西安交通大學

博士学位论文

基于人机交互形态与动态行为的安全认证与监控方法研究

申请人：沈超

学科专业：控制科学与工程

指导教师：管晓宏教授　蔡忠闽副教授

2014 年 02 月

Secure Authenticaiton and Monitroing through Holistic and Procedural Behavior of User Interaction

A dissertation submitted to

Xi'an Jiaotong University

in partial fulfillment of the requirement

for the degree of

Doctor of Engineering Science

By

Chao Shen

(Control Science and Engineering)

Supervisor: Prof. Xiaohong Guan, Associate Prof. Zhongmin Cai

November 2013

论文题目：基于人机交互形态和动态行为的安全认证和监控方法研究
学科专业：控制科学与工程
申 请 人 ：沈超
指导教师：蔡忠闽 副教授　管晓宏 教授

摘 要

人机交互生物行为特征识别是一种利用用户操作人机交互设备与各种智能终端交互时所产生的人机交互行为特征进行身份安全分析的技术。缺少适合于现有计算环境的有效安全认证和监控手段是造成目前信息系统中身份安全问题日益严重的重要原因。口令、身份卡、指纹等身份验证方式，通常需要额外的硬件设备或难以持续性的对用户身份进行分析，而人机交互行为无需记忆或携带，难以被窃取，不需要额外的硬件，且可无缝融入用户与计算机的交互过程，实现无干扰的全程身份安全分析。

基于人机交互行为的安全认证和监控是个新兴的研究领域，它利用计算机用户操作人机交互设备时所展现的人机交互行为特征进行身份安全的分析。围绕这个主题，本文以最典型的人机交互设备“鼠标”为研究对象，开展了如下几方面的研究工作：

1) 针对人机交互行为的特征建模问题，从鼠标交互行为的时空轨迹形态分析入手，提出了一种基于光标运动时空轨迹形态特征的身份认证方法。解决了复杂人机交互过程的行为特征刻画问题，建立了用户独特的人机交互行为模型，实现了用户身份的准确认证。

2) 针对人机交互行为的行为结构化描述问题，从鼠标交互行为的轨迹形态信息和运动过程信息入手，提出了一种判决级上融合光标轨迹形态特征和运动过程特征的身份认证方法。解决了非结构性人机交互过程的行为表示问题，从形态和动态两方面分别建立了人机交互行为的结构化描述模型，显著的提升了身份认证的精度，有效地缩短了行为认证所需要的时间。

3) 针对人机交互行为的行为波动性问题，从鼠标交互行为中存在的交互模式入手，提出了一种基于频繁交互行为模式挖掘的身份监控方法。解决了多变人机交互过程的行为波动性问题，提取了稳定的行为模式特征刻画量，实现了用户身份的准确检测和监控。

4) 针对计算机和移动网络环境中用户信息感知的需求，根据“人机交互行为包含身份信息”这一结论，提出了一种基于多种人机交互行为的身份隐私属性感知和分析方法。验证了在智能计算系统中利用人机交互行为对操作者身份隐私属性进行感知的可行性，实现了用户身份信息的准确感知和推测，为计算机和移动网络用户信息感知分析提供一种新的技术手段。

5) 创建了 XJTUMOUSE 人机交互行为数据库。从操作数、用户数、应用场景而言，它是当前国际上唯一可获得的中等规模的算法评估数据库。该数据库已经向国内外同行共享。

关 键 词：人机交互；鼠标交互行为；身份认证；身份监控；隐私分析
论文类型：应用研究

Title: Secure Authenticaiton and Monitroing through Holistic and Procedural Behavior of User Interaction

Speciality: Control Science and Engineering
Applicant: Chao Shen
Supervisor: Prof. Zhongmin Cai, Prof. Xiaohong Guan

ABSTRACT

User interaction biometric is the analysis of interactions between users and intelligent systems to identify users' identity, and has recently experienced growing interest from computer security and biometrics researchers. The lack of a reliable and convenient security mechanism to identity verification is the main reason to increasing identity security problems in information systems. Traditional verification mechanism, like Password, ID card, and fingerprint, usually need additional hardware to capture the data or are difficult to continuously (actively) authentication users. While the user interaction behavior has the advantage of no need to memory and carry, requiring no specialized hardware, and could achieve an unobtrusive and non-intrusive secure authentication and monitoring.

As an emerging behavioral biometric, user interaction behavior aims to address the authentication and monitoring problem by verifying users on the basis of their operating styles. Focusing on this topic, this dissertation takes the most typical human interface device, Mouse, as the research object, and mainly includes the following issues:

1) To address the problem of feature modeling of user interaction behavior, we start by analyzing space-time shape characteristics of mouse motion, and present a track-shape-feature-based authentication approach. We establish interaction behavior model for each individual user, and achieve an accurate user authentication.
2) To address the problem of structure description of user interaction behavior, we start by investigating both holistic and procedural information of mouse motion, and present an efficient authentication approach by fusing holistic and procedural behavior characteristics on the decision level. We capture mouse behavior from static and dynamic perspectives, and significantly improve the authentication performance.
3) To address the problem of behavioral variability of user interaction behavior, we start by analyzing recurring behavior segment of mouse interaction behavior, and present a behavior-pattern-mining-based user monitoring approach. We obtain much more stable behavior characteristics from behavior patterns, and reach a practically useful level for realistic deployment.
4) To meet the request of perceiving users' privacy information in the current computing

environment, we present a privacy recognition method based on the conclusion that there is indeed identity information in user interaction behavior. We develop weighted random forest classifiers for five privacy traits – gender, age, ethnicity, handedness, and language, and successfully recognize these demographics. This work presents the first use of user interaction behavior to infer privacy traits of computer users unobtrusively and inexpensively.

5) A public user interaction behavior dataset is established, not only for this study but also to foster future research. This dataset contains high-quality mouse-behavior data from 58 subjects under authentication and monitoring scenarios. To our knowledge, this study is the first to publish a shared mouse-behavior dataset in this field.

KEY WORDS: Human-computer interaction; Mouse interaction behavior; User authentication; User monitoring; Privacy analysis

TYPE OF DISSERTATION: Applied Research

目　录

CONTENTS

1 绪论

随着各类信息系统的应用日益广泛，因身份验证失效造成的各类社会问题也日益严重：股票、网银账号被盗用造成重大财产损失[1,2]，国家敏感机密信息更是面临着前所未有的泄漏风险。现有的基于拥有物（Possession-based，如身份卡）或者基于知识（Knowledge-based，如密码）的身份验证方法有许多局限，如需要携带、易遗忘、易丢失和被篡改等。而生物特征识别技术（Biometric Technology）能够克服这些传统方法所存在的局限和问题，它通过度量难于伪造和篡改的人自身的内在生理或者行为特性来提供身份安全保证。

1.1 身份验证与生物特征识别

1.1.1 身份验证方法

身份验证（Identity Verification）是信息系统安全的核心问题之一。它作为安全策略的重要组成部分，在计算机系统中对用户、设备或其它访问实体身份的合法性进行验证，授予其特定的访问权限，从而保证了计算机资源的安全使用。互联网的普及和电子商务的蓬勃发展，迫切需要一种安全、便宜和使用方便的身份验证技术。

现有的身份验证技术主要包括三类[3]，分别利用了不同的信息：

1) 基于知识的（Knowledge-based），如密码、口令等；

密码和 PIN 的使用构成了最简单的验证机制。验证过程通常对验证代码（用户提供的密码）和校验代码（系统中保存的密码备份）进行字符串匹配。

2) 基于拥有的（Possession-based），如身份卡、令牌等；

密码令牌和智能卡是属于物理验证设备，用来克服密码带来的某些缺点。该方法的好处是不能像密码一样自由地被共享。如果用户把令牌给了其他人，那么这个人可以用来登录，但用户自己就不能进行登录。

3) 基于生物特征（Biometrics-based），如指纹、虹膜等；

生物特征验证依赖于可自动测量的生理或行为特征，用户通过相应的生理特征或行为习惯表明自己的身份信息。

然而，这些传统的身份验证技术都存在自身的缺陷：密码和口令是当前互联网上应用最广泛的身份验证手段，但难于记忆、容易搞混和泄露，安全性不高；ID 卡需要随身携带、易失窃或失效；基于指纹，虹膜甚至是 DNA 等生物特征的身份验证方法是目前国内外研究的热点[4-7]，也是当前最为准确的身份验证手段，但这类方法可能被伪造，需要额外的硬件设备，实施成本较高。

1.1.2 生物特征识别

生物特征识别技术[8]在许多安全场合已经被广泛使用。其概念可以追溯到 1000 多年以前[7]。在东亚，制陶工人将自己的手指印在陶器上，作为表明身份的印记。在埃及的尼罗河谷，商人最初就是根据身高，眼睛的颜色和肤色这些基本的身体特征互相辨认。关于生物特征最普遍的定义是[8]：“A physiological or behavioral characteristics, which can be used to identify and verify the identity of an individual”（能被用户识别和验证人的身份的生理或行为特征）。前已有许多生物度量被用于获取人的身份信息，一些常用的生物特征示例如图 1-1 所示，它们可被大致分为两个类别[9,10]：

1) 生理特征（Physiological Characteristics），来源于人体部分的物理特征量的直接度量。生理特征的示例包括人脸（Face）、指纹（Fingerprint）、虹膜（Iris）、人耳（Ear）、掌纹（Palmprint）、视网膜（Retina），DNA 等，其中最常用的是人脸和指纹。
2) 行为特征（Behavioral Characteristics），来源于人体所实行的具有独特性的行为度量。行为特征的 示例包括声音（Voice）、签名（Signature）、步态（Gait）、击键（Keystroke）等，其中最常用的是声音和签名。

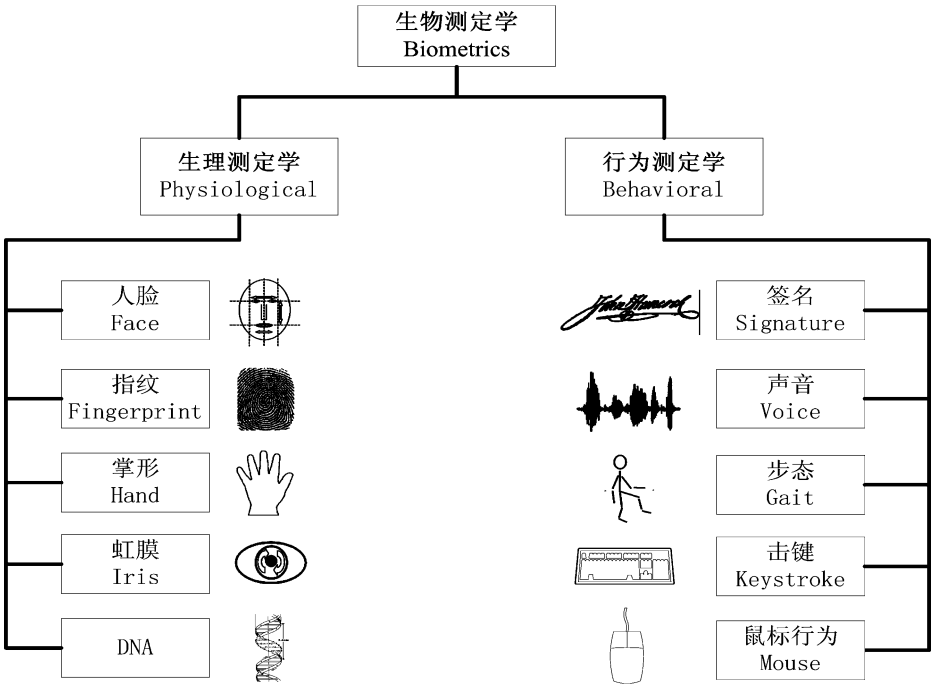


图 1-1 生物特征识别方法的研究分类

生物特征识别是当前的身份安全研究领域的热点，国内外在该领域都进行了大量的研究工作[4,5,7,9,11-16]，特别是生理特征的很多方法和技术已经产品化并投入实际应用。生物特征识别技术因其高度的可靠性和有效性，越来越受到人们的重视。如指纹识别被用于指纹考勤、罪犯鉴定等；为了提高安检效率，很多机场也采用了面部和虹膜识别技术。更新的行为特征，比如鼠标，目前更多地处于研究阶段。相比大多数的生理特征而言，行为特征的判决能力偏弱。这是因为行为特征易受健康状态、用户心情和

