature, MDS),并取得了良好的实验结果,但需要每个用户提供将近 13h 的输入数据,使得数据采集过程十分漫长,无法移植于用户身份认证领域。Gamboa 等通过搭建网页互动系统(Web Interaction Display and Monitoring, WIDAM)监视用户在进行记忆游戏过程中的鼠标行为,实现对用户人机交互行为数据的采集与存储,并利用贪心搜索算法选出能够描述用户身份的最佳特征集[8]。Pusara 等记录了 18 个用户在 Internet Explorer 中浏览网页的鼠标行为,利用决策树作为分类算法尝试对用户身份进行再认证[9]。Hashia 等设计的认证系统要求用户在登陆时将鼠标逐次移动到指定的点位,并将该过程中采集的用户行为数据特征与用户注册时的行为进行比对[10]。Oliveira 等利用在线的数据挖掘系统,从用户的鼠标行为数据中提取了 217 项特征并生成 CSV 文件,为身份认证系统提供了数据支持[11]。然而,这些研究都要求用户在特定的环境下进行指定的操作,无法准确地反映真实世界中用户使用鼠标的场景。

近几年,机器学习在身份认证领域一直具有杰出的表现,也被引入到对鼠标行为分析的方法之中。Nakkabi 等利用模糊聚类算法对[7]中的分类算法进行了改进,大幅提高了身份认证的准确率[12]。Shen 等与 Zheng 等采用支持向量机作为分类方法处理用户的鼠标行为数据,并取得了良好的效果[13-14]。

2 基于鼠标行为的身份认证

2.1 用户鼠标行为分析

用户鼠标行为主要由用户当时所进行的活动来决定,但同时也会受到用户的生理特征、行为习惯或心理状态的影响,使得不同用户的鼠标行为特征呈现出一定的差异性,因此对鼠标行为的分析能够在一定程度上揭示用户的身份特征,成为实现用户身份认证的依据。

本文将第 i 个时刻记录的用户鼠标行为表示为 $\{t_i, B_i, S_i, x_i, y_i\}$，其中 t_i 为记录时刻（以 s 为单位，记录起始时刻为 0s），x_i 与 y_i 为鼠标指针的坐标（以像素为单位，屏幕左下角为坐标原点），B_i 与 S_i 分别为鼠标的按键及其对应状态，其关系见表 1。

表 1　鼠标的按键及其状态

按键(B)	—	Left	Right	—	Scroll
状态(S)	Move	Press/Release	Press/Release	Drag	Up/Down

基于对用户鼠标行为的分析，本文提出了 57 项鼠标行为特征，包括 47 项一级特征以及 10 项二级特征，其中一级特征是对鼠标基本行为的量化描述，而二级特征则反映了基本行为之间的关系，具体如表 2 所示。

表 2　描述用户鼠标行为的特征

特征类别		特征描述	特征编号
一级特征	移动行为	8 个方向的平移次数、平移速度的均值与标准差	1～24
		角速度的均值与标准差	25～26
	点击行为	左键单击所用时间的均值与标准差	27～28
		右键单击所用时间的均值与标准差	29～30
		双击内的两次单击时间与其时间间隔的均值、标准差	31～36
	拖拽行为	拖拽速度的均值与标准差	37～38
	滚屏行为	向上滚屏的次数，滚屏时间的均值与标准差	39～41
		向下滚屏的次数，滚屏时间的均值与标准差	42～44
	静置行为	静置时间占比，静置时间的均值与标准差	45～47
二级特征	转换关系	鼠标移动到左击的转换时间的均值与标准差	48～49
		鼠标移动到右击的转换时间的均值与标准差	50～51
		按下左键到拖拽的转换时间的均值与标准差	52～53
		拖拽到松开左键的转换时间的均值与标准差	54～55
	嵌套关系	滚屏内鼠标移动速度的均值与标准差	56～57

2.1.1　一级特征

用户的鼠标行为可以看作 5 类基本行为在时间上的有序排列：移动、点击、拖拽、滚屏与静置。不同用户对鼠标的基本操作会受其生理特性或使用习惯的影响，例如手腕的移动速度、手指点击的力度、对鼠标左右键的熟悉程度等。

