基于鼠标行为特征的用户身份认证与监控

沈超[1]，蔡忠闽[1]，管晓宏[1,2]，房超[1]，杜友田[1]

（1. 西安交通大学 智能网络与网络安全教育部重点实验室 机械制造系统工程国家重点实验室，陕西 西安 710049；
2. 清华大学 自动化系 清华信息科学与技术国家实验室，北京 100084）

摘 要：从人机交互和生理行为层面上对计算机用户的鼠标行为进行研究，提取出新的鼠标行为特征，并通过大量实验对鼠标行为特征及特征空间进行了分析，提出了一种利用人机交互时计算机用户的鼠标使用行为特征进行身份认证和监控的方法。同时设计了基于顺序前进贪婪搜索和支持向量机的鼠标生物特征身份识别模型，并通过对 20 个用户进行身份识别与认证实验，得到了 1.67%的误识率和 3.68%的拒识率，该结果明显优于传统的分类识别方法（BP、RBF 和 SOM），展示了基于鼠标行为特征进行身份认证和监控的有效性和可行性。

关键词：生物测定学；顺序前进贪婪搜索；支持向量机；身份认证；身份监控

中图分类号：TP393 **文献标识码：**A **文章编号：**1000-436X(2010)07-0068-08

User authentication and monitoring based on mouse behavioral features

SHEN Chao[1], CAI Zhong-min[1], GUAN Xiao-hong[1,2], FANG Chao[1], DU You-tian[1]

（1. MOE Key Lab for Intelligent Networks and Network Security (KLINNS) and State Key Lab for Manufacturing Systems (SKLMS),Xi'an Jiaotong University, Xi'an 710049, China;
2. Department of Automation, Tsinghua National Lab for Information Science and Technology, Tsinghua University, Beijing 100084, China）

Abstract: With an empirical study of mouse behavioral features using qualitative and quantitative analysis from the physiological layer and the interactive layer, an identif tion method based on sequential forward greedy selection and SVM was proposed. Specifically, an identity verification experiment, in which 20 participants were involved, showed that the performance of proposed method was encouraging with fa acceptance rate (FAR) of 1.67% and false rejection rate (FRR) of 3.68% for user classification. Experimental results show that the proposed method have better performance than conventional classification and recognition methods (BP, RBF, SOM), and also provide a strong evidence for the effectiveness and feasibility of user authentication and monitoring based on mouse activities.

Key words: biometrics; SFGS; SVM; identity authentication; identity monitoring

---

收稿日期：2009-10-28；**修回日期：**2010-04-10

基金项目：国家高技术研究发展计划（"863"计划）基金资助项目（2007AA01Z464, 2007AA01Z475, 2008AA01Z415**）；国家教育部博士点基金资助项目（**20070698107**）；国家自然科学基金创新群体基金资助项目（**60921003**）；国家"十一五"科技支持计划重点课题基金资助项目（**2006BAK11B02**）；国家杰出青年科学基金资助项目（**60825202**）；国家自然科学基金资助项目（**60905018**）**

Foundation Items: The National High Technology Research and Development Program of China (863 Program)(2007AA01Z464, 2007AA01Z475, 2008AA01Z415); The Ph.D. Programs Foundation of Ministry of Education of China (20070698107); The National Natural Science Fund for Innovation Group (60921003); The Key Projects in the National Science & Technology Pillar Program in the Eleventh Five-Year Plan Period (2006BAK11B02); The National Science Fund for Distinguished Young Scholars (60825202); The National Natural Science Foundation of China (60905018)

1　引言

安全的身份认证是保证计算机及网络系统安全的基本前提。现有的身份认证技术主要包括三类[1,2]，分别利用了不同的信息：1）记忆信息，如密码、PIN 等；2）辅助设备、如 ID 卡、令牌等；3）生物特征，如指纹，虹膜等。这些传统的识别技术自身均存有缺陷，如密码难于记忆并容易搞混和泄露，ID 卡需要随身携带且易失窃或失效，生物认证需要额外的硬件设备。鉴于此，研究人员仍然在不断寻找新的身份认证手段和方法。其中基于计算机输入行为特征的认证方法，因为不需要添加额外的设备，在当前大多数计算机系统中可以直接部署，实施无干扰的监控，逐渐成为身份认证研究中的新热点[3~10]。