时间变化等因素的影响，而生理特征则相对稳定不变。然而基于生理特征的身份验证技术都只在登录计算机时对用户身份进行验证，无法用于计算机使用过程中用户身份的实时监控。

1.2 新兴的人机交互行为特征

人机交互行为（Human-Computer Interaction Behavior）的基本定义为[17]：“A process of using computer to locate and identify human and tracking human body movement in order to understand human behavior and actions, then responds intelligent feedback”（使用计算机交互设备来识别用户身份并追踪用户身体移动的方式，目的是使计算机理解用户的行为和动作，以提供智能的响应）。更加直观地讲，人机交互行为是指用户使用鼠标、键盘、触摸屏等人机交互设备（Human-Interaction Device）操作各类智能终端系统时所产生的交互行为。尽管人机交互行为分析在人机交互、生物力学等领域有着长期的研究，但使用人机交互行为作为生物行为特征用户身份安全分析（身份认证、身份监控、身份隐私分析）则是近年来计算机安全和模式识别领域相对新兴的研究课题。

人机交互过程中的行为特征建模与分析，属于生物行为特征的研究范畴。人机交互过程中的生物行为特征的研究不是生物测定学研究的主流，学术界一直对这方面的研究存在疑虑，最大的争议就在于“特征是否存在”，即动态变化的行为中到底有没有可用于身份识别的稳定不变的特征。早在二次世界大战时期，就有所谓的“Fist of the sender”方法：情报部门根据电报发送员的按键特征来识别发报员的身份[18]。随着各种基于 Internet 的重要网上应用的迅速发展，迫切需要一种可以在现有的计算机体系框架内安全、便宜、方便的解决身份识别问题的方法，而现有的主流生物测定学方法都需要精度较高的专门硬件的支持，自 2003 年以后，研究者们正渐渐对人机交互行为产生了浓厚的兴趣。

作为一类独特的生物行为特征，人机交互行为有着如下的理想特性[6,17]:

1) 独特性（Unique）-- 人机交互行为似乎是独特的，它依赖于个体的手形结构、移动习惯、移动姿势等。手部的运动是非常复杂的动态行为，它涉及到手掌及多个手指的运动以及这些关节之间的交互作用，其特性可归类为静态特征和动态特征。静态特征通常反映那些基于几何的度量。如手部移动距离等[30-33]；相对而言，动态特征对于行为的时间变化比较敏感，如手部的移动快慢[34-36]。由于个体之间身体结构和行为上的基本特性不同，从而人的手部运动为为其作为身份特征提供了一种独特的线索。
2) 非侵犯性（Unobtrusive）-- 人机交互行为能够被秘密提取，而用户并不知道他或她正在被观察和分析。在信息收集阶段，人机交互行为也不象指纹和视网膜那样需要用户的密切协作。尽管今天的一些商业生物特征识别系统已经具备较好的可靠性（如指纹考勤机），然而它们在一定程度上缺乏用户的可接受性[37]。譬如，用户可能反感接触指纹扫描仪、用户不乐意密切注视虹膜捕捉器等，因

为他们认为这也许会损害他们的手和眼睛。使用人机交互行为将会完全避免那样的问题，因为它可以在用户操作计算机的过程中完成数据的捕获和身份的验证，它不需要用户额外的配合，这必然提升了用户的可接受性。

3) 无需额外的硬件（No Need of Additional Equipments）-- 指纹和人脸等生物特征通常需要额外的硬件设备进行生物特征数据的获取 (如指纹需要指纹扫描仪、人脸需要近距离的摄像头等)，而人机交互行为使用标准的计算机输入设备，如鼠标、键盘、触摸屏等，对生物特征数据进行获取，因此极大的降低了实施成本。
4) 难于隐藏（Difficult to Conceal）-- 人脸可能化妆或用面具隐藏；手掌可被模糊；耳朵被头发遮盖看不见等，这些都会导致相应生物特征的失效。然而，用户在使用计算的时候必须操作计算机交互设备，因此用户的人机交互行为通常是可见的。

当然，人机交互行为也有其自身的缺点，它易受如下一些因素的影响：

1) 情绪（Emotion）--情绪（例如高兴或伤心等）可能影响用户的正常人机交互过程。
2) 身体健康（Physical Health）-- 手指或臂膀的受伤、精神方面的剧烈变化等都必然影响用户操作人机交互设备的运动特性。
3) 心理（Psychology）-- 用户的心理变化也会影响人机交互特征，比如心理轻松时人机交互行为的自然和心理紧张时人机交互行为的慌乱等。
4) 熟练程度（Practice）-- 人机交互过程是一个从生涩到熟练的过程，因此用户操作人机交互设备的熟练程度可能影响用户的人机交互行为特征。

尽管上述缺点是人机交互行为特征本质存在的，其它生物行为特征也有着相应的缺点，如易被伪装和更改等，特别是当个体想摆脱识别而不给予合作的时候。一些外部因素，诸如人机交互设别的类型、交互屏幕分辨率的大小等，都影响到了人机交互行为的自动特征提取过程。由于人机交互行为是一种时空变化的交互模式，其处理对象是实时捕获的交互行为数据，因此对它的及时响应性要求也相应较高。

许多过去相关的人机交互行为分析研究工作使我们看到了它的研究前景。如近些年来对键盘交互行为特征的研究表明，所谓的“击键动力学”(Keystroke Dynamics)是一种很好的身份测定指标。根据操作者击键过程中，各个键被按下的持续时间及按键之间的间隔时间，就可以判别出操作者的身份[14,18-29,38-48]。文献[48]中提供的数据表明，击键动力学的识别效果略差于指纹识别方法，却要好于人脸及语音识别方法，见图 1-2。

此外，在 2012 年 12 月份美国国防高级研究项目署 DARPA（Defense Advanced Research Projection Agency）赞助的 Active Athentication（Authentication without the cooperation of users）计划的驱动下[49]，卡内基梅隆大学、加州伯克利大学、麻省理工学院等 12 家高校或公司都计划开展使用人机交互行为进行主动身份认证的工作。有些工作在目前可获得的小数据库上达到了 90％以上的身份认证精度。这些初始的结果令

人鼓舞，同时也激发了更多研究者们对基于人机交互行为的身份安全分析的强烈兴趣。

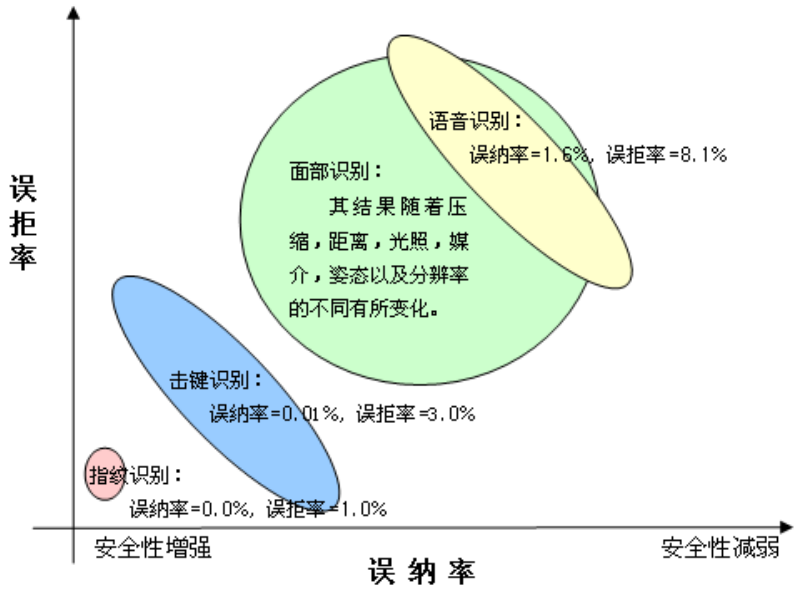


图 1-2 击键动力学与其它生物特征识别方法的结果对比

1.3 人机交互行为的身份验证研究的背景和意义

根据最新的 CSI/FBI 的计算机安全调查报告[49]，越来越多的计算机安全问题来源于内部攻击，如用户离开时忘记退出系统，密码的泄露和破解，指纹等生物信息的伪造等，均可使攻击者顺利通过登录时的验证，以合法用户的身份从内部进行攻击或窃取信息。所以，在计算机使用过程中对异常行为进行检测，实时地对用户身份进行验证显得越来越重要。

人机交互行为特征与操作者的动作习惯，运动控制协调能力以及神经反应速度等多种生理特性具有密切的联系。因此，交互过程中的轨迹形态、速度变化模式，触控操作中手指与触摸屏的接触面积、形状乃至压力等大量行为特征都可为操作者的身份验证提供有价值的信息。基于人机交互行为的身份验证是指计算机通过分析用户人机交互行为特征来验证用户身份真实性的过程。在系统登录过程中验证用户身份真实性称为身份认证，在系统使用过程中验证用户身份真实性称为身份监控。同传统方法相比，该方法具有独特优势：

1) 人机交互行为特征作为身份依据无需记忆或携带，也无法被窃取，安全性高，而且不需要额外的硬件，适用于现有的计算环境；
2) 人机交互行为能够无缝融入人机交互过程，可以实现无干扰的全程身份跟踪与监控。

从方法上讲，基于人机交互行为的身份验证属于生物行为特征识别（Behavioral Biometrics）的范畴[6,50]，后者一直是模式识别领域的重要研究方向。基于人机交互行为的身份验证涉及了人机交互行为特征提取、表达和融合及分类器学习等多个问题。

交互行为特征提取、表达和融合涉及时间序列分析、模式识别和人机交互等多个学科或方向，分类器学习则是模式识别和机器学习中的重要问题。此外，基于人机交互行为的身份验证还与其它科学问题有密切联系，譬如信息系统安全监控[51]，在线手写签名识别[11]和人体快速运动模型的建立[52,53]等，对其进行深入研究必然会促进这些相关科学问题的解决。

综上所述，随着互联网和各种网络应用的蓬勃发展，身份安全问题直接威胁到每个网络用户的切身利益，开展基于人机交互行为的身份认证与监控研究，提出适合于现有计算环境的身份验证新手段和新方法，不仅可以推动模式识别和机器学习等相关领域中重要科学问题的研究进展，而且对于国家政治、社会经济和公众利益的安全也具有重要的现实意义。

1.4 研究内容和论文结构

以计算机用户身份安全分析为研究背景、以目前人机交互行为中最为典型和广泛应用的鼠标交互行为为研究对象，我们进行了基于人机交互行为的身份认证、身份监控和身份隐私分析研究。该研究主要涉及人机交互中鼠标交互行为的结构化描述、特征空间度量、学习器构建等步骤。首先，我们建立了本领域第一个公开的多应用场景下的人机交互行为数据库，即 XJTUMOUSE 数据库，然后针对不同的身份安全问题（身份认证、监控和隐私分析），我们提出了几种简单而有效的身份安全验证方法。论文各个章节安排如下：

第二章详细回顾了基于人机交互行为的身份安全验证的研究现状的，包括其相关研究、当前主要采用的方法、主要的研究难点等。

第三章分析了人机交互行为的输入特性并建立身份认证与监控场景下的行为数据集。实现了三种不同的鼠标交互行为数据截获技术：消息钩子、原始输入和过滤驱动，从采样时钟分辨率、时间精度和位置信息等方面对不同方法所获取数据进行了差异分析。分析结果表明使用消息钩子获取的数据最为丰富和稳定。在使用消息钩子获得原始鼠标交互行为数据上定义并分割了鼠标交互行为操作。

第四章针对人机交互行为的特征建模和认证问题，从鼠标交互行为的时空轨迹形态分析入手，阐述了基于光标运动时空轨迹形态特征的身份认证方法。对于每个交互序列而言，提取描述鼠标交互行为时空轨迹形态的特征向量；利用距离度量和成分分析获取低维的鼠标特征量；引入单分类学习器构建身份认证和识别模型。实验结果表明该算法获得了非常有效的认证性能。

第五章针对人机交互行为的行为结构化描述和多视图建模问题，从鼠标交互行为的轨迹形态信息和运动过程信息入手，描述了判决级上融合光标轨迹形态特征和运动过程特征的身份认证方法。首先采用 Box-Cox 幂指数变化模型对交互行为中的形态信息进行表示，然后基于近邻传播聚类的思想对交互行为中的过程信息进行建模，接着在决策层对两种信息进行融合。在不同融合规则下的实验结果表明：融合认证性能均

优于使用任何单一模态下的认证精度，极大的提升了认证性能。

第六章针对人机交互行为的行为波动性和监控问题，从鼠标交互行为中存在的交互模式入手，介绍了基于频繁交互行为模式挖掘的身份监控方法。首先，结合计算机用户日常操作鼠标进行交互的特性，利用基于模式生长的序列模式挖掘方法获取交互行为的频繁子序列；然后从稳定的频繁子序列中提取稳定的特征刻画量，以精确而有效地用户身份进行监控。实验结果表明该方法能够从行为模式中获取稳定的特征刻画量，极大的提升了身份监控的精度。