1）移动行为

鼠标的移动行为可通过鼠标的移动轨迹特征来描述，其存储形式为一系列记录的指针坐标。Gamboa 等为了获得更准确的鼠标轨迹，对 WIDAM 所采集的坐标点进行三次多项式拟合[9]，但是拟合曲线与真实的鼠标移动轨迹存在一定的偏差，降低了数据的可靠性，因此本文只考虑采集的原始指针坐标。

鼠标的移动行为可分为平移与转向，分别选取平移速度与角速度作为两类行为的量化特征。设在 i 时刻，鼠标指针所在的点位为 P_i，则 P_{i-1}，P_i，P_{i+1} 为鼠标移动轨迹上连续的 3 个点，向量 $\boldsymbol{P}_{i-1}\boldsymbol{P}_i$ 为一次平移，折线 $P_{i-1}P_iP_{i+1}$ 为一次转向，其平移速度与角速度分别为

$$v_i = \frac{\| \boldsymbol{P}_{i-1}\boldsymbol{P}_i \|}{t_i - t_{i-1}}, \omega_i = \frac{\angle P_{i-1}P_iP_{i+1}}{t_{i+1} - t_{i-1}} \tag{1}$$

根据 Ahmed 等的研究，用户在不同方向上的鼠标行为存在显著差异[7]，因此移动方向也是鼠标移动行为的重要特征。如图 1 所示，以 45°为区间规定 8 个鼠标移动方向。由于转向行为并无明确的方向

可言,因此仅对各方向上的平移行为进行特征统计。选取各方向上平移行为的数目、各方向上平移速度的均值与标准差、角速度的均值与标准差作为描述鼠标移动行为的一级特征。

2)点击行为

鼠标的点击行为由按下按键与松开按键 2 种基本操作组成,根据按键及点击次数不同分为左键单击、右键单击与双击。单击行为包含一次按下按键与松开按键的行为,其所用时间为 2 个行为之间的时间差,即

$$\delta_i = t_i - t_{i-1} \tag{2}$$

双击行为由两次相邻的单击行为组成,所用时间为两次单击时间与其间隔时间之和。本文设定双击内的两次点击间隔不得超过 0.5s,否则视为连续的两次单击行为。

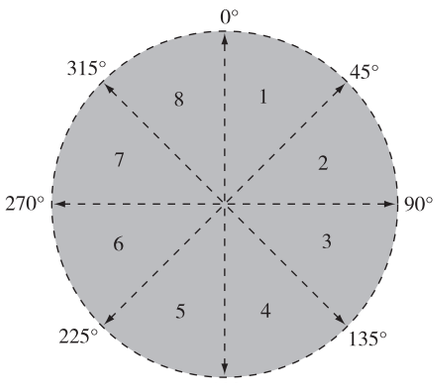


图 1 鼠标移动方向的区域划分

3)拖拽行为

鼠标的拖拽行为可以视为一段时间内保持左键按下的移动行为,以按下左键为始,松开左键为终。一般而言,在用户日常使用鼠标的过程中,拖拽行为在数量上远小于移动行为,因此本文在分析拖拽行为时不考虑指针的移动方向。将拖拽过程中鼠标指针平移速度的均值作为拖拽速度,即

$$v_d = \sum_i v_i / \mathrm{count}\{i\} \tag{3}$$

式中 count$\{i\}$为拖拽次数,并将拖拽速度的均值与标准差作为描述鼠标拖拽行为的一级特征。需要注意的是,有些用户在进行鼠标单击的行为时,会因迟疑的心理或行为习惯等原因,在保持按住按键一段时间后才松开,这段时间内鼠标产生的轻微移动不应视为拖拽行为,因此本文设定只有当鼠标指针的移动超出一定的范围(4×4 的像素区域)时才视为有效的拖拽行为。

4)滚屏行为

鼠标的滚屏行为根据滚屏的方向分为向上与向下滚屏。本文分别统计两类滚屏行为的次数,并取其所用的时间的均值与标准作为描述滚屏行为的一级特征。

5)静置行为

当指针坐标保持不变且持续时间超过一定的阈值(文中设定为 2s),则认为鼠标处于静置状态。考虑到外界因素的影响可能导致一定的系统误差,本文设定当鼠标的位移距离小于 1 像素时,可认为鼠标处于静置状态,并将鼠标保持该状态的时间长度作为静置时间。选取静置时间的均值与标准差,以及静置时间在总时间内的占比作为描述鼠标静置行为的一级特征。