基于计算机输入行为特征的认证与监控是研究通过键盘、鼠标等计算机输入设备的使用行为特征来识别计算机操作者身份的可行性及相关方法。计算机输入行为研究主要是围绕击键行为特征进行的[3,4]，但随着图形界面的日益普及，鼠标已逐渐超越键盘成为图形交互环境下的主要输入设备，并受到越来越多研究者的关注[5~7,8~14]。从 2003 年开始，国外有 4 个小组对鼠标的使用行为特征进行了初步的研究[5~7,10,12]，内容多为基于统计的鼠标行为特征。2003 年，Ahmed 等人[10]第一次提出了用鼠标行为特征识别用户的可能性，对用户鼠标行为中的一些简单物理量，如鼠标移动速度、鼠标移动距离、单击次数以及这些量之间的关系进行统计分析，结果表明在不同的用户间，这些统计量存在差异，并提出基于这些差异识别用户身份的初步方法。随后，Hocquet 等人[14]进行了一个有 10 个用户参与的实验，得出的结果有 37.5%的错误率。然后 Pusara 和 Brodley[5]提出了一种基于鼠标运动的用户再认证方案。他们提出对于每个用户的每个请求都用决策树分类器建立一个不同的模型。我们小组[8,9]研究了由各种因素引起的鼠标行为波动性对识别效果的影响，将波动性定义为由一系列因素的变化导致的用户鼠标操作模式上的差异，这些因素包括：物理环境，图形用户界面的设定，应用场景，用户计算机熟练度，用户的精神状态，用户的身体状况等。同时，在对鼠标行为特征空间分析的基础上，提出了一种基于降维处理的方法来消除各种因素引起的鼠标行为波动性问题。实验结果表明这些因素都可能引起用户鼠标行为的不确定性，并且发现在鼠标行为特征中存在较强的相关性，而采用主成分分析、流形学习等降维处理的方法可以有效地消除各种因素引起的波动性，减弱行为特征间的相关性，降低这些因素对身份识别精度的影响。

尽管不同研究者得到的识别精度有所差别，但这些工作基本证实了利用用户的鼠标行为特征进行身份区分的可行性。

基于此，本文提出了一种利用人机交互时用户的鼠标使用行为特征进行身份认证和监控的方法。通过采集各种应用环境下的鼠标行为数据，从人机交互和用户生理行为层面上对鼠标行为进行研究，提取出鼠标操作的交互行为特征和生理行为特征并对其进行定性、定量的实验分析。同时，采用基于顺序前进贪婪搜索的特征选择及评价的方法，对 20 个用户 2 个月的鼠标行为数据进行比较分析，并结合支持向量机的方法建立了基于鼠标生物行为特征的身份认证和监控模型。实验结果表明，该方法能够显著提升识别准确度，误识率与拒识率分别从 14.79%和 12.35%降低到 1.67%和 3.68%，明显优于传统的分类识别方法（BP、RBF 和 SOM）。这一结果说明，计算机用户间的鼠标行为存在着显著的不同，借助模式识别的一些方法，可以实现基于鼠标行为特征的较为准确的身份认证和跟踪。

本文结构如下：第 2 节介绍了鼠标行为特征并进行了相应的实验分析；在第 3 节介绍了鼠标行为特征选择及身份认证与监控方法；第 4 节是实验结果及分析；第 5 节是本文的结束语。

2　鼠标行为特征的研究

鼠标行为特征的研究是通过监测计算机用户的鼠标输入，获取用户使用鼠标时的行为特征数据，分析用户的鼠标行为模式，并以此为依据来进行用户身份的认证。日常鼠标动作包括鼠标的移动、鼠标的左右键单击及双击、鼠标的拖拽运动、鼠标中键的滚动及鼠标的静止等。许多图形交互界面中的复杂任务都可以通过一系列简单的鼠标操作来完成。

2.1　鼠标行为特征的简述

基于鼠标行为特征的身份认证中一个基本的假设是：对每个用户而言，其鼠标操作都存在与其他用户具有显著区别的使用模式。对这些不同的模式中鼠标行为进行刻画所得到的特征就构成了鼠

表 1 身份认证与监控模型鼠标行为特征输入向量

特征类别		特征描述	维数编号
对话层特征	操作频率分布	常用的 8 种操作的频率百分比，包括：左键单击、右键单击、中键单击、左键双击、左键拖拽、中键拖拽、中键滚动、静止事件	1~8
	静止时间占空比	在一定监控时间内静止时间所占的比率	9
	屏幕范围分布	用户在划分的屏幕 9 个区域内进行操作所占的百分比	10~18
	移动距离频率	3 种距离范围下移动的频率百分比	19~21
	移动方向频率	8 个方向上进行移动操作的频率百分比	22~29
生理层特征	单击时间间隔	左键单击时间间隔的均值，方差	30~31
	双击时间间隔	左键双击总时间间隔及 3 个内部时间间隔的均值，方差	32~39
	平均移动速度	按移动距离将移动分为三类，每类移动的平均移动速度	40~42
	移动速度极值位	按移动距离将移动分为三类，每类移动的速度极值位置	43~45