第七章针对计算机和移动网络环境中用户信息感知的需求，根据“人机交互行为包含身份信息”这一结论，介绍了基于多种人机交互行为的身份隐私属性感知和分析方法。在随机森林学习框架下，对计算机用户的身份隐私属性进行建模和识别。信息取证分析场景下的实验结果验证了基于鼠标和键盘交互行为对计算机用户的身份隐私属性进行识别和推测的可行性。该方法填补了在智能计算系统中对操作者身份隐私属性进行分析的空白，为计算机用户信息感知分析提供一种新的技术手段。

第八章描述了基于鼠标交互行为的身份认证和监控原型系统。该系统在用户登录及使用计算机过程中实时采集用户的鼠标交互行为数据，为正常用户建立行为特征模型，认证及监控当前用户身份，有效阻止和防御非法用户的侵入。

第九章对全文进行了总结，并展望了未来的研究工作。

（注：所有的研究成果可参见我的个人网站[①]）

① http://nskeylab.xjtu.edu.cn/people/cshen/

2 人机交互行为研究现状

2.1 引言

随着各类信息系统的应用日益广泛，网络银行、电子商城等电子交易账号被盗用造成的重大财产损失，国家敏感机密信息的泄漏所造成的风险，导致各类信息系统的身份安全问题变得日益严峻。而缺少适合于现有计算环境的有效身份安全认证和监控手段是造成这些问题的一个重要原因。作为新兴的生物行为特征，人机交互行为无需记忆或携带，难以被窃取，不需要额外的硬件，且可无缝融入用户与计算机的交互过程，实现无干扰的全程身份安全分析，已成为当前身份安全认证和监控领域的研究热点。本章首先介绍人机交互行为分析在身份安全中的研究现状；接着重点阐述了鼠标交互行为在相关领域的研究现状；然后回顾了当前国际上主要的鼠标交互行为分析方法和应用；最后对其研究难点作了较为详细的分析和讨论。

2.2 基于人机交互行为的身份验证的研究概述

人机交互行为是近年来兴起的研究领域，它旨在从相似的人机交互行为中寻找和提取个体间的可区分的差异来自动进行身份的验证。基于人机交互行为的身份验证系统的一般流程如图 2-1 所示。行为捕获软件在计算机用户登录或使用计算机的过程中记录用户的人机交互行为数据，生成人机交互行为序列；结合行为的语义分析，对行为进行分割和表示；经过行为波动性的处理，得到行为空间中稳定的特征量；结合在行为数据库已经存储的人机交互行为的模板，行为分类器最后给出身份验证的结果。

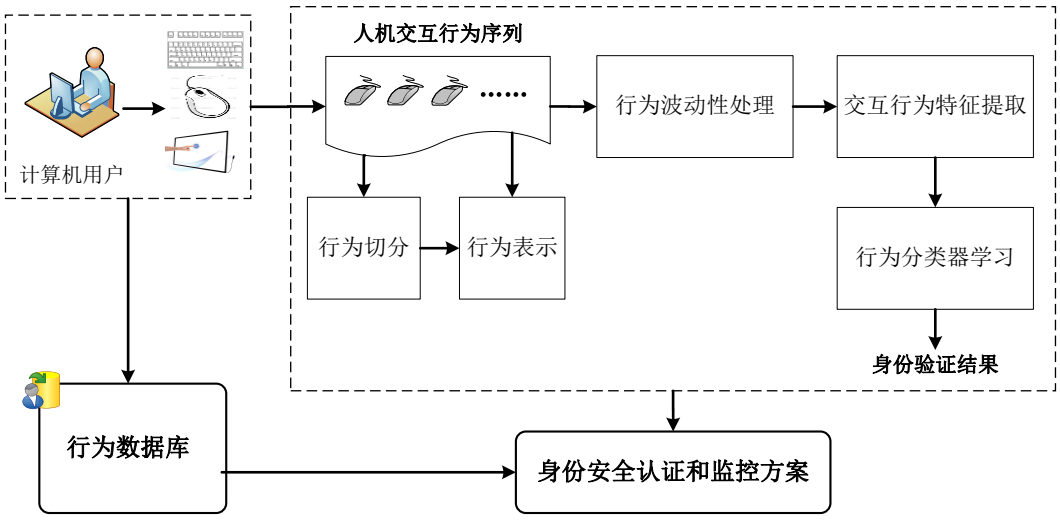


图 2-1 基于人机交互行为的身份验证系统的一般框架

从图 2-1 我们能够看到基于人机交互行为的身份安全验证分析是个非常具有挑战

性的研究课题，它涉及许多困难的问题，比如人机交互行为分析领域中的行为结构化描述（Stucture Description of HCI Behavior）、信号分析领域中的波动性去除（Noise Reduction）和模式识别领域中的特征提取和学习分类器（Feature Extraction and Pattern Classification）等问题。在当前计算环境中，人机交互行为主要包括键盘交互行为、鼠标交互行为、触摸屏交互行为。下面我们分别对这些交互行为进行简单的介绍。

2.2.1 键盘交互行为分析

在图像用户界面（Graphical User Interface, GUI）普及之前，键盘是人机交互过程中最主要的输入设备。键盘交互行为是在人机交互过程中，操作者使用键盘敲击时所展现出的生物行为特征。键盘交互行为产生差异的直接原因在于不同操作者敲击键盘的手指力度和手指移动快慢不同，间接原因则跟操作者的精神状态以及用户对输入字符串的熟悉程度有关。目前的人机交互行为研究主要围绕着用户操作计算机键盘的行为进行[14,18,19]。美国 NSF 和 NIST 的相关研究[18]都表明，用户的键盘交互行为隐含了可用于区分不同用户的独特属性，可以作为一种身份验证和识别的手段。

2.2.2 鼠标交互行为分析

自图形用户界面普及之后，鼠标开始取代键盘，成为图形交互环境下的主要输入设备。击键交互行为研究的进展使研究者们不禁要问，是否也存在“鼠标交互行为”，可以根据用户使用鼠标所产生的交互行为作为生物行为特征对操作者的身份进行验证和识别。鼠标交互行为是当前计算环境下最典型且使用最广泛的人机交互行为。它是指在人机交互过程中，特别是在图形用户界面环境下，操作者使用鼠标时所展现出的生物行为特征。目前，计算机用户输入行为研究主要是围绕击键交互行为特征进行，而鼠标作为图形化人机交互环境下的主要输入设备，对其交互行为特征的研究尚处初级阶段。

2.2.3 触摸屏交互行为分析

随着智能电脑、平板及手机的发展，智能系统开始逐渐提供支持触摸屏的人机交互。触摸屏交互行为是在人机交互过程中，操作者使用触摸屏时所展现出的生物行为特征。目前，触摸屏交互行为的研究主要集中在改进人机交互过程中的用户体验，相关的安全应用还鲜有报导。

2.2.4 小结

鼠标作为当前计算环境下使用最广泛的人机交互输入设备，其交互行为是最为典型的人机交互行为。本文以鼠标交互行为作为研究对象，对基于人机交互行为的身份安全认证和监控方法进行了研究。下面详细阐述了鼠标交互行为在身份安全应用中的研究现状和问题。

2.3 基于鼠标交互行为的身份验证问题描述

尽管鼠标交互行为分析在人机交互学领域（例如费茨法则）已经有着长期的研究，但基于鼠标交互行为的身份安全分析仅仅在近几年才引起了研究者的注意。早期的基于交互行为的身份安全分析主要是围绕用户操作计算机的击键行为进行。国外的研究开始较早[14,18,19]，在 2000 年后开始引起了相关研究者的极大兴趣[20-29]。随着图形用户界面的普及和飞速发展，鼠标开始取代键盘成为图形交互环境下的主要输入设备。最早利用鼠标交互行为进行身份安全分析的是 2003 年 PAMI 上的一篇论文，Everitt 等首次讨论了利用鼠标签名进行身份认证的可能性[54]。它主要涉及基于鼠标交互行为的身份认证框架及移动轨迹刻画方法。

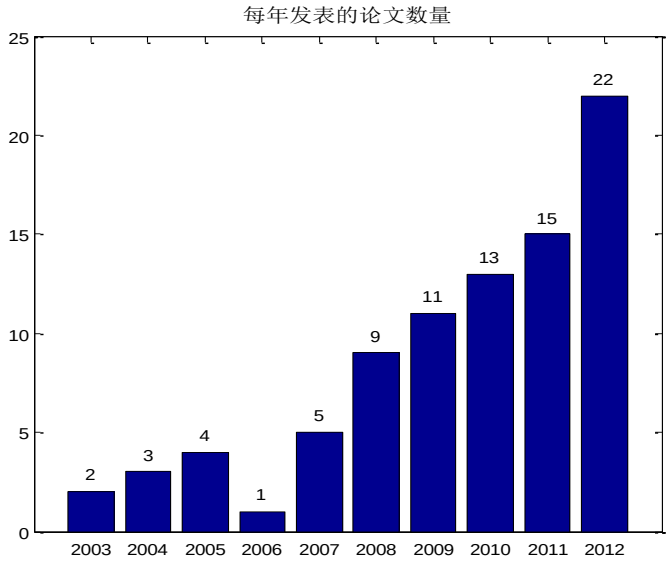


图 2-2 鼠标交互行为分析论文的年发表量

对于鼠标交互行为分析研究的浓厚兴趣导致了近年来基于鼠标交互行为的身份验证技术的快速发展，这可以从粗略统计得到的有关鼠标交互行为分析研究每年发表的论文数量中所看到（见图 2-2）。近年来鼠标行为特征的研究工作逐渐增多[55-83]，相关领域重量级的学术会议上也开始出现不局限于身份验证问题的研究论文：2009 年 ACM 计算机与通讯安全大会（ACM Conference on Computer and Communications Security）有论文讨论鼠标行为特征用于检测网络游戏中的“游戏机器人(Bot)”[84]；2010 年 ACM 信息检索大会（ACM SIGIR Conference on Research and Development in Information Retrieval）又有论文指出鼠标行为特征有助于分析电子商务中用户的购买倾向[85]；2012 年 IEEE 可靠性系统和网络大会（IEEE/IFIP International Conference on Dependable Systems and Networks）有论文使用鼠标交互行为进行身份监控[86]。在其它有关人机交互、模式识别、生物测定学等重要国际会议上，如 CHI（ACM Conference on Human Interaction）、CVPR（International Conference on Computer Vision and Pattern Reconition）、ICB（International Conference on Biometrics）等，也经常可以看到有关

鼠标交互行为分析应用的论文。这表明鼠标交互行为特征研究开始被不同的专业领域所关注，正逐渐成为计算机安全和模式识别研究中的新热点。

这里我们将详细回顾这个令人兴奋的领域。为了完整性，我们也简单给出了基于鼠标交互行为的身份安全研究领域的介绍。当前的鼠标交互行为分析算法和相应的身份安全分析算法是回顾的重点。为了便于讨论，我们特别选择不同的规则和安全应用来归类那些论文到不同的之类中以阐述其研究现状。最后，我们详细讨论了基于鼠标交互行为的身份安全分析的研究难点。

2.4 相关研究领域

鼠标交互行为分析长期以来都是个相对活跃的研究主题，特别是在生物力学（Biomechanics）[52,53]、人机交互学（Human-Computer Interaction）[17]、心理学（Psychology）[87]及计算机安全（Computer Security）[88]等领域。这归因于如下的研究兴趣，如鼠标精确指点定位的需求、行为反应身份信息的能力等。近年来，指点行为建模、行为波动性分析与行为识别技术的发展也为基于鼠标交互行为的身份安全分析提供了强有力的工具。

2.4.1 生物力学领域中鼠标交互行为分析

鼠标的使用主要以手部动作为主，所涉及的肌肉骨骼组织包括手指，手掌、前臂、上臂、腕关节、肘关节、肩膀、颈部以及背部。而手部运动的基本条件是运动的协调和稳定，在操作鼠标时，手部相关的肌群同时起制动和稳定两种作用。了解手部生物力学特点是研究鼠标交互行为操作的前提。

鼠标的使用较常出现手指的屈曲和伸展以及手掌握持的动作[89]。而手指屈曲运动作用的肌群有屈指伸肌、屈指浅肌、蚓状肌以及掌侧骨间肌；手指伸展运动作用的肌群有伸指肌、蚓状肌以及背侧骨阅肌。由于关节本身结构的缘故，手掌只能做二轴的运动。在垂直面上，为掌曲/屈曲（palmar flexion）与背屈/伸展（dorst flexion）；在水平面上，则为尺偏（ulnar deviation）与桡偏（radial deviation）。背屈动作角度可达 75°～80°，掌屈动作则可达 85°～90°；尺偏动作可达 35°～37°，桡偏动作则可达 15°～20°（见图 2-3 和图 2-4）。