2.1.2 二级特征

用户的鼠标行为往往是多类基本行为的组合,例如当用户在选定文本时,需要依次进行移动、点击、拖拽等行为;当用户浏览网页时,在滚屏翻页时也会进行移动、点击等行为。本文对用户鼠标行为进行分析时,还考虑了基本行为之间的关系,并提出相应的二级特征。

1)转换关系

当用户操作鼠标从一种基本行为转而进行另一种时,需要一定的反应时间,该时间的长短会受到用户对不同操作的熟悉程度或行为习惯的影响。基于基本特征之间的转换关系,选取从鼠标移动到左击,鼠标移动到右击,按下左键到开始拖拽,拖拽结束到松开左键之间的时间间隔作为两种基本行为之间的转换时间,将其均值与标准差作为描述转换关系的二级特征。

2)嵌套关系

基本行为之间的嵌套关系主要出现在鼠标的移动行为与滚屏行为之间，这是由于用户在进行连续的滚屏行为时，往往会穿插进若干鼠标指针的移动行为，通常出现于用户浏览网页或者阅读文章的过程中。将连续的滚屏行为分为一组(本文设定每组滚屏行为之间的时间间隔不小于 1.5s)，计算其间鼠标移动的平移速度，将其均值与标准差作为描述嵌套关系的二级特征。

2.2　基于极限学习机的认证方法

本文所提出的身份认证方法采用极限学习机作为分类器。极限学习机(Extreme Learning Machine，ELM)是由 Huang 等提出的一种新型单隐层反馈神经网络(Single-hidden-Layer-Feedforward neural Network，SLFN)算法[15]。ELM 不仅具有良好的泛化能力，并且相比传统的 BP(Backpropagation)神经网络具有更快的学习速度。

设用户总数为 N'，每个用户的鼠标行为都是一个样本。将第 i 个用户的鼠标行为视为正类，其余 $(N-1)$个用户视为负类，则对第 i 个用户的身份认证问题在本质上是一个二类分类问题，可以通过构建 SLFN 来解决。设样本的特征数为 m，则训练集可表示为 $T=\{X_i \mid 1\leqslant i\leqslant N\}$，其中 $X_i=(x_i,t_i)$为第 i 个样本，$\boldsymbol{x}_i=[x_1,\cdots,x_m]^{\mathrm{T}}$ 为特征向量，$t_i\in\{1,-1\}$为对应的输出(1 表示为正类，-1 表示负类)，则一个隐藏节点数为 L 的 SLFN 可表示为

$$\sum_{j=1}^{L}\beta_j g(W\cdot\boldsymbol{x}_i+b_j)=o_i, \tag{4}$$

式中：$g(x)$为激活函数；β_j 与 b_j 为第 j 个隐藏节点对应的输出权重与偏置；$\boldsymbol{W}_j$ 为对应的输入权重；而 o_i 为 SLFN 的输出，则 SLFN 的学习目标是

$$\min_{\beta_j,\boldsymbol{W}_i,b_j}\ \|\boldsymbol{H}\boldsymbol{\beta}-\boldsymbol{T}\| \tag{5}$$

式中：$\boldsymbol{H}=\begin{bmatrix} g(\boldsymbol{W}_1\cdot\boldsymbol{x}_1+b_1) & \cdots & g(\boldsymbol{W}_1\cdot\boldsymbol{x}_1+b_L)\\ \vdots & \cdots & \vdots \\ g(\boldsymbol{W}_1\cdot\boldsymbol{x}_N+b_1) & \cdots & g(\boldsymbol{W}_1\cdot\boldsymbol{x}_N+b_L)\end{bmatrix}$，$\boldsymbol{\beta}=\begin{bmatrix}\beta_1^{\mathrm{T}}\\ \vdots\\ \beta_L^{\mathrm{T}}\end{bmatrix}$，$\boldsymbol{T}=\begin{bmatrix}t_1\\ \vdots\\ t_N\end{bmatrix}$。该学习目标可以等效于损失函数 $E=\sum_{i=1}^{N}\left(\sum_{j=1}^{L}\beta_j g(\boldsymbol{W}\cdot\boldsymbol{x}_i+b_j)-t_i\right)^2$ 的最小化问题，传统的机器学习方法往往采用梯度下降法求解，通过不断地迭代优化参数来寻找最小值，因此学习速度较慢。ELM 则是通过随机选取输入权重 $\boldsymbol{W}_j$ 与偏置 b_j 来确定隐藏层的输出矩阵 $\boldsymbol{H}$，利用求解线性系统 $\boldsymbol{H}\boldsymbol{\beta}=\boldsymbol{T}$ 来训练神经网络，最后计算出输出权重 $\hat{\beta}=\boldsymbol{H}^{\dagger}\boldsymbol{T}$，其中 $\boldsymbol{H}^{\dagger}$ 为 Moore-Penrose 广义逆。由于 ELM 不需要通过迭代求参，需要确定的参数只有隐藏层节点数 L，因此 ELM 在学习速度上具有相当的优势。