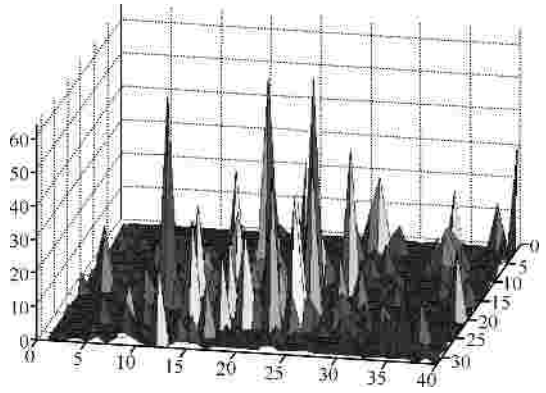
标行为特征。本文从人机交互和用户生理行为层面上的鼠标行为研究出发，提取出了新的鼠标行为特征，并将其分为两类：交互层的特征，与应用环境相关，反映用户使用习惯的特征，如用户经常进行哪些类型的操作；生理层的特征，即用户在使用鼠标过程中所反映出的独特的生理特征，如鼠标移动的轨迹特征等。表 1 是对本文所提取鼠标行为特征的简单描述。

2.2 典型特征分析

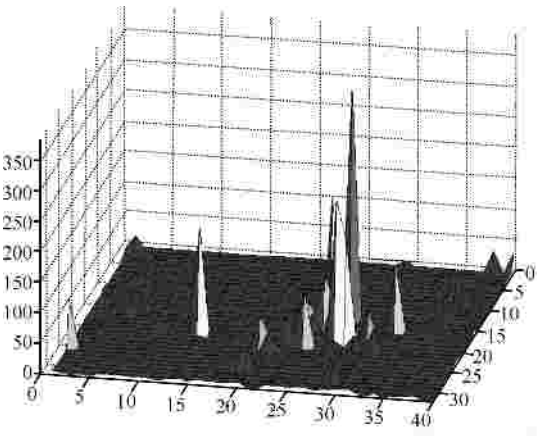
用户在操作鼠标的过程中，因使用习惯及生理习性的差异，其鼠标行为特征也互不相同，例如鼠标单双击的时间，鼠标左右键的使用习惯，鼠标移动时的速度等。产生这些差异的直接原因在于不同用户的鼠标行为操作有较大的区别，例如鼠标的移动和鼠标的点击时间，前者在于不同用户移动鼠标的力度及准确定位能力的不同，而后者在于不同用户点击鼠标的手指力度的不同；间接原因则跟用户的精神状态以及用户对操作过程的熟悉程度有关。下面，本文通过对部分鼠标行为特征的定性、定量的实验分析，初步验证了基于鼠标行为特征对用户身份进行区分的有效性及可行性。

2.2.1 鼠标操作在屏幕区域的分布

实验记录用户在自然状态下的鼠标行为或在模拟 GUI 界面下完成指定的动作采集行为数据，统计用户鼠标操作在各个屏幕区域所占的比例。图 1 中 x, y 坐标轴表示计算机屏幕的水平和竖直方向，z 坐标轴表示鼠标在相应屏幕区域内的操作次数，可以看出：与其他生物测定学特征类似，鼠标操作在屏幕区域的分布情况在不同用户间有着较大的差异，图 1(a)的操作大部分集中在屏幕中部的区域，且分布比较分散，而图 1(b)的操作非常集中，且都分布在屏幕的小范围内。



(a) 用户 1



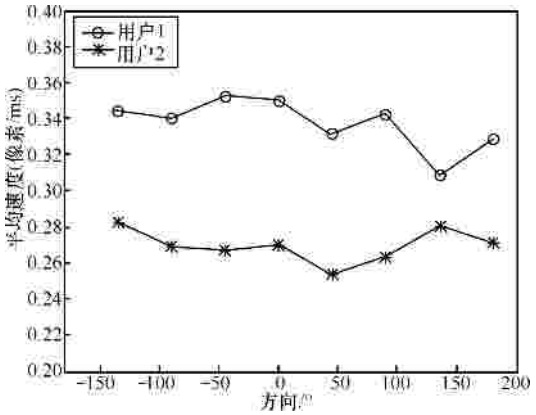
(b)用户 2

图 1 不同用户鼠标操作在屏幕不同区域分布

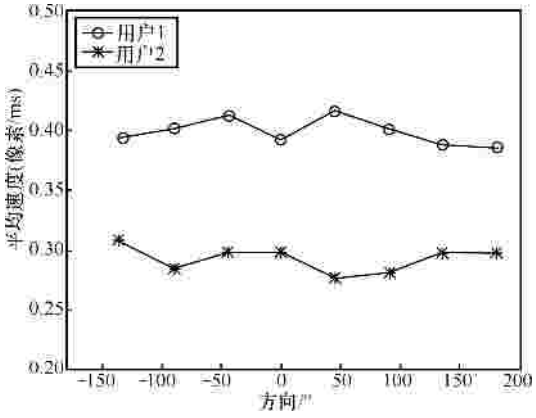
2.2.2 移动速度与距离、方向、目标大小的关系

实验在模拟图形交互界面的环境中，要求用户将鼠标从起点移至目标位置并点击。起点位于计算机屏幕的中心，移动距离是固定的，目标位于起点周围 0^o、45^o、90^o、135^o、180^o、-135^o、-90^o 和 -45^o 8 个方向，并且目标面积的大小分别为 5mm、8mm 和 12mm 的圆。采取随机在 8 个方向上弹出对话框的方式来测试移动速度与移动方向和目标大小的