鼠标操作主要是以手腕为支点，而控制腕部动作的肌群为手部提供两种功能：手部的初步定位和稳定腕部为手提供工作台。这些功能会引起一系列的前臂动作，主要包括前臂的旋前与旋后运动，而使用鼠标时会有较多的前臂旋前动作。由此可知，鼠标的各种操作是由前臂肌肉调节，并通过腕部的连结、手部关节的配合以及手部内部肌群的协调运作，从而共同完成各种复杂的操作任务和模式。

尽管早期的研究详细的描述了鼠标交互操作的生物力学运动结构和过程，但是并没有指明鼠标交互操作能否作为一种生物行为特征适用于生物识别的目的。

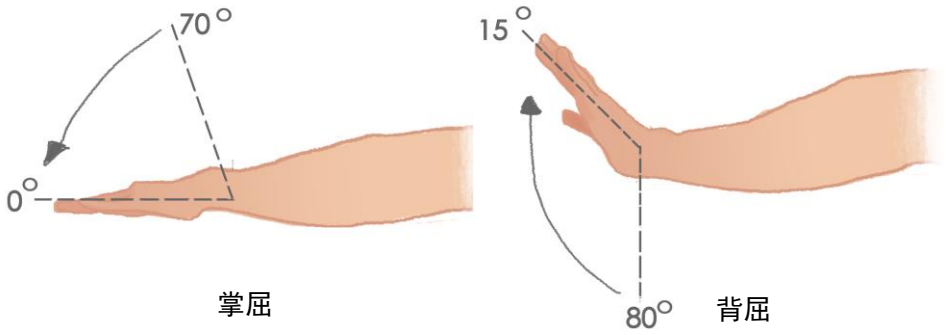


图 2-3 掌屈和背屈

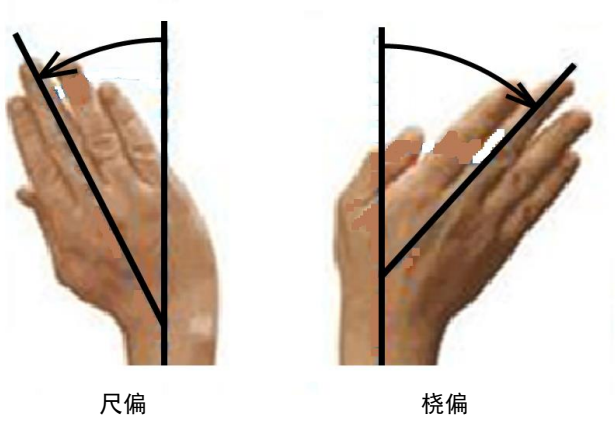


图 2-4 尺偏和桡偏

2.4.2 人机交互领域中鼠标交互行为分析

人机交互领域中鼠标交互行为分析[90,91]是一个旨在提供快速和精确的鼠标交互定位的研究领域，它可以提供建模人体上肢在快速定位运动（如用户移动鼠标的过程）的线索，有助于利用运动模型来分析指点运动过程，从而为工效学设计中鼠标交互定位操作绩效提供重要参考材料，同时设计简洁易用的人机交互模式。

鼠标交互定位操作绩效研究是从客观方面考察鼠标装置定位操作的可用性。绩效指标常包括鼠标定位操作的速度，正确率和有效难度指数与指点定位运动时间的比值[92]。有研究者发现影响鼠标定位操作绩效的 GUI 因素主要有指点目标的大小、距离和方向等。1954 年 Fitts 用铁笔移动方式研究手定位运动，发现手定位运动所需时间随目标距离增大而增长，随目标宽度增加而缩短[93]。然而在 1978 年，Card 等人[94]发现：被试用的 4 种输入装置（鼠标，操纵杆，步键和文本键）在 5 种目标距离（1cm，2cm，4cm，8cm，16cm）和 4 种目标宽度（1，2，4，10 个字符）组合下进行计算机文本选择任务时，输入装置的移动时间随距离的增加而增长，随目标宽度的增加而缩短。距离对错误率影响较小，但目标宽度对错误率有显著影响。尽管菲茨定律对指点定位时间有良好的预测性，但在界面设计中，一味地增加图符、按钮或菜单选项宽度来获得高用户绩效一来受到特定界面空间的限制，二来这种做法也并不经济。许多研究者对目标方向因素做过相关探讨，但研究结果不一。如 Card[94]，Kotani 和 Horii[95]研究了右

上 90 度扇区内的目标方向对鼠标移动时间的影响，结果发现不存在目标方向主效应。而另一些研究者却发现目标方向明显影响了鼠标的移动时间。如 Boritz[96]研究了饼式菜单中的项目选择，发现水平向右的鼠标运动比垂直向下运动更快；Whisenand 和 Emuriand[97]研究了鼠标向 8 个方向(水平、垂直和对角线方向)的运动，发现水平方向的鼠标运动最快，最慢的是垂直方向，对角线方向介于两者之间。导致以上研究结果不一致的原因可能是研究者采用的实验范式、鼠标运动的范围不完全一样。实际上，目标方向对指点装置定位运动的效应受操作肢体的解剖和生物力学特点，任务的操作特点和精度要求以及装置的操作特点及性能等多种因素的影响 。此外，Thompson 等人[98]认为在考察指点装置定位操作的可用性时，应该将控制显示比考虑在内，因为它是改变任务难度的一个参数 。

人机交互领域的研究提供了鼠标交互行为的物理运动模型，确信了鼠标交互行为可用于身份识别的观点。尽管人们同意可以采用菲茨定律、席克定律、转向定律等能够较为准确的描述鼠标交互行为的运动过程，但是仍然没有一致的看法来解释如何利用该运动模型进行身份验证。

2.4.3 计算机安全领域的鼠标交互行为分析

基于鼠标交互行为的身份安全认证和监控是通过分析计算机用户的鼠标动力学行为特征，分析用户的鼠标行为模式，对鼠标操作行为进行建模，并以此为依据来进行用户身份有效性的验证。鼠标行为安全是一个全新的研究课题，目前相关研究工作正处于起步阶段。文献中关于鼠标行为的身份认证和监控研究最早出现于 2003 年。此后，共有五个研究小组围绕鼠标行为进行了研究，在中小规模实验中证实了将鼠标行为作为身份验证手段的有效性[30,32,34,35,54,55,58-60,63,64,66-68,70,71,74,75,99-102]，实验环境下行为分类的准确率最高达到了 90%以上[32]。

Ahmed 和 Traore 在文献[30,31]中最早进行鼠标行为特征的研究，且于 2003 年 5 月申请了专利。他们对用户鼠标行为进行统计分析，实验结果表明在不同用户间这些统计量存在差异，并提出基于这些差异认证用户身份的初步方法。Pusara 和 Brodley 在文献[100]中对 18 个用户使用 IE 浏览器浏览相同网页时的鼠标行为数据进行了分析，研究了利用统计行为特征进行身份区分的可行性。Gamboa 和 Fred 等在文献[99]中研究了 50 个人在一种记忆力测试游戏中的鼠标行为，讨论了用预先设定的鼠标操作进行登录认证的可能性。Garg 等在文献[103]中提出了一种新的方法，通过参数化用户的动机、用户的技能等级、用户的应用、鼠标和键盘的活动来自动生成用户数据。他们的工作反映了使用鼠标行为数据对用户的身份进行监控想法，但并没有提出具体的方法。Jorgensen 等人[76]对基于鼠标行为的身份安全分析方法进行了回顾，讨论了鼠标行为身份安全分析不同的应用场景以及影响鼠标行为应用的因素。

前期的研究结果已经证实不同计算机用户之间的鼠标交互行为行为存在差异，可以用于用户的身份验证。但是，目前基于鼠标行为的身份验证准确率并不高，并且检测时间过长。文献[99]中进行身份认证要达到 90%以上的准确率需要使用 100 个“笔划”；

文献[32]进行身份监控要保证 95%以上的准确率，必须观察到 2000 次以上的鼠标操作，平均报警时间为 13.55 分钟，需要在检测性能和时间之间折衷。因此，如何提高身份验证准确率并保证较短的身份验证时间，是基于鼠标行为进行身份验证的关键。

2.4.4 鼠标行为分类

鼠标行为分类是鼠标行为认知的一个重要环节，它旨在区别计算机用户的鼠标点击、鼠标移动等交互行为。例如 Pusara 和 Brodley[100]从不同鼠标操作事件组合的角度利用树形结构对鼠标交互行为进行了分类，包括鼠标点击、鼠标一般移动、鼠标拖拽移动、鼠标点击移动等鼠标交互行为。

2.5 基于鼠标交互行为的身份安全认证和监控的研究概述

尽管基于鼠标交互行为的身份安全认证和监控是一个新的研究领域，但目前已经出现了许多研究机构从事这方面的研究，最有代表性的是加拿大维多利亚大学 Victoria①、美国卡内基梅隆大学 CMU②、北卡罗莱纳州立大学 NCSU③、威廉玛丽学院 WMU④等高校的研究工作。

表 2-1 当前基于鼠标交互行为的身份安全认证和监控研究中常用的特征类型

行为特征表达类型	典型的算法（Typical Publications）
行为统计特征	[30-32]
空间特征	[32,100]
速度特征	[32,63,100]
形态特征	[99]

当前的基于鼠标交互行为的身份安全认证和监控研究主要通过分析时空模式或运动变化过程得到鼠标交互行为特征，并以此特征为基础对用户的身份合法性进行判别。鼠标交互行为特征包含了两类重要的描述量：运动轨迹形态刻画量和时空模式动态刻画量。前者捕捉了鼠标运动轨迹的整体形态信息；后者捕捉了用户操作鼠标进行交互任务时的行为动态变化特性。目前文献中定义的鼠标交互行为特征可以细分为四类：1）行为统计特征，是指在一段时间内鼠标操作的统计分布特征，主要包括单击次数、双击次数、各种操作所占比例、移动速度和移动距离的分布等[30-32]；2）空间特征，是指鼠标运动过程中的空间坐标特性，主要包括鼠标光标位置、方向、距离等[32,100]；3）速度特征，是指鼠标运动过程中的时空变化特性，主要包括速度、加速度、角速度等[32,63,100]；4）形态特征，是指鼠标运动过程中的轨迹形态特性，主要包括曲率等[99]。文献中已证实上述鼠标交互行为特征可以反映出用户间鼠标行为的差异，具有一定的身

① http://www.uvic.ca/engineering/ece/isot/
② http://www.cs.cmu.edu/~maxion/
③ http://www4.ncsu.edu/~tyu/
④ http://www.cs.wm.edu/~hnw/

份可区分性。当前在基于鼠标交互行为的身份安全认证和监控研究中使用的不同行为特征表达类型如表 2-1 所示。

基于鼠标交互行为的身份安全认证和监控研究按照其应用场景可以分为两大类[76]：身份认证和身份监控。在身份认证过程中，用户使用鼠标完成一些预先设定的交互操作，分析这个过程中的鼠标行为，判断当前用户身份是否合法。身份监控对鼠标操作没有任何限制，在用户登录之后持续地记录并分析用户的鼠标行为，判断用户的身份是否发生了变化。当前的基于鼠标交互行为的身份安全检测研究按照不同的应用场景类型的划分如表 2-2 所示。

表 2-2 当前基于鼠标交互行为的身份安全认证和监控研究中的应用场景

应用场景	典型的算法（Typical Publications）
身份认证	[36,54,55,62-64,83,101]
身份监控	[31,32,34,70,78,86,100,102]

目前对鼠标动力学的研究大部分集中在身份监控[31,32,34,70,78,86,100,102]。例如文献[32]把鼠标行为分为 4 类：移动、拖拽、移动点击和静止，对鼠标行为的移动速度、移动方向、操作类型、移动距离、持续时间等物理量作了统计分析，分析了使用鼠标交互行为进行身份监控的可行性。文献[102]提取了鼠标移动轨迹的长度、弯曲度和直线性作为鼠标行为特征，得到了身份监控的平均错误率在 10.9%与 24.3%之间。文献[100]采集了用户使用 IE 浏览器 2 小时的鼠标行为数据，提取了鼠标移动的统计特征，使用决策树算法验证了基于统计行为特征对用户身份进行检测监控的可行性。