3　实验结果

3.1　数据集

本文所采用的数据来自于 Balabit 提供的公开数据集，其中包括 10 名用户多次利用 RDP 客户端访问远程服务器的会话过程中产生的鼠标行为数据[16]，最初公开于 DataPallet 举办的数据挖掘竞赛。根据竞赛所设置的场景，用户的所有鼠标行为均通过介于客户端与服务器之间的网络监视设备记录并存储，并且对用户的会话长度或操作没有任何限制。除此以外，网络检测设备还监测并记录了若干异常用户的行为，因此 Balabit 数据集所提供的数据能够在一定程度上反映现实场景。

在 Balabit 的数据集中，用户的鼠标行为数据表示为{ Record Timestamp，Client Timestamp，But-

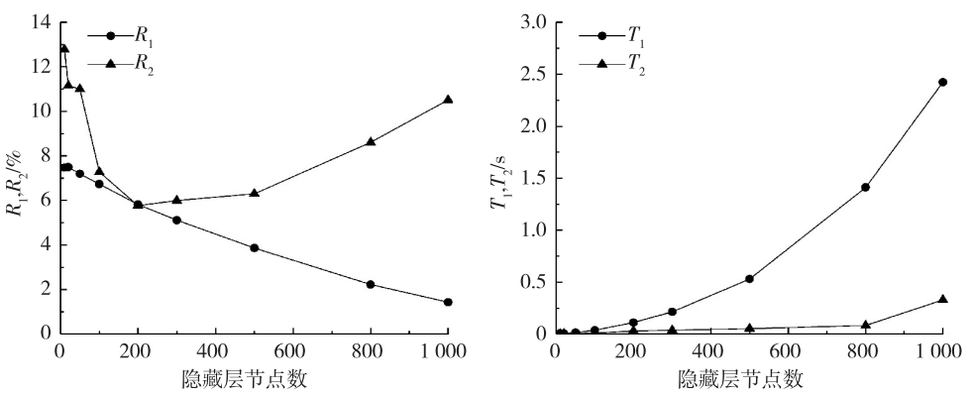
ton, State, x, y }, 其中 Record Timestamp 为网络检测设备记录该条数据的时间戳, Client Timestamp 为 RDP 客户端的记录时间戳, 而 Button, State, x, y 分别对应于 2.1 中的 B_i, S_i, x_i 与 y_i。由于本文考虑的是在终端上的用户身份认证问题, 故选取数据集中的 Client Timestamp 作为鼠标行为的记录时刻 T_i。

3.2 实验结果

为验证所提出的认证算法的有效性, 选取拒真率(False Rejection Rate)和认假率(False Acceptance Rate)作为评价指标, 其中拒真率即认证算法拒绝合法用户访问的概率, 认假率是指将异常用户错误地识别为合法用户的概率。考虑到 ELM 中, 输入层与隐藏层之间的权重与偏置的取值具有随机性, 通常会导致分类结果不稳定, 因此以下所有实验均采用 10-折交叉验证, 并选择 sigmoid 函数作为核函数。

3.2.1 确定 ELM 中隐藏层节点数

ELM 的分类性能与其隐藏层的节点数相关。为了选取合适的节点数目, 对于数据集中的 10 名已知用户, 依次指定其中 1 名为正常用户, 将其余用户(包括异常用户)的鼠标行为标记为异常鼠标行为, 进行身份的鉴别, 并将 10 次交叉验证实验的均值作为最终的实验结果, 共进行 10 轮实验。实验结果如图 2 所示, 其中 R_1 与 R_2 分别为拒真率与认假率, T_1 与 T_2 分别为训练时间与测试时间。