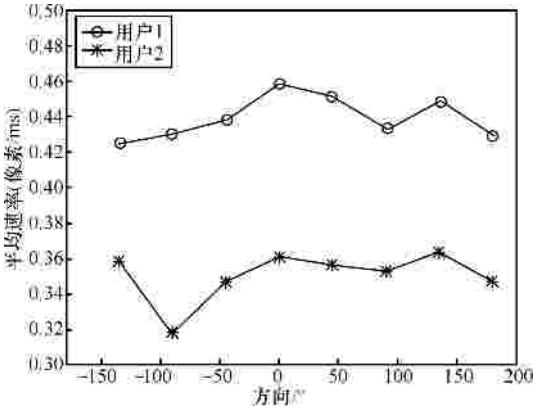
关系。不同用户在相同移动距离下平均移动速度与移动方向和目标大小的关系如图 2 所示。从中可以看出，鼠标在各个方向上的移动速度以及速度随着方向的变化趋势均存有差异。移动速度随目标面积的加大而增大，其原因是：目标越小，定位操作精度越高，移动时间越长。



(a) 多方向速度图（目标大小为 5mm）



(b) 多方向速度图（目标大小为 8mm）



(c) 多方向速度图（目标大小为 12mm）

图 2　目标大小分别为 5mm、8mm 和 12mm

2.3　特征提取

鼠标数据是以人机交互过程中的会话为单位获取的，每个会话包含用户 30min 的鼠标活动数据。对采集到的每个会话的鼠标数据，提取鼠标操作频率分布、静止事件占空比、操作屏幕范围分布、移动时间频率、移动方向频率、单击时间间隔、双击时间间隔、平均移动速度这 8 个特征子集构成了用户鼠标行为特征样本集。

3　特征选择及身份认证与监控方法

由各种鼠标行为特征组成的参量空间就是鼠标行为的特征空间。特征空间中的各种特征从不同方面描述了鼠标行为的特性或鼠标行为的表现形式，是鼠标行为分析和识别的有效标志。本文针对计算机用户在人机交互过程中所形成的鼠标行为特征空间，评价并选择最佳的特征组合，并研究基于鼠标行为特征空间的身份识别方法。

3.1　基于顺序前进贪婪(SFGS)的特征选择与评价

顺序前进贪婪选择（SFGS, sequential forward greedy selection）是使每一步所做的选择看起来都是当前最佳的，期望通过所做的局部最优选择来产生出一个全局最优解。设由鼠标行为特征样本集生成的行为特征集矩阵为

$$\boldsymbol{F}=\begin{bmatrix} f_{11} & f_{12} & \cdots & f_{1n} \\ f_{21} & f_{22} & \cdots & f_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ f_{m1} & f_{m2} & \cdots & f_{mn} \end{bmatrix} \tag{1}$$

其中，f_{ij} 表示第 i 个样本的第 j 个特征，m 和 n 分别表示样本和特征的个数。首先，本文定义了分类准确度对特征选择的过程进行评价：$d_{ij}=\frac{S_r}{S}$，d_{ij} 表示对 i 维的特征变量组合的第 j 类特征组合进行测试的分类准确度，S 表示所有测试样本的个数，S_r 表示在测试时正确分类样本的个数；然后，从所有的特征变量中选取出 d_{1j} 值最佳的特征变量组合，并以此特征变量为基础，增加一个维度，计算所有二维可能组合的 d_{2j} 值，并选出最佳值；接下来，在已选特征的基础上每次按照评价准则从备选特征中选择一个与已选特征子集组合对分类贡献最大的特征加入子集，顺序加入，直到分类识别准确率不再提高为止。

3.2　基于 SVM 的身份分类识别方法

支持向量机(SVM, support vector machine)[14]是建立在计算学习理论的结构风险最小化原则之上。其主

要思想是针对两类分类问题，在高维空间中寻找一个超平面作为两类的分割，以保证最小的分类错误率。

在基于鼠标行为特征的身份分类识别中，每个类的识别被视为一个独立的两类分类问题。假设所有的用户为 k 类，记为 $L=\{b_1,b_2,\text{L},b_k\}$。设属于类 b_i 的样本个数为 N_i，可以将 k 类的分类问题转化为两类分类问题：对任何一类 b_i 而言，训练正例是该类所包含的全部样本；而反例是在训练集中不属于该类的所有其他类的样本。