与身份监控不同，身份认证要求用户完成预先设定的操作，此时用户的鼠标行为表现得更有规律[36,54,55,62-64,83 ,101]。例如文献[99]设计了一种记忆力测试游戏，提取了鼠标移动的速度、加速度、角速度、曲率等特征量，用决策树分类算法进行身份认证实验。文献[55]设计了一个结合用户名密码和鼠标动力学的身份认证系统，该系统给用户显示一个虚拟键盘，要求用户使用鼠标输入用户名和验证码，使用文献[99]定义的“笔划”，对用户的身份进行认证。文献[64]设计了一个迷宫实验，用户操作鼠标从起点移动到终点完成一次实验。该文献提取了鼠标移动的水平速度和垂直速度，使用编辑距离比较不同用户的速度差异。

为了更加直观和便于讨论，我们将根据鼠标交互行为特征分析方法和应用场景对当前的研究细化为不同子类（注意：有些方法在下面的分类框架下可能会有所重叠）。

2.5.1 基于鼠标运动过程统计特性的方法

基于运动轨迹统计形态特性的方法[78,83,100,102,104,105]旨在将鼠标交互过程中的操作信息进行统计分析，利用操作信息的统计量作为用户的身份模型。它通常需要观察较长一段时间的鼠标交互过程以从中获得操作行为的统计量，将得到的统计量与已建立的用户身份模型进行匹配，来判断用户的身份合法性。

例如，Hocquet 等人的工作[104]提取了鼠标移动信息的描述性统计量来对用户的身份进行建模，包络移动距离统计量、时间统计量、速度统计量等。他们在预先设定的游戏场景中捕获了鼠标行为数据，并建立了该场景下的身份识别模型。基于论文所提出的描述性统计量，获得了 37.5%的错误率。

Schulz 等人的工作[102]将鼠标交互行为分割为多条鼠标移动曲线，并根据移动长度、移动曲率、移动曲线变化率对这些移动曲线进行划分。在不同划分的类别中，生成相应的统计直方图，将统计直方图的刻画量作为描述用户身份模型的参量进行身份建模。在实验环境下，他们收集了 72 用户的行为数据，并在此基础上进行了身份验证的实验，得到了 16.6%的错误率。

另一个有代表性的工作是由 Pusara 和 Brodley[100]完成的。他们采用了滑动窗口的方法对鼠标交互行为进行切分，分割出指点窗口大小的鼠标行为数据。对窗口内的行为数据，提取了频数、角度、距离和速度等平均量来形成用户的身份模板参量。在 18 个用户的实验数据基础上，该方法得到了 3.06%的错误拒绝率和 27.5%的错误识别率。

Zheng 等人的工作[78]提取监控模式下的鼠标运动轨迹的角度信息参量，包括移动轨迹方向、轨迹曲率角度、轨迹曲率距离。对长时间交互下的鼠标交互行为提取上述角度信息参量，拟合形成统计分布近似曲线，采样统计分布曲线中的 100 个数据点建立用户的身份模型。实在结果表明该方法能够达到 1.3%的检测错误率。

近来 Sayed 等人[83]提取用户使用鼠标进行签名的统计量建立用户的身份模型。他们采用的统计量均为平均测量量，包括坐标、速度、距离和曲率。在采集了 39 个用户的基础上，该方法的得到了 5.26%的错误拒绝率和 4.59%的错误接受率。

这类方法的优点是身份模型的建立较为直观，并且能能够提取较为稳定的交互行为特征；缺点是需要长时间的观察且计算复杂度较高。

2.5.2 基于鼠标运动轨迹动态变化特性的方法

在基于鼠标交互行为的身份安全认证和监控中一个很直观的思想就是鼠标交互运动很大程度上依赖于时空轨迹的变化，包含了很多的动态变化的信息。这类方法[54,55,60,62-64,101,106]通常对鼠标交互行为的动态运动过程进行表示，从中获得行为的描述量并建立身份模型，以判断用户身份信息的合法性。

早期的工作将鼠标交互行为看成是一段段的移动曲线，并对每段移动曲线进行特征的提取。Gamboa 等人[55]研究了 50 个人在一种记忆力测试游戏中的鼠标行为，他们对用户的每段鼠标移动曲线的速度、加速度、角速度、曲率等特征量进行了统计分析，从每段移动中提取了 63 维特征形成身份特征向量。接着在高维特征空间中选择特征子集，利用概率的方法进行了身份认证实验，实验中发现基于 90 秒的用户鼠标数据，可以得到超出手写签名识别认证 4 倍的准确率，讨论了用规定鼠标操作进行登录认证的可能性。

Revett 等人的工作[62]提取了每段移动中的时间信息建立用户的身份模型。用户在一个预先设定好的图形界面下使用鼠标移动并且点击指定的图标，进行登录任务的模

拟。6 个用户的实验结果表明只利用移动时间信息的用户身份认证方法错误拒绝率为4%，错误识别率为 3.5%。

接着，Bour 和 Fullu 的工作[64]利用动态时间规整的方法对比了不同鼠标移动曲线之间的差异，并以此差异为依据对用户身份的合法性进行判别。用户被要求使用鼠标在一个迷宫的场景下进行 18 段移动，以轨迹曲线及轨迹速度曲线为身份模板建立用户的身份模型。28 个用户的实验结果表明该方法能够达到 26.8%的错误率。

近来，Aksari 等人和 Hashia 等人的工作[63,101]从一系列指定的鼠标移动中提取鼠标移动点的特征，包括速度、偏移量、角度、加速度等，再将这些点的特征进行组合形成对应移动段的特征描述量，从而建立身份认证模型。身份认证的实验结果表明利用移动点特征的身份认证结果为 5.9%的错误率。

总体来说，利用鼠标运动轨迹动态特征能够对鼠标交互行为过程进行细粒度的刻画，达到较好的身份检测准确率，同时可以在短时间内进行身份的认证或检测，具有较低的计算复杂度，但目前的研究仍是在小范围的实验环境中进行，且检测准确率不高。

2.5.3 身份认证

基于鼠标交互行为的身份认证一直都鲜有研究涉及，原因是身份认证过程中所要求的认证时间短，然而短时间内的鼠标行为会存在较大的波动性，因此如何从较短时间的鼠标交互行为中提取稳定且有效的身份信息是该研究的难题。它的目标是在用户身份认证或登录系统时，要求用户使用鼠标完成一些预先设定的操作，捕获并分析这个过程中的鼠标行为，提取相应的行为特征，并以此为依据判断当前用户身份的合法性。

Hashia等人[101]和Bours等人[64]针对对鼠标交互行为进行身份认证进行了一些初步的研究。他们要求用户在进行身份认证时完成固定的鼠标操作序列，提取这些操作序列中的移动行为刻画量对用户的身份进行认证。他们采用了基于距离的分类器将测试数据特征同身份注册时的数据特征进行比较得到最后的认证结果。Hashia等人在15个用户的实验数据上得到了15%的错误认证率，而Bours等人在28个用户的实验数据上得到了28%的错误认证率。

接着，Gamboa等人的工作[55]提出了一种基于鼠标行为的网页认证模式。在用户认证时，所开发的原型系统在网页中显示一个虚拟的键盘，并要求用户使用鼠标点击该虚拟键盘键入用户名和密码。从鼠标的移动中提取相关的特征，同时使用贪婪搜索的算法进行特征选择。然后基于Weibull分布建立用户的正常身份模型。在50个用户的数据上，研究者们得到了6.2%的错误认证率，但没有报道认证时间的长短。此外，该研究在特征选择的过程中使用了用户的测试数据，这可能会导致对结果估计的过拟合问题。

Revett等人[62]提出了一种新型的认证框架，该框架要求用户操作鼠标完成一个类似加锁的人机交互界面。包含6个用户的小范围实验得到了3.5%的错误识别率和4%的错

误拒绝率。需要注意的是，本研究中的实验细节和实验流程并没有详细的说明。

近来，Aksari等人[63]呈现了一种基于固定序列的鼠标移动的身份认证系统。该系统在身份认证环节让用户依次完成7次鼠标移动，并从中提出移动相关的特征，例如移动时间、距离、速度等。基于欧式距离的方法构建了行为分类器，实验共采集了10个用户的交互行为数据。实验结果表明该系统可达到5.9%的错误认证率，但认证时间并没有在文中阐明。

从这些研究结果我们可以看出，当前的实验都是在小范围的数据上完成的，例如文献[58,62]中采集了6个用户的数据，文献[63]采集了10个用户的数据，这个规模的实验并不足够验证鼠标交互行为在身份认证场景下的可区分性，因此更大规模和进一步的深入分析需要进行来验证该方法和技术的可行性及可适用性。

2.5.4 身份监控

基于鼠标交互行为的身份监控是目前鼠标交互行为安全的研究热点，这是因为鼠标能够在用户成功登录系统后持续性的进行交互，从而具有进行身份监控和主动认证的潜力[31,32,34,70,78,86,99,100,102]。它的主要优势在于对鼠标交互行为没有任何限制，可以在用户正常使用计算机的过程中对用户身份进行检测。

在早期的研究工作中，Pusara和Brodley[100]提出了一种基于鼠标交互行为的用户身份再认证方法。鼠标交互数据被分割为一系列固定时间窗口下的鼠标交互事件。针对固定长度的鼠标数据块，该研究利用统计的特征分析方法，对鼠标移动情况和鼠标事件进行了量化得到行为特征，再用决策树算法研究这些统计特征对不同用户的可分性。在11个用户的实验结果下表明，当窗口包含3000个以上的鼠标操作时，可以得到0.43%的错误识别率和1.75%的错误拒绝率。但完成3000个鼠标操作一般情况下需要30分钟左右的时间，且11用户的样本数量比较小。

接下来，Gamboa和Fred[99]首次提出了利用鼠标交互行为进行实时的身份检测。在他们的研究中，鼠标移动被分割成为一条条的移动曲线，并且从不同的曲线中提取移动曲线的速度、加速度、角速度、曲率等特征量，进行统计分析以形成高维的特征空间。在高维特征空间中选择特征子集，利用概率的方法构建了身份认证模型。实验中发现基于90秒的鼠标交互行为数据，在50个用户的实验上可以得到2%的错误检测率，同时讨论了用规定鼠标操作进行登录认证的可能性。但该研究的特征选择过程中利用了身份测试的数据，可能会导致结果的过优化。

Ahmed 和 Traore[31,32]等人针对鼠标交互行为在身份监控的应用进行了深入的分析，并得到一些很有意义的发现。他们将低层次的鼠标行为事件（例如鼠标点击的按下和弹起及鼠标的移动）组合成为高层次的鼠标操作（例如鼠标的点击移动）。接着针对这些高层次的鼠标操作，提取了行为刻画量，如鼠标移动速度、鼠标移动的距离、单击次数、双击次数，并对这些量之间的关系进行统计分析。在 26 个用户的实验数据的基础上，结果表明在不同用户间，这些统计量存在显著差异，并提出基于这些差异来进行用户身份认证的方法，在 17.22 分钟的观测时间内可获得 2.46%的错误检测率。

Schulz[102]提出了一种基于行为时间流分割的鼠标行为监控方法。该研究将鼠标操作事件根据不同的属性进行划分，得到不同长度、曲率、曲率变化率下的鼠标移动曲线。计算不同划分下的统计特性，形成相应的统计直方图作为鼠标行为的身份模板。然后建立基于距离的身份检测模型，72个用户的实验结果表明，该方法能够达到24.3%的检测错误率。

近来，Zheng等人[78]提出了基于细粒度的鼠标轨迹角度信息的身份监控方法。他们通过分析一定时间长度下的移动曲线的角度相关特征来表示行为的细粒度信息，并采用统计分析的方法提取角度相关特征的稳定分量。采用支持向量机建立了身份检测模型，30个用户的实验结果得到了1.37%的错误检测率，但其检测时间长达37.37分钟。此外，该研究还讨论了检测时间和检测错误率之间的关系。

上述的研究结果进一步证实了利用鼠标交互行为进行身份监控的可行性，但难点在于如何在较短的检测时间内提升检测结果。

2.5.5 身份隐私属性分析

基于鼠标（或人机）交互行为进行身份隐私属性的分析是一个全新的领域，目前国际上还没有其它研究小组进行该方法的可行性分析。我们小组在2013年[107]首次提出了利用人机交互行为进行计算机用户身份隐私属性的推测，包括性别、年龄、种族、左右手使用习惯等等。我们首先通过对捕获的人机交互行为进行分析，提取多模态的交互行为特征，并对这些特征进行建模，以对计算机操作者的交互行为进行全面的特征空间分析及准确的刻画。接着引入融合贝叶斯学习与随机森林学习框架，对身份隐私属性信息进行建模。最用采用多决策融合的方法以精确而有效的对计算机操作者的身份隐私属性进行识别。该研究收集了58名用户的鼠标行为数据及51名用户的击键行为数据，并根据此建立了标准的交互行为数据集。实验结果表明本研究提出的方法能够准确地对用户的身份隐私属性进行识别。当利用人机交互信息对用户身份隐私属性进行识别时，识别率均高于85%。当利用键盘交互数据对用户的种族信息进行识别时，相关的识别率为87.32%。该结果验证了在计算机取证分析的场景下，基于人机交互行为对计算机用户身份隐私属性进行识别和推测，并表明该方法能够对计算机网络犯罪提供一种高效且可靠的技术手段。