(a) 不同节点数下的FRR与FAR (b) 不同节点数下的训练时间与测试时间

图 2 隐藏层节点数对 ELM 分类性能的影响

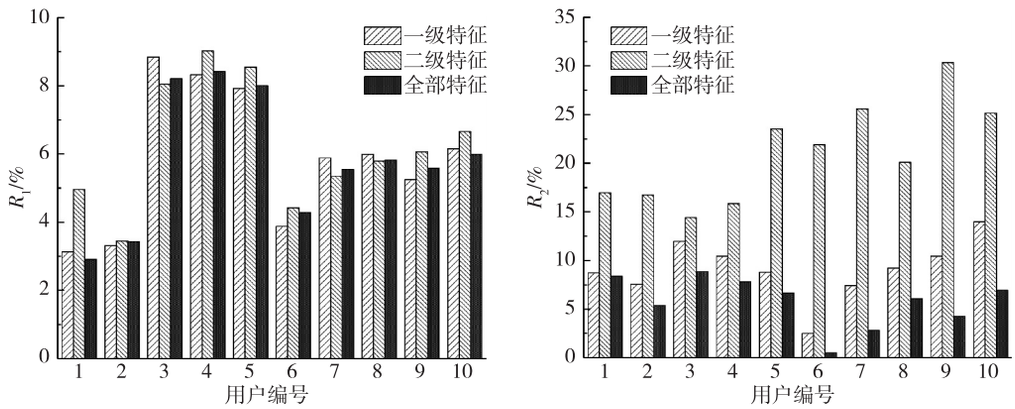
由图 2(a)可知, 当隐藏层的节点数低于 200 时, 增加隐藏层的节点数能够降低拒真率与认假率; 当节点数超过 200 后, 认假率会大幅增加。考虑到隐藏层节点数的增加会提高整个系统的运行时间(如图 2(b)所示), 降低认证系统的效率, 因此选定最佳的隐藏层节点数为 200, 此时拒真率为 5.82%, 认假率为 5.77%, 训练时间与测试时间分别为 0.11s 和 0.03s。

3.2.2 鼠标行为特征对认证性能的影响

为了验证 2.1 中所提出的两类鼠标行为特征对认证效果的影响, 分别在只选择一级特征与只选择二级特征的情形下进行认证实验, 将实验结果与选择全部特征的情形进行对比, 对比结果如图 3 所示。

根据对比实验的结果, 单独选择一级特征或二级特征能够保证较低的拒真率, 说明两类鼠标行为特征都具有一定的有效性; 同时, 在选择一级特征的基础上, 引入二级特征能够大幅降低认假率。对于认证系统而言, 高认假率意味着更高的安全风险, 因此在身份认证中综合选择两类鼠标行为特征具有相当的必要性。

进一步考察认假率的变化可以发现, 引入二级特征对于用户 6 与用户 9 的身份认证效果提升最为明显。根据对各用户不同基本行为的统计(见表 3), 用户 6 与用户 9 的行为种类分布比较分散, 因此其



（a）特征选择对拒真率的影响　　（b）特征选择对认假率的影响

图 3　特征选择对认证结果的影响

鼠标行为之间的关系也更为复杂，这表明了二级特征能够有效地反应鼠标基本行为之间的关系。

表 3　各用户不同基本行为的占比　　%

用户编号	1	2	3	4	5	6	7	8	9	10
移动行为	89.56	91.75	90.01	96.26	93.89	79.99	95.64	96.02	89.41	95.91
点击行为	0.09	0.09	0.05	0.02	0.07	0.08	0.06	0.31	0.05	0.08
拖拽行为	1.05	0.53	1.32	0.53	2.00	0.75	0.47	0.53	0.73	0.64
滚屏行为	4.75	5.88	1.37	1.09	2.64	1.71	0.41	0.37	1.45	0.20
静置行为	4.55	1.75	7.25	2.09	1.39	17.47	3.42	2.76	8.36	3.17

3.2.3　ELM 与其他分类器的比较

为了比较 ELM 与其他传统分类算法的性能优劣，分别采用 CART 分类决策树、BP 神经网络（BPNN）与支持向量机（SVM）基于所提出的鼠标行为特征对每个用户进行身份认证，将实验结果的平均值作为衡量该算法的指标，其结果见表 4（其中 BPNN 的隐藏层节点数设为 20，最大迭代次数设为 500）。