令训练集 $E=\{(z_i,y_i)\,|\,i=1,2,\text{L},l\}$，其中 $z_i\in R^N$，$y_i\in\{+1,-1\}$，求 (w,b) 使得

$$R(w,b)=\int\frac{1}{2}\left|f_{w,b}(z)-y\right|\mathrm{d}r\,(x,y) \tag{2}$$

达到最小。其中 $r\,(x,y)$ 表示特征向量 x 与所属类别的联合分布密度 $f_{w,b}(z)=\mathrm{sgn}[wz+b]$。为了求出 (w,b)，需求解如下的优化问题：

$$\max\quad W(a)=\sum_{i=1}^{l}a_i-\frac{1}{2}\sum_{i,j=1}^{l}a_ia_jy_iy_j(z_iz_j) \tag{3}$$

同时满足：$0\le a\le g(i=1,2,\text{L},l)$ 与 $\sum_{i=1}^{n}y_ia_i=0$。

接着，为了判断某个样本 x 是否属于类 b，首先计算 $z=F\,(x)$，再计算如下决策函数：

$$f(x)=\mathrm{sgn}\left(\sum_{i=1}^{n}a_iy_i(z_iz)+b\right) \tag{4}$$

若 $f(z)=1$，则 x 就属于类 b，否则 x 就不属于该类。$z=F\,(x)$ 为 SVM 算法中的核函数。

4 实验结果

4.1 身份检测框架

为了能够获取并处理相应的鼠标行为数据，在前述行为特征分析的基础上，本文提出了基于鼠标行为的身份检测框架，如图 3 所示。该框架主要包括 3 个模块：数据获取模块、行为分析模块、行为匹配模块。数据获取模块负责采集用户的鼠标行为数据，进行相应的数据预处理，将原始鼠标数据转换成有意义的操作数据；行为分析模块负责对处理过的数据进行特征提取、特征选择，并产生鼠标的模板特征；行为匹配模块负责训练身份识别算法，对比用户行为特征与模板特征，并产生识别结果。此外，该框架中还包含了相应的数据集用来保存所有已知用户的模板特征，故可以作为实际应用中身份检测的基本框架。

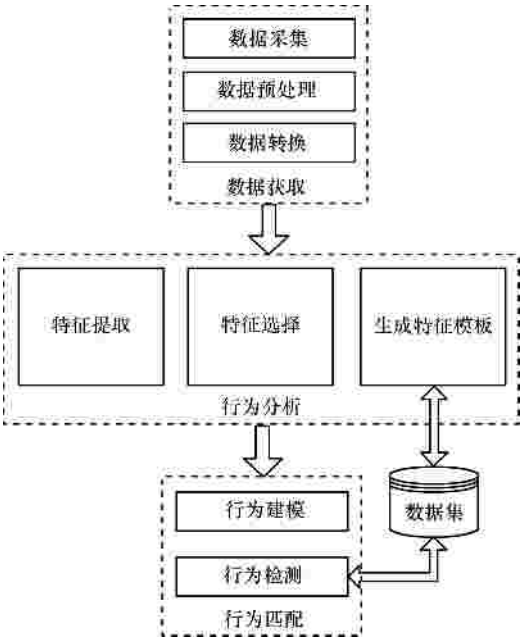


图 3 基于鼠标行为的身份检测框架

4.2 数据采集

鼠标行为数据的采集是在用户的日常工作中完成的，每个参与数据采集的用户都在各自的计算机上安装一个可以被动监控记录用户鼠标行为的软件，并将采集的数据自动送到采集服务器。本文共采集了 20 个计算机用户在 2 个月内的鼠标行为数据，采集的精度为 100sample/s。参与者电脑的显示器均为 17 英寸 LCD，显示分辨率都为 1024×768，内存均为 2GB，其他的硬件配置略有不同的：中央处理器分别为 Pentium 4 2.4GHz（3 台），Pentium 4 2.8GHz（7 台），Core 2 Duo 3.0GHz（10 台），硬盘的大小分别为 80GB（3 台），160GB（17 台）；软件系统使用的是 Windows 不同版本的操作系统：Windows 2000（3 台）和 Windows XP（17 台）。采集到的输入数据包括一系列的鼠标动作、屏幕坐标、系统时间、进程信息等。

4.3 数据预处理

采集到的鼠标数据中或多或少都会存在一些干扰或噪音，对含有这种干扰的数据进行分析，必定会降低识别的准确性。例如，不同的计算机用户有不同的鼠标单击速度，一般人的鼠标单击时间间隔大约在 40~500ms 之间，有时差异可能会更大。如果对所有用户设立统一的过滤阈值，阈值定低了，会将一些点击速度慢的人的正常数据滤除掉；阈值定高了，又会带来很大的误差，因此分别为不同用户确定不同阈值 L_i 是更客观的选择。

$$L_i=kM_i \tag{5}$$

其中，M_i 是第 i 个用户的左键单击时间间隔，系数 k 可以通过一些优化工具来确定。

4.4　实验结果

4.4.1　特征选择与评价实验

本文从 20 个用户中随机选取 10 个用户参与该实验，每个用户采集 30 组数据。同时根据在第 2 节中定义的特征提取方法提取出各个用户相应的鼠标行为特征集，并采用顺序前进贪婪搜索算法进行特征选择和评价。