2.5.6 与其它生物行为特征的融合

针对于鼠标交互行为与其它生物行为特征的融合，国际上还鲜有报道。只有 Ahmed 和 Traore 在 2005 年[30]提出使用击键交互行为和鼠标交互行为融合的方法进行用户的身份监控和检测。

2.6 基于鼠标交互行为的身份安全认证和监控的研究难点

尽管目前已经涌现了一些基于鼠标交互行为的身份安全认证和监控方法，但这些工作更多地是出于探索性的研究目的。因此需要强调的是，鼠标交互行为的身份安全

研究仍处于起步阶段，这是因为：1）过去的工作通常是在无受限的实验环境下进行的，而鼠标交互行为作为一种人机交互行为会受到各种环境因素的影响，比如计算环境的软硬件配置，因此是否在鼠标交互行为中存在可区分的身份信息还需在受控环境下进一步的验证；2）目前算法的测试和评估都是在非通用的小样本数据库上进行的；3）即使在上述条件下，识别率还远没有达到它可能的上限。

从早期研究结果来看，研究鼠标交互行为中是否存在有区分性的身份信息、及在实际场景中开发和实现高度可靠与鲁棒的身份认证与监控系统是非常有挑战性的问题。这些挑战包括非结构化的行为表示、行为波动性的影响以及由于心情、操作环境或者是身体状态等所导致的鼠标行为变化等。在给定条件下，生物识别系统的性能不仅依赖于场景的条件特性，而且还依赖于采集的数据质量、识别算法能力、传感器性能、非协作的个体、数据库特性等许多因素。在复杂情况下，环境和技术上的挑战将剧烈增加。非常明显，鼠标交互行为安全的研究仍处于探索阶段，许多开放的问题，特别是下面三类问题，仍有待解决。

2.6.1 行为结构化表示

在生物行为特征识别的研究中，建立一个清晰的结构化表示或描述框架，对于分析提取精确的行为特征以及准确进行行为比较起着重要的作用[8]。在步态、语音、签名、击键识别或验证等方向的研究中，都存在或建立了较为清晰的行为描述结构。例如步态研究中，人的基本肢体结构和具有周期特征的行走过程为步态模型的建立和行为特征的提取奠定了基础[12]；在签名识别的研究中，文字的字形及组成结构为签名特征的描述和比较提供了基本框架[11]。

然而，当前鼠标行为验证的研究直接从整体上对行为建模、提取特征，没有充分考虑行为内部的结构因素[31,32,99,100,108]。这不仅导致行为模型的精度降低，而且身份验证的灵敏度也受到很大影响。例如文献[32]中的方法要保证 97%的准确率，一次行为采样必须包含 2000 次以上的鼠标操作，这相当于正常用户要完成约 20 分钟的鼠标行为验证才能登陆系统，或异常用户进入系统 20 分钟后才能被检测出来。过高的平均报警时间（Mean Time To Alarm，MTTA）严重的影响了现有方法的实用价值。

尽管鼠标行为缺乏整体性的结构，但存在大量可用的结构化信息，具体体现为：1) 在任务模式中，通常是依照固定的操作序列完成特定的任务（如 “弹出菜单”时“鼠标右键点击+移动+左键点击”的操作序列），这些操作序列蕴含着明确的语义关系。通过语义分析可以把任务结构提取出来；2) 对于不属于任务模式中的行为，绝大多数操作可以归属为某种典型的操作模式（如水平左移 vs. 垂直下移）。同种模式中的操作具有强的相似性，每种模式都可看作一个结构，通过序列模式挖掘的方法可以将这类结构提取出来。鼠标行为的结构化描述对精确的行为表达及行为匹配有着重要作用，能够大幅提高鼠标行为验证在实际应用中的精度。

2.6.2 行为特征的定义和提取

行为特征的定义和提取是生物行为特征识别中的重要环节[4-7]，其核心问题是如何在变化的行为中抽取出可以表示身份信息的稳定特征。目前鼠标行为认证的研究工作主要定义了三类特征：1) 统计特征，包括单击次数、双击次数、各种操作比例、移动速度/距离的分布等[31,32]； 2) 空间形态特征：位置、方向、距离[100]、曲率[99]； 3)速度特征，包括速度、加速度、角速度等[99,100]。在前期的研究工作中已证实上述行为特征可以反映出用户间鼠标行为的差异，可实现用户的身份验证。

当前鼠标行为特征研究中的主要问题是：操作级特征多，过程性特征少，缺少对光标轨迹动态形态细节的刻画。此外，当前研究中也没有充分考虑指点行为的不平稳性及波动性，缺少对行为特征稳定性的全面评价。本研究基于中长期鼠标行为数据对现有行为特征进行了研究[34]，发现文献报道的大部分行为特征在长期行为中都表现出了比较明显的波动性。

由以上分析可知，在鼠标行为特征的定义与提取方面，细粒度的行为特征，特别是运动轨迹细节特征的提取和表达还亟待深入研究，尤其运动轨迹分段描述与弹性匹配，特征的提取与评价在目前的鼠标行为验证中还未有研究，对其进行深入研究对于提高鼠标行为模型的准确性和完备性有重要意义。

2.6.3 行为分类器性能评估及改进

改进系统性能的评估方法，确定变化的数据集对于识别性能的影响，为了收集数据、设计试验而创建标准的协议等是最大的难点之一。当前，鼠标交互行为相关研究的局限是缺乏一个标准的鼠标交互行为评估数据库。另一个局限是缺乏个体内及个体之间的变化与试验条件一致、也与实际情况相一致的知识。因此，如何规范地创建一个较大规模的通用鼠标交互行为数据库非常关键。

1）行为分类器的构建和评估

行为分类器的构建与学习是生物行为特征识别研究中的重要环节，神经网络、支持向量机、贝叶斯分类器是在生物行为特征识别中被广泛使用的分类器[4-7]。神经网络是一种经典成熟的分类器；SVM 具有良好的推广能力，适合于仅有少量训练样本的情况；贝叶斯分类器能够将先验信息较好地纳入到识别框架中来。在已有的指点行为验证的研究中，以前馈多层神经网络[32]、决策树[100]、简单的条件概率模型[99]作为行为分类器，得到的身份认证或监控结果差异较大，甚至采用同一种分类器也会得到截然不同的检测结果。因此，对这些行为分类器进行基准化的评估，并根据评估结果确定适用于鼠标交互行为的分类器是提升检测结果的重要环节。

2）评估鼠标交互行为作为生物特征的潜力

从经验和初步的实验结果中，我们知道能够根据人的计算机使用习惯和方式来对用户进行区分。这提出了“鼠标交互行为是否在人之间是充分可区别的”问题。鼠标交互行为安全刚刚起步，研究者们正开发技术来验证鼠标交互行为所具有的能力。尽管

早期的鼠标交互行为研究展现了令人鼓舞的结果，然而人的鼠标操作模式，不像指纹和虹膜，未必对于个体而言是唯一的。因此，人们需要进一步确认人能够通过鼠标交互行为进行身份验证的观念确实成立。正如上所述，当前鼠标交互行为作为特征的局限是合适的评估数据库的缺乏及个体内与个体间的变化对于实际条件下因素的一致性知识的缺乏。因此，进一步评估鼠标交互行为作为生物特征的潜力是非常重要的。

3）提高评估数据库的质量和规模

在身份验证领域，数据库的质量和规模是两个非常重要的因素。创建用于开发目的、具有一定规模的通用数据库和标准测试协议必将有益于身份验证算法的开发和评估。当然最好能够拥有一个独立的用于测试目的的数据库，那样才更具说服力。任何数据库都必须控制影响鼠标交互行为的因素变化，这些变化可能是计算环境、身体状态及心理状态等。而且数据相对于可控环境下之外，应当采集在实际应用场景下交互行为数据库。只有那样的数据库（更多的人数和条件变化数等）才允许我们对获取的鼠标交互行为的局限性有所开发。本研究正致力于创建一个标准的数据集来度量或确定影响性能的因素。

总之，高级性能评估方法应当能够：a）确定生物特征的基本局限性；b）确定变化的数据集对于性能的影响；c）创建标准的协议用于收集数据、评估系统及设计实验：d）科学地识别影响性能的关键因素。

2.7 结论

缺少适合于现有计算环境的有效身份安全分析手段是造成目前信息系统中身份安全问题日益严重的重要原因。口令、身份卡、指纹等身份验证方式，通常要求额外的硬件设备或难以持续性的对用户身份进行分析，而人机交互行为无需记忆或携带，难以被窃取，不需要额外的硬件，且可无缝融入用户与计算机的交互过程，实现无干扰的全程身份安全分析。

鼠标交互行为一种典型的人机交互行为。基于鼠标交互行为的身份安全分析是个新兴的研究领域，它利用计算机用户操作鼠标时所展现的人机交互行为特征进行身份安全的分析。尽管目前鼠标行为验证的研究工作取得了一定的进展，但要使之成为一种真正实用的身份验证方法仍具有很大的挑战性。针对现状分析中讨论的问题，将深入研究鼠标交互行为的表示、行为特征的提取与评价及分类器学习与性能评估三个问题，并深入探讨身份认证、身份监控及身份隐私分析的应用。这些问题与生物行为特征识别、模式识别和机器学习等相关领域中的多个重要科学问题密切相关，它们的解决将有助于鼠标交互行为验证在极大程度上突破目前的进展，并推动相关领域研究的发展，为解决日益复杂的网络信息系统中身份安全问题提供理论依据和技术支持。

3 鼠标交互行为输入特性研究及数据集建立

在图形交互环境中，用户通过对人机交互设备进行操作，来实现对计算机的控制，完成各种指令输入。应用计算机用户鼠标行为进行身份认证，首先就需要获取计算机用户鼠标操作的原始数据。原始数据的采集十分关键，数据的精确度直接影响所提取的特征准确性乃至整个系统的精度。

本章首先对 Windows 环境下鼠标交互行为输入特性进行了分析，定义了基本的鼠标事件信息。然后分析三种鼠标数据采集技术（消息钩子、原始输入、过滤驱动）的基本原理，开发了三种数据采集技术下的采集软件。接着从理论和实验上对比这三种技术的差异。接下来，从获得的鼠标事件信息中定义并分割出鼠标行为操作。最后建立了本领域首个鼠标交互行为数据集。

3.1 鼠标交互行为输入原理

Windows 操作系统是目前使用最为广泛的图形用户操作界面，本文以 Windows 系统下的图形用户操作界面为例研究和分析鼠标交互行为的输入特性。当用户使用鼠标进行操作时，操作系统会不断地检测鼠标输入设备的运行状态，对计算机用户的鼠标输入行为进行响应。

在大多数多用户操作系统中，应用程序与操作系统本身是隔离的。操作系统内核代码运行在处理器的特权模式下，称为内核模式，可以访问系统数据和硬件；应用程序代码运行在处理器的非特权模式下，称为用户模式，只能使用有限的一组接口，对系统数据的访问受到限制，无法直接访问硬件[109]。一个简化版本的总体结构如所图 3-1 示。

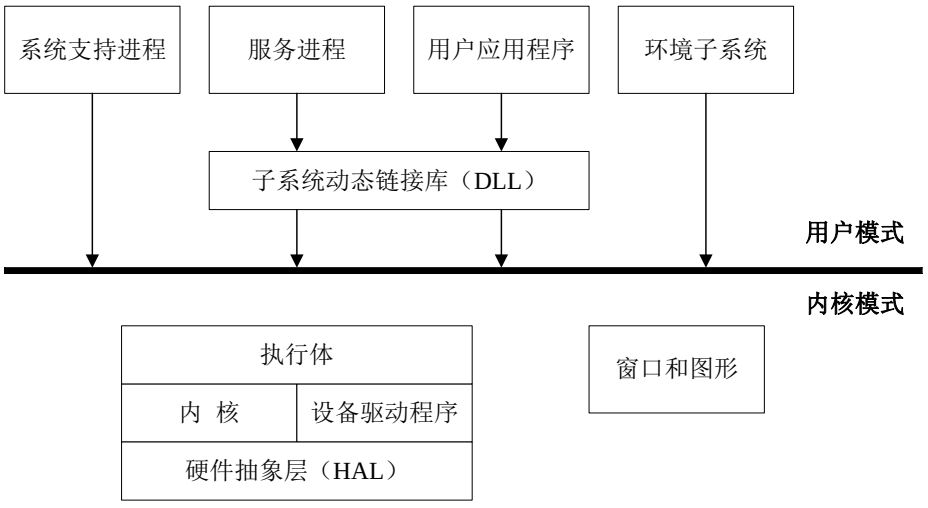


图 3-1 简化的 Windows 结构图[109]