根据表 4 的实验结果，CART 决策树的高拒真率与高认假率使其难以成为合适的身份认证算法，而 BP 神经网络、SVM 与 ELM 在用户身份认证上都具有较高的准确性，然而 ELM 在学习速度上具有显著的优势。要实现实时无干扰的用户身份认证，需要持续地对用户的鼠标行为进行监视与特征提取，不断对分类模型进行训练以提高准确性，因此 ELM 以其较快的训练速度与良好的泛化能力可以成为合适的认证算法，能够保证认证系统的运行效率。

表 4　不同算法的认证结果

算法	训练时间/s	认证时间/s	拒真率/%	认假率/%
CART	0	0.003	10.52	19.30
BPNN	9.42	0.04	6.39	5.76
SVM	4.28	0.02	6.27	6.24
ELM	0.11	0.03	5.82	5.77

4　结　语

文章提出了一种基于用户鼠标行为特征的身份认证方法，提出了基于鼠标基本行为的一级特征以及基于基本行为关系的二级特征，并实现对用户身份的认证。对于复杂的用户鼠标行为，二级特征的引入能够有效地降低认证算法的认假率，进一步提高了身份认证的可靠性。本文通过实验表明了在确定

了合适的隐藏层节点数后,极限学习机能够保证较好的认证准确率,并且在运算效率上比起传统的分类算法具有明显的优势。

参考文献:

[1]MATYAS V, RIHA Z. Toward reliable user authentication through biometrics[J]. IEEE Security & Privacy Magazine, 2003, 1(3): 45-49.

[2]SHI E, NIU Y, JAKOBSSON M, et al. Implicit authentication through learning user behavior[C]// International Conference on Information Security. Berlin: Springer-Verlag, 2011: 99-113.

[3]FOUAD K M, HASSAN B M, HASSAN M F. User authentication based on dynamic keystroke recognition[J]. International Journal of Ambient Computing and Intelligence, 2016, 7(2): 1-32.

[4] MORALES A, FIERREZ J, ORTEGAGARCIA J. Towardspredicting good users for biometric recognition based on keystroke dynamics[C]// European Conference on Computer Vision Workshops. Zurich: Springer, 2016: 711-724.

[5]桑应朋. 基于计算机击键动力学的用户身份鉴别[D]. 成都: 西南交通大学, 2004.

[6] AHMED A A E, TRAORE I. Detecting computer intrusions using behavioral biometrics[C]// Conference on Privacy, Security and Trust St. Andrews: DBLP, 2005: 91-98.

[7]AHMED A A E, TRAORE I. A new biometric technology based on mouse dynamics[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(3): 165-179.

[8]GAMBOA H. A behavioral biometric system based on human-computer interaction[J]. Proceedings of SPIE-The International Society for Optical Engineering, 2004, 5404:381-392.

[9]PUSARA M, BRODLEY C E. User re-authentication via mouse movements[C]// ACM Workshop on Visualization and Data Mining for Computer Security. New York: ACM, 2004:1-8.

[10] HASHIA S, POLLETT C, STAMP M. On using mouse movements as a biometric[C]//In Proceeding in the International Conference on Computer Science and its Applications. Singapore: ICCSA, 2005:143-147.

[11] OLIVEIRA P X, CHANNARAYAPPA V, O'DONNEL E, et al. Mouse movement biometric system[C]//Proceedings of Student-Faculty Research Day. New York: Pace University, 2013: 21-28.

[12] NAKKABI Y, TRAORE I, AHMED A A E. Improving mouse dynamics biometric performance using variance reduction via extractors with separate features[J]. IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 2010, 40(6):1345-1353.

[13] SHEN C, CAI Z, GUAN X, et al. User authentication through mouse dynamics[J]. IEEE Transactions on Information Forensics & Security, 2013, 8(1):16-30.

[14] ZHENG N, PALOSKI A, WANG H. An efficient user verification system using angle-based mouse movement biometrics[J]. ACM Transactions on Information and System Security, 2016, 18(3): 1-27.

[15] HUANG G B, ZHU Q Y, SIEW C K. Extreme learning machine: theory and applications[J]. Neurocomputing, 2006, 70(1): 489-501.

[16] FÜLÖP Á, KOVÁCS L, KURICS T. Balabit mouse dynamics challenge data set[EB/OL]. (2017-06-20)[2017-10-12].https://github.com/balabit/Mouse-Dynamics-Challenge.

(责任编辑:李艳)