实验从空特征子集开始，每次加入 1 维特征到已选特征子集中，直到全部 45 维特征都已经选择完毕，最后根据分类准确率从中选取最优的特征组合。表 2 展示了特征选择和评价的结果，表中第 2 列的数字即表 1 中描述的维数编号，对应其所代表的特征。

表 2　身份识别模型鼠标行为特征输入向量

序号	已选特征子集	分类准确率
1	30	76.93%
2	30,2	86.80%
…	…	…
25	30,2,18,31,5,15,45,6,34,23,26, 13,36,21,44,10,17,22,29,19,3,16,1,43,27	97.60%
26	**30,2,18,31,5,15,45,6,34,23,26,13,36,21,44,10,17, 22,29,19,3,16,1,43,27,39**	**97.73%**
27	30,2,18,31,5,15,45,6,34,23,26,13,36,21,44,10,17, 22,29,19,3,16,1,43,27,39,41	97.47%
…	…	…
44	30,2,18,31,5,15,45,6,34,23,26,13,36,21,44,10,17, 22,29,19,3,16,1,43,27,39,41, 7,20,28,14,8,42,40,9,32,11,24,33,4,12,37,35,25	95.73%
45	30,2,18,31,5,15,45,6,34,23,26,13,36,21,44,10,17, 22,29,19,3,16,1,43,27,39,41,7, 20,28,14,8,42,40,9,32,11,24,33,4,12,37,35,25,38	95.60%

从实验结果可以看出，30 号特征（左键单击时间间隔的均值）以及 2 号特征（右键单击的频率）对分类的贡献最大，具有较高的区分性和稳定性。当选择包含 26 维特征的子集{30, 2, 18, 31, 5, 15, 45, 6, 34, 23, 26, 13, 36, 21, 44, 10, 17, 22, 29, 19, 3, 16, 1, 43, 27, 39}时，取得最好的分类准确率，达到了 97.73%，之后再增加新的特征时，分类效果反而有所下降。

4.4.2　基于 SVM 的身份认证实验

1) SVM 建模：核函数选择和参数调整

本文从 20 个用户中随机选取 10 个用户参与这个实验，为了避免正常和异常训练样本比例差距过大，使测试结果受先验偏向的影响过大，每次选取一个用户的 30 组数据作为正常样本，其他 9 个用户各选取 5 组数据作为异常样本，进行 5 折交叉验证实验。交叉验证实验再重复 10 次，每次选取不同的用户作为正常用户，对各次实验的分类准确率做平均。

实验提取全部 45 维特征，采用交叉验证方法，对 Linear、Polynomial、RBF、Sigmoid 4 种核函数分别进行实验测试，实验结果表明放射性核函数 RBF 的分类准确率最高，说明 RBF 核函数能够适应于鼠标行为特征空间的分布特性，因此本文选择 RBF 作为 SVM 模型的核函数。

在 SVM 建模中，还有 2 个重要的模型参数：正则化参数 C 与核函数参数 g 。正则化参数 C 即误差惩罚参数，它决定了对误判样本的惩罚程度，用来平衡模型复杂度和经验风险值，C 的大小对最优分类面的位置有较大影响。考虑到计算复杂度以及 C 和 g 可能互相影响，实验中对参数(C, g)按指数增长序列进行组合，得到的实验结果如图 4 所示。

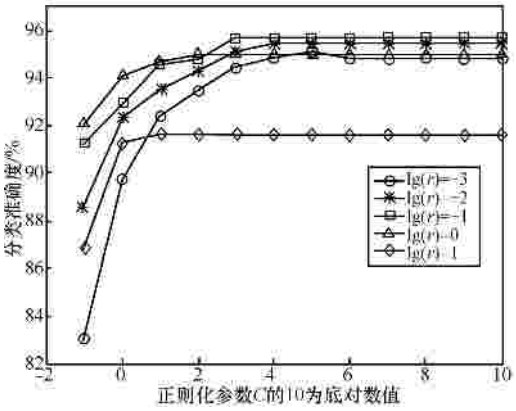


图 4　模型参数组合实验结果

从图 4 中可以看出，当 g 确定时，正则化参数 C 增大到一定值之后，对实验结果的影响不大，分类准确率基本不变。这是由于作为 SVM 算法得到的最优的分类面只能在很小的范围内波动，无论给再大的惩罚，也不能很大程度上改变分类面的位置，因此最后的准确率不会发生太大的变化。实验获得的最优结果是 95.60%，本文在达到这一测试结果的 (C, g)组合中选取 $C=2^5=32$，$g=2^{-1}=0.5$ 作为后续实验中模型的参数。