在图 3-1 中，中间一条粗线将 Windows 操作系统的用户模式和内核模式划分开来。用户应用程序不直接调用原始的 Windows 操作系统服务，它们通过一个或多个子系统动态链接库来发起调用。子系统 DLL 的角色是，将一个文档化的函数转化为一些恰当的内部 Windows 系统服务调用。硬件抽象层是指一层特殊的代码，它把内核、设备驱动程序和 Windows 执行体的其余部分，跟与平台相关的硬件差异隔离开来。

客户端/服务器运行时子系统（Client/Server Runtime Subsystem），即 csrss.exe，是微软 Windows NT 操作系统的一个内核组件，它是 Win32 子系统的用户模式端。csrss.exe 进程有一个原始输入线程（Raw Input Thread, RIT），这个线程负责处理所有的硬件输入，比如鼠标输入、键盘输入、触摸板输入等。此外，系统维护一个全局的消息队列，称为系统硬件输入队列（System Hardware Input Queue, SHIQ），用于存储系统中硬件触发的消息。RIT 和 SHIQ 构成硬件输入模型的核心[110,111]，如图 3-2 所示。

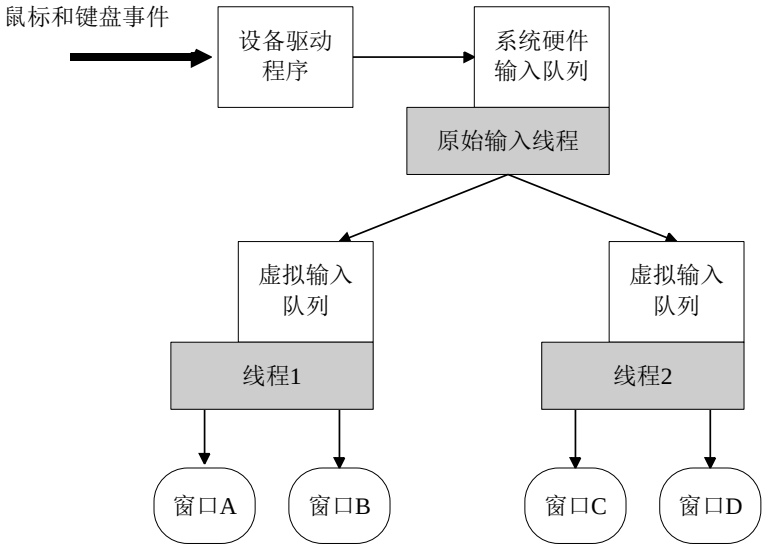


图 3-2 Windows 系统硬件输入模型

RIT 向鼠标驱动发送一个读请求要求读取数据，通常鼠标驱动不会满足这个请求，RIT 处于等待状态。当用户按下和放开一个鼠标按钮或者移动鼠标的时候，将触发鼠标的中断，引起中断服务例程的执行，中断服务例程由鼠标驱动提供。鼠标驱动读入输入数据并向 SHIQ 增加一个鼠标事件，这将唤醒 RIT。RIT 从 SHIQ 中提取这个项，并转换成适当的 WM_BUTTON 或 WM_MOUSEMOVE 消息，再把转换成的消息添加到目标窗口所属线程的虚拟输入队列（Virtualized-input Queue, VIQ）。线程依次从 VIQ 中取消息并将其回传给操作系统，由操作系统调用窗口过程响应消息。RIT 处理完一个消息后再循环等待更多的消息出现在 SHIQ 中[110,111] 。

简单地说，RIT 总是要求读入数据，然后等待鼠标事件到来。当鼠标移动或点击的时候，鼠标驱动读入输入数据并向 SHIQ 增加一个鼠标事件。RIT 处理 SHIQ 中的消息，然后继续要求读入数据，等待鼠标事件的到来。

鼠标事件进入系统最终被应用程序响应，经过了多次信息转换和传递。鼠标事件

首先被驱动程序获取，然后这个事件被添加到 SHIQ 中，接下来被转换成消息添加到线程的 VIQ 中，最后传递给窗口过程。在这个过程中我们可以从不同的截获点截获鼠标事件。如图 3-3 所示。

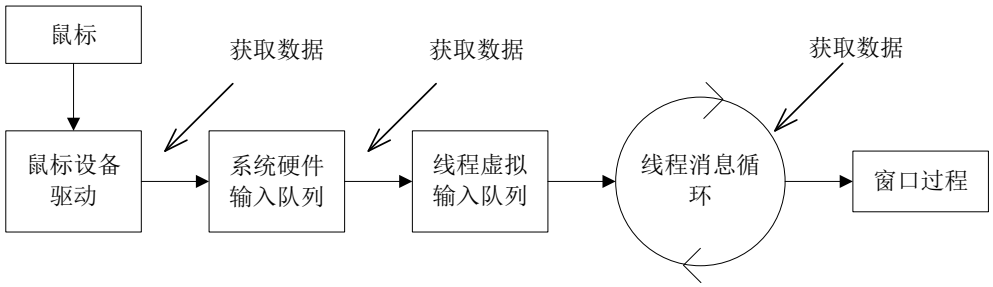


图 3-3 从不同的截获点获取鼠标数据

3.2 鼠标交互行为数据截获

根据鼠标交互行为的输入原理，可以从鼠标输入事件在 Windows 系统中传递的不同位置进行原始数据采集。本文从图 3-3 所示的三种不同位置下实现了相应的数据截获技术：第一种技术是鼠标消息钩子技术（Message Hook），在鼠标事件被 RIT 发送到相应线程的消息队列后，在线程获取到鼠标消息之前对数据进行截获；第二种技术是鼠标原始输入（WM_INPUT）技术，原始输入模型和传统的输入模型不同，应用程序向系统注册设备，表明它希望从这个设备获取输入，对应的设备有输入到来时，系统直接把从设备输入的数据传给应用程序；第三种技术是鼠标过滤驱动技术（Filter Driver），也就是在鼠标驱动之上编写自己的鼠标过滤驱动程序，拦截所有发往真实驱动的请求（IRP），获取 IRP 中的数据进行相应处理。下面详细叙述这三种技术的实现过程。

3.2.1 三种数据截获技术

1）基于消息钩子的鼠标交互数据获取技术

消息钩子(Message Hook)是 Windows 消息处理机制的一个平台，应用程序可以在上面设置子程序以监听指定窗口的某种消息，而且所监听的窗口可以是由其它进程所创建的。当消息到达后，在目标窗口处理函数之前处理它。消息钩子机制允许应用程序截获处理 window 消息或特定事件。

（1）鼠标消息钩子的基本原理

鼠标消息钩子加载在线程消息队列和鼠标所在窗口的消息传递路径中，截获所有由线程消息队列发来的鼠标消息，分析鼠标消息中的内容，获得当前鼠标输入行为数据。其原理图如图 3-4 所示。

每一个 Hook 都有一个与之相关联的指针列表，称之为钩子（Hook）链表，由系统来维护。这个列表的指针指向指定的、应用程序定义的、被 Hook 子程调用的回调函数，也就是该钩子的处理子程。当与指定的 Hook 类型关联的消息发生时，系统就把这

个消息传递到 Hook 子程。最近安装的钩子放在链的开始，而最早安装的钩子放在最后，也就是后加入的先获得控制权。

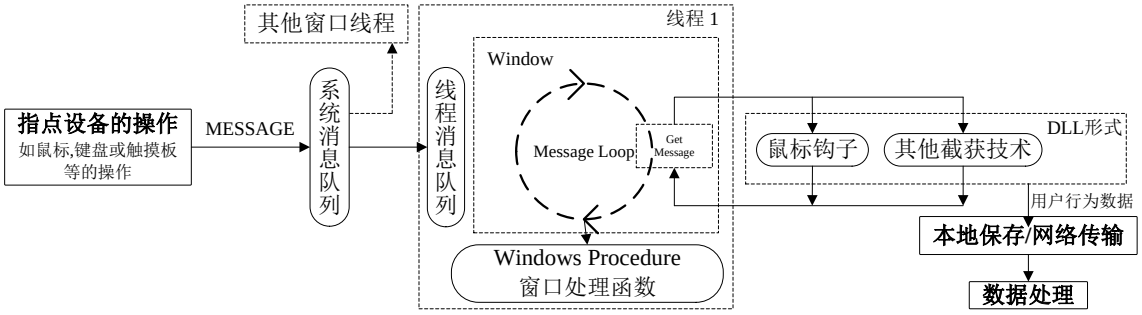


图 3-4 鼠标消息钩子原理[111]

（2）鼠标消息钩子的实现

安装鼠标钩子就是把一个自定义的钩子过程安装到鼠标钩子链表中，之后系统在把鼠标消息传给窗口过程之前先将它们交给钩子过程处理。

调用 SetWindowsHookEx 安装系统钩子监视系统中所有的鼠标消息。钩子函数置于独立的 DLL 中，系统会自动将这个 DLL 映射到受钩子函数影响的所有进程的地址空间。访问同一个 DLL 的各进程之间使用内存映射文件共享数据。

钩子函数获取的鼠标消息包括消息类型和一个 MOUSEHOOKSTRUCT 结构体。消息类型有按键按下或弹起、鼠标移动、滚动等。MOUSEHOOKSTRUCT 结构体的定义如下：

```
typedef struct {
    POINT       pt;             //光标在屏幕坐标系的 x、y 坐标
    HWND        hwnd;           //光标所在窗口的句柄
    UINT        wHitTestCode;   //光标在窗口的具体位置编码
    ULONG_PTR   dwExtraInfo;    //附加信息
} MOUSEHOOKSTRUCT, *PMOUSEHOOKSTRUCT;
```

POINT 类型的结构体表示了光标在屏幕坐标系的 x、y 坐标，光标在窗口的具体位置是指边框、菜单或其他位置。

```
typedef struct {
public   int    x;              //x 轴坐标
public   int    y;              //y 轴坐标
} POINT, *POINT;
```

本研究为了方便获取需要的鼠标原始数据，自定义了一个鼠标消息钩子内容结构体如下所示：

```
public class Mouse_Hook   {
public int x;                   //x轴坐标值
public int y;                   //y轴坐标值
public int messageCode;         //消息类型编码
```

```
public int timeStamp;          //时间戳
public String processName;   //进程名
public int flag;                  //鼠标消息有效信息
}
```

（3）鼠标消息钩子截获内容

本文使用全局鼠标消息钩子截获到的数据点信息包括鼠标消息类型和鼠标数据结构。鼠标消息类型描述了鼠标行为动作类型，如左键按下，右键弹起，滚动，移动等，在 Windows 中，鼠标消息分为两类：客户区鼠标消息和非客户区鼠标消息。具体编码如表 3-1 所示。

表 3-1 鼠标消息钩子消息类型编码

鼠标消息类型	客户区编码（十进制）	非客户区编码（十进制）
初始状态	512	160
移动或静止	512	160
单击按下（左/中/右）	513/516/519	161/164/167
单击弹起（左/中/右）	514/517/520	162/165/168
双击按下（左/中/右）	515/518/521	163/166/169
双击弹起（左/中/右）	514/517/520	162/165/168
中键滚动	522	522

2）基于原始输入的鼠标交互数据获取技术

（1）鼠标原始输入的基本原理

鼠标原始输入采用的是原始输入模型。原始输入模型及其相关的API可以比较容易的从输入设备中获取原始输入，包括鼠标和键盘。原始输入不隐藏原始输入的细节，同时支持Windows管理器不支持的HID设备。

原始输入模型不同于前面叙述的传统的 Windows 硬件输入模型：在原来的输入模型中，一个应用程序通过发送到它窗口的消息获取与设备无关的消息，例如 WM_CHAR,WM_MOUSEMOVE 和 WM_APPCOMMAND。在原始输入模型中，一个应用程序想获取原始数据，必须首先注册它想要获取原始输入的那些设备，应用程序会收到 WM_INPUT 消息。

（2）鼠标原始输入的实现

首先需要注册以获取设备的原始输入。默认情况下，没有应用程序会接受 WM_INPUT 消息。为了接受从一个设备发送原始输入，必须注册这个设备。为了注册这个设备，一个应用程序首先必须创建一个指明它所希望接受设备类别的 RAWINPUTDEVICE 结构。