2) 身份认证实验结果

在本实验中，在经过 SFGS 特征选择与未经过 SFGS 特征选择的前提下，分别采用了 SVM 方法与

传统的分类方法（BP、RBF 和 SOM）进行了身份认证的实验。

本文采集了 20 个用户的数据，总共产生了 600 个鼠标样本集。对每个用户，使用全部样本中的 1/2 作为训练样本，其余 1/2 的样本作为测试样本，根据实验中对除用户 i 之外的 n-1 个用户的异常行为数据的测试结果，计算得到用户 i 的误识率（FAR）；根据对用户 i 的各组数据进行交叉验证时测试的结果，计算得到用户 i 的拒识率（FRR）。对每个用户的误识率和拒识率做平均得到综合的用户身份认证实验结果，如表 3 所示。

表 3 用户身份识别与认证实验结果

方法	经过 SFGS 特征选择		未经过 SFGS 特征选择	
	FAR	*FRR*	*FAR*	*FRR*
SVM	1.67%	3.68%	4.36%	5.58%
BP	7.23%	6.35%	10.77%	7.38%
RBF	7.89%	6.24%	11.25%	7.16%
SOM	10.38%	9.69%	14.79%	12.35%

对未经特征选择的鼠标行为特征样本集采用 SVM 进行分类实验，得到的误识率和拒识率分别为 4.36%和 5.58%，明显优于传统的识别方法（BP 神经网络：*FAR*=10.77%，*FRR*=7.38%；RBF 径向基网络：*FAR*=11.25%，*FRR*=7.16%；SOM 自组织神经网络：*FAR*=14.79%，*FRR*=12.35%）。传统的模式识别方法在解决鼠标行为特征识别这种高位空间中自由分布的问题时，其性能在理论上得不到保证。而 SVM 方法能够合理地将身份识别问题转化为二次寻优问题，在先验知识相对不足的情况下，仍可以保持较好的分类准确率和稳定性，并且该方法通过最大化分类平面的边缘来控制模型的分类能力，不依赖于鼠标行为特征样本的先验概率，具有良好的健壮性。同样对经过特征选择的鼠标行为特征样本集进行相似的实验，实验结果得到了显著的提高，误识率和拒识率分别从 14.79%和 12.35%（SOM 自组织神经网络）降低到 1.67%和 3.68%（SVM）。这说明基于 SFGS 和 SVM 的身份认证和监控方法不但能够选择最佳的鼠标行为特征组合，对各类特征的重要性进行研究，还能降低鼠标特征空间的维数，显著的提高身份认证和监控的准确度。

4.5 实验结果讨论

4.5.1 实验设置的充分性讨论

对用户身份的合法性进行判定主要有 2 种实际的应用需求：身份认证和身份识别。前者是指用户声明自己的身份并利用相关特征数据来证实该身份，将该用户的相关特征数据与其声明用户的模板进行比较，是一种一对一的匹配方法；后者是指不知道用户的身份信息而直接根据其特征数据来确认他的身份，将该用户的特征数据与所有 N 个用户的模板进行比较，是一种一对 N 的匹配方法。相比较而言，身份认证所需的数据量和准确度均低于身份识别。因此，本文采集 20 个用户的鼠标行为数据进行用户的身份认证实验，将认证用户的鼠标行为特征与其声明用户的特征模板进行匹配，判定用户身份的合法性，可以较为充分地支持本文的方法和结论；但若要基于鼠标行为进行用户的身份识别实验，在身份信息不明的情况下确认其身份的合法性，则需要利用更多、更长时间的数据进行分析。

4.5.2 模型训练的实用性讨论

本文中采集到 20 个用户在 2 个月的日常工作中的鼠标行为数据，并利用此数据集对构建的模型进行训练和测试。这样的数据集对于模型的训练来说是充分的，但为了进一步提高模型的可训练性和精确性，在实用中先利用初次获得的数据进行模型的训练，同时将持续监控用户实际的鼠标使用行为并记录相应的数据，将判定后的数据加入先前的数据集中，从而获得足够的、高质量的训练数据，并按照一定的更新规则，对现有的模型进行更新或重构，使模型的训练更加充分，以获得更高的模型检测准确度。

4.5.3 认证与监控的适用性讨论

在实时的身份监控过程，由于可以较长时间地观察用户行为，本文实验中以 30min 为单位观察用户鼠标行为是可行的。但对于身份认证过程，30min 的观察时间是难以接受的，实际应用中须大幅度地降低观察行为所用时间，并对不同的观察时间对检测结果的影响做进一步的研究和分析。同时针对用户鼠标行为中存在趋势性变化或长周期波动，在实用中可以引入自适应机制，构建在线的、实时的自适应检测模型，以解决用户行为发生漂移的情况。

5 结束语

鼠标行为特征识别已成为生物测定学领域的一个新的研究热点，并可部署在各种安全应用之中。本文提出了一种利用人机交互时用户的鼠标使用行为特征进行身份识别的方法。从人机交互和用

户生理行为层面出发，提取出了新的鼠标行为特征，并通过大量实验对鼠标行为特征及特征空间进行了分析。同时对 20 个用户 2 个月的鼠标行为数据进行比较分析，提出了一种基于顺序前进贪婪搜索和支持向量机的身份认证和监控方法。结果表明该方法不但能够选择最佳的鼠标行为特征组合，对各类特征的重要性进行研究，还能降低鼠标特征空间的维数，显著地提高身份认证与监控的准确度。同时验证了计算机用户间的鼠标行为有着显著的不同，借助模式识别的一些方法，可以基于鼠标行为特征实现较为准确的身份认证和跟踪。

参考文献：

[1] O'GORMAN L. Comparing passwords, tokens, and biometrics for user authentication[J]. Proceedings of the IEEE, 2003, 91(12): 2021-2040.

[2] WAYMAN J, JAIN A, MALTONI D. Biometric Systems, Technology, Design and Performance Evaluation[M]. Springer Publishing Company, 2005.

[3] OBAIDAT M S, SADOUN B. Verification of computer users using keystroke dynamics[J]. IEEE Transaction on System, Man, Cybernetics, 1997, 27(2):261-269.

[4] **高艳**, **管晓宏**, **孙国基等**. **基于实时击键序列的主机入侵检测**[J]. **计算机学报**, 2004, 27(3):336-400.
GAO Y, GUAN X H, SUN G J, *et al*. The host-based intrusion detection based on real time keystroke sequences[J]. Chinese Journal of Computers, 2004, 27(3): 336-400.

[5] PUSARA M, BRODLEY C E. User re-authentication via mouse movements[A]. Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, DMSEC Session[C]. Washington DC, USA, 2004. 1-8.

[6] GAMBOA H, FRED A. A behavioral biometric system based on human computer interaction[J]. Proceedings of SPIE, 2004, 54: 4-36.

[7] AHMED A A E, TRAORE I. Anomaly intrusion detection based on biometrics[A]. Proceedings of 6th IEEE Information Assurance Workshop[C]. New York, USA, 2005.452- 453.

[8] **房超**, **蔡忠闽**, **沈超等**. **基于鼠标动力学模型的用户身份认证与监控**[J]. **西安交通大学学报**, 2008, 42(10):1235-1239.
FANG C, CAI Z M, SHEN C, *et al*. Authentication and monitoring of user identities based on mouse dynamics[J]. Journal of Xi'an Jiaotong University, 2008, 42(10):1235-1239.

[9] SHEN C, CAI Z M, GUAN X H, *et al*. Feature analysis of mouse dynamics in identity authentication and monitoring[A]. Proceedings of the 2009 IEEE International Conference on Communication[C]. Dresden, 2009.1-5.

[10] AHMED A A E, TRAORE I. Detecting computer intrusions using behavioral biometrics[A]. 3rd Annual Conference on Privacy, Security and Trust, St[C]. Andrews, Canada, 2005.91-98.

[11] 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.

[12] GARG A, VIDYARAMAN S, UPADHYAYA S, *et al*. USim: a user behavior simulation framework for training and testing idses in GUI based systems[A]. Proceedings of 39th Annual Simulation Symposium[C]. Huntsville, AL, 2006.196-203.

[13] AHMED A A E, TRAORE I. System and Method for Motion-Based Input Device Computer User Profiling[P]. Patent (pending): Filed May 03/2004, International Filing No. PCT/CA2004/000669.

[14] HOCQUET S, RAMEL J Y, CARDOT H. Users authentication by a study of human computer interactions[A]. Proc Eighth Ann.(Doctoral) Meeting on Health, Science and Technology[C]. 2004.

作者简介：

沈超（1985-），男，陕西西安人，西安交通大学博士生，主要研究方向为计算机及网络信息安全。

蔡忠闽（1975-），男，福建晋江人，博士，西安交通大学教授、博士生合作导师，主要研究方向为计算机网络安全、网络化系统行为分析、可信计算。

管晓宏（1955-），男，四川江安人，博士，西安交通大学教授、博士生导师，主要研究方向为计算机网络信息安全、系统优化与调度。

房超（1983-），男，陕西咸阳人，西安交通大学硕士，主要研究方向为计算机及网络信息安全。

杜友田（1980-），男，山东日照人，博士，西安交通大学讲师，主要研究方向为网络信息理解、网络安全及机器学习。