接着读取原始输入。应用程序会收到符合所注册的设备的原始输入消息。当一个应用程序收到了原始输入，应用程序的消息队列就会得到一个 WM_INPUT 消息，系统

状态被设置为 QS_RAWINPUT。应用程序得到的 WM_INPUT 消息不仅包括鼠标信息，还有击键以及其他输入设备的信息。

最后需要释放注册的设备。需要设置一个包含 dwFlags 为 RIDEV_REMOVE，hwndTarget 为 0 的 RAWINPUTDEVICE 结构的 RAWINPUTDEVICE 类型数组，然后再用这个数组注册设备 RegisterRawInputDevices。

（3）鼠标原始输入截获内容

本文采集到的数据形式是 RAWINPUT 结构体，使用该技术采集鼠标输入数据时，它有一个指针成员指向 RAWMOUSE 结构体，这个结构体的定义如下：

```
typedef struct tagRAWMOUSE {
    USHORT usFlags;              //鼠标状态
    ULONG  ulButtons;            //保留字段
    USHORT usButtonFlags;        //鼠标按键的变换状态
    USHORT usButtonData;         //鼠标按键状态为滚动时，滚动增量
    USHORT ulRawButtons;         //鼠标按键的原始状态
    USHORT lLastX;               // x 方向的相对运动或绝对运动
    USHORT lLastY;               // y 方向的相对运动或绝对运动
    USHORT ulExtraInformation;   //设备附加信息
} RAWMOUSE, *PRAWMOUSE, *LPRAWMOUSE;
```

相比于鼠标消息钩子，鼠标原始输入的消息类型编码有所不同，如表 3-2所示：

表 3-2 鼠标原始输入消息类型编码

鼠标消息类型	十进制编码
左键按下	1
左键弹起	2
右键按下	4
右键弹起	8
中键按下	16
中键弹起	32
滚动	1024
静止	0

3）基于过滤驱动的鼠标交互数据获取技术

（1）鼠标原始输入的基本原理

由于即插即用（Plug and Play, PnP）设备的流动性和多样性，Windows 的 PnP 设备驱动一般是层次化和模块化的。一个物理设备的驱动任务，由几个驱动程序一层一层共同完成。同一类设备的公共部分放在上层驱动模块中，针对具体产品特殊性开发的代码放在下层驱动模块中。每层一个设备对象，它们联系在一起，组成一个设备栈。

鼠标驱动由上下两层构成。上层是鼠标的类驱动，实现了鼠标类驱动的.sys 模块是

mouclass.sys。要实现过滤，需要生成过滤设备对象插入到现有设备栈的合适位置。这样，系统发送给目标设备的请求，就会先发送到这个过滤设备。过滤设备处理完这个请求后继续下发给原来的设备，原来的功能不会受到影响。在一个设备栈中，端口设备的上方或类设备的上方或下方，都可以插入过滤设备对象。由于我们只需要获取鼠标输入数据，而不关心获取的是从 PS/2 鼠标还是从串行口鼠标输入的数据，因此将过滤设备对象插入到类设备的上方。

（2）鼠标原始输入的实现

本文首先生成鼠标过滤驱动的sys服务，然后使用vc++编写控制sys服务开启和卸载的应用程序，最后通过加载控制sys服务的应用程序dll，实现在系统要求的c#.net环境下采集鼠标过滤驱动原始数据。

一个驱动对象代表了一个驱动程序，或者说一个内核模块。设备对象是唯一可以接收请求的实体，任何一个“请求”（IRP）都是发送给某个设备对象，再交给设备对象的驱动对象处理，每个驱动对象生成多个设备对象。具体步骤为：1）创建鼠标过滤驱动对象；2）填写驱动对象的分发函数指针；3）找到所有的鼠标设备，驱动对象生成过滤设备并绑定；4）解除过滤驱动绑定。

（3）鼠标原始输入截获内容

本文获得的数据是 MOUSE_INPUT_DATA 结构体，这个结构体的定义如下：

```
typedef struct _MOUSE_INPUT_DATA {
    USHORT UnitId;                  //鼠标设备单元号
    USHORT Flags;                   //鼠标指示标识
    union {
        ULONG Buttons;              //ButtonFlags 和 ButtonData 的快速印象
        struct {
            USHORT ButtonFlags;     //鼠标按键的变换状态
            USHORT ButtonData;      //鼠标按键变换状态为滚动时，鼠标滚动数据
        };
    };
    ULONG RawButtons;               //鼠标按键的原始状态
    LONG LastX;                     // x 方向的相对运动或绝对运动
    LONG LastY;                     // y 方向的相对运动或绝对运动
    ULONG ExtraInformation;         //设备具体信息
} MOUSE_INPUT_DATA, *PMOUSE_INPUT_DATA;
```

鼠标过滤驱动的消息类型和鼠标原始输入的消息类型相同，如表 3-2 所示。

3.2.2 不同数据截获技术的对比分析

本文实现了上述的三种鼠标交互行为数据获取技术，并安装了三个鼠标数据采集器采集鼠标交互数据，对比分析它们获取的原始数据包含的时空信息，以选择出适合

于身份安全分析的采集技术。我们从数据的位移信息、时间精度、坐标范围及消息类型等方面进行了对比分析。表 3-3 是消息钩子得到的鼠标交互行为数据片段，表 3-4 是原始输入得到的鼠标交互行为数据片段，表 3-5 是过滤驱动得到的鼠标交互行为数据片段。这三个数据片段表示的是同一次鼠标左键双击。

表 3-3　消息钩子技术获取的鼠标左键双击数据

消息类型	x 坐标	y 坐标	时间戳/毫秒
512	631	521	4827104
513	631	521	4827288
514	631	521	4827352
515	631	521	4827424
514	631	521	4827520
512	631	521	4830928

表 3-4　原始输入技术获取的鼠标左键双击数据

按键的变换状态	x 方向的移动	y 方向的移动	时间戳/秒
0	0	1	1.90845070825884
1	0	0	2.06848726437319
2	0	0	2.13247253813637
1	0	0	2.2044540331824
2	0	0	2.30047851898882
0	0	1	5.70845743563182

表 3-5　过滤驱动技术获取的鼠标左键双击数据

标识位	按键的变换状态	滚动增量	x 方向的移动	y 方向的移动	时间戳/百纳秒
0	0	0	0	1	129166460612343750
0	1	0	0	0	129166460614062500
0	2	0	0	0	129166460614687500
0	1	0	0	0	129166460615312500
0	2	0	0	0	129166460616250000
0	0	0	0	1	129166460650468750

从这三个表中可以看出，消息钩子技术获取的光标位置是绝对坐标。原始输入和过滤驱动技术获取的光标位置是相对坐标。除此之外，这三种技术获取的数据在按键状态和时间信息上也存在差异，下面详细叙述。

1）位移信息

鼠标消息钩子采集到的原始数据位移是绝对位移；而鼠标原始输入和鼠标过滤驱动采集到的原始数据位移是相对于上一采集点的位移。

2）坐标范围

通过分析数据样本发现，鼠标消息钩子得到的鼠标数据点坐标对应光标在屏幕坐标系中的绝对坐标，取值范围和屏幕分辨率对应；而鼠标原始输入和鼠标过滤驱动得到的鼠标数据点坐标对应的是光标的物理位移，取值范围为0-65535。这个数值经过转换可以和屏幕坐标对应。

3）时间精度

鼠标消息钩子得到的鼠标消息结构中自带有时间戳信息（如MouseLLHookStruct定义），时间精度为毫秒，数据点采样时间间隔为15ms左右；鼠标原始输入和鼠标过滤驱动得到的鼠标消息结构中不包含时间戳信息（如RAWMOUSE 和 _MOUSE_INPUT_DATA定义）。为了获取数据点的时间戳，系统使用API函数获得时间信息。鼠标原始输入使用函数QueryPerformanceCounter获得计算机硬件高性能定时器的当前计数值，使用函数QueryPerformanceFrequency获得高性能定时器的时钟频率，两者相除得到时间戳，这个时间戳的时间精度可以达到纳秒甚至更高，数据点采样时间间隔为8ms左右。鼠标过滤驱动采用KeQuerySystemTime获取当前系统时间，这个时间的精度达到10微秒，数据点采样时间间隔为15ms左右。

4）原始输入和过滤驱动截获数据类似

通过观察原始数据样本，发现原始输入和过滤驱动采集到的原始数据点数目以及对应数据点的X、Y轴坐标和消息类型编码相同。但是，由于两种技术分别采用精度不同的API函数获取数据点的时间，所以原始输入和过滤驱动数据点时间戳信息不一样。

5）消息类型

鼠标原始输入和鼠标过滤驱动的双击事件由两次单击事件组成，消息类型也由两次单击消息类型组成；然而，鼠标消息钩子的双击事件由专门的消息类型编码，其第二次单击的消息类型编码不同于第一次。

6）按键状态

消息钩子获得的消息类型区分单击和双击，即双击的两次按下以不同的状态表示；而原始输入和过滤驱动没有专门的状态表示双击，双击的两次按下以同样的状态表示。消息钩子获得的滚动不区分方向，正向滚动和反向滚动都用 522 表示；而原始输入和过滤驱动以负值表示正向滚动（靠近用户方向），以正值表示反向滚动（远离用户方向）。

7）其他信息

鼠标消息钩子得到的还包括所在窗口信息，如窗口句柄、光标在窗口的具体位置等；鼠标原始输入和鼠标过滤驱动能获得和设备相关的其他信息。

基于以上的差异对比分析，本文选择消息钩子的方式进行鼠标行为交互数据的捕获。具体来说，鼠标消息钩子的优点如下：

- 消息钩子自带时间戳，更加准确地表示当前数据点的时间信息；原始输入和过滤驱动是在得到数据点之后采用 API 函数计算时间，不能准确地传递时间信息。
- 消息钩子得到的是数据点绝对位移，方便从原始数据中提取特征（如计算当前路

径等)；原始输入和过滤驱动得到的是相对位移，要想获取某些特征，必须首先在当前光标坐标的基础上不断累加相对位移得到绝对位移，这样降低了数据点坐标的准确性。

- 消息钩子只需通过消息类型编码就可以方便地判断双击事件；原始输入和过滤驱动必须判断两次连续单击之间的时间间隔来判断双击事件。
- 消息钩子类型很多，不光可以得到所有进程的鼠标操作原始数据，还可以获取某个特定进程的鼠标操作原始数据。
- 技术位于 Windows 用户应用层，实现简单，采集数据比较方便；原始输入和过滤驱动技术偏于 Windows 硬件层，技术实现和运行时出现问题的几率更大。

3.3 鼠标输入行为模式的研究

3.3.1 获取的输入行为数据

如前所述，本文在 Windows 图形环境中利用鼠标消息钩子技术采集鼠标输入行为数据，其格式为：鼠标动作，屏幕坐标，系统时间，进程信息等，如表 3-6 所示。实验中计算机用户使用的鼠标均为 Windows 操作系统标准的三键式鼠标。

表 3-6 鼠标输入行为记录信息

记录信息	鼠标动作	屏幕坐标	系统时间
数据项	基本事件类型编码	（横向 x 坐标，纵向 y 坐标）	系统时间/毫秒
示例	513	（312，508）	3418652

我们观察到的指点输入行为是由原始的指点设备事件组成的时间序列。例如下面的一段原始输入数据，代表了鼠标在编号为 1 的进程中，在屏幕坐标（823，808）处进行了一次左键单击（按下到弹起）的操作（利用消息钩子获得的鼠标操作对应的操作数值如所表 3-7 所示），按下和弹起的系统时间分别为 5818756 和 5818876。

```
状态     x 坐标   y 坐标   系统时间      进程信息
513,     823,     808,     5818756,      1
514,     823,     808,     5818876,      1
```

采集时记录的系统时间为计算机硬件的高精度计时器，单位为毫秒(ms)。

采集时记录的进程信息为鼠标事件所在的应用进程信息，如网页浏览（IE 浏览器），文字处理（Word），OS 文件管理（Windows Explorer Shell）等。

采集时记录的屏幕坐标为鼠标光标所在的屏幕位置坐标，以屏幕分辨率的像素（pixel）为单位。如果操作系统的分辨率为 1024×768，则屏幕坐标范围也从 (0, 0) 至 (1024, 768)，其中左上角为（0，0），如图 3-5 所示。

表 3-7 消息钩子下鼠标操作所对应的数值

动作	数值（十进制）	窗口的非客户区内数值（标题栏，边框等）
初始状态	512	
移动或静止	512	160
左键按下	513	161
左键放开	514	162
左键双击	515	163
右键按下	516	164
右键放开	517	165
右键双击	518	166
中键按下	519	167
中键放开	520	168
中键双击	521	169
中键滚动	522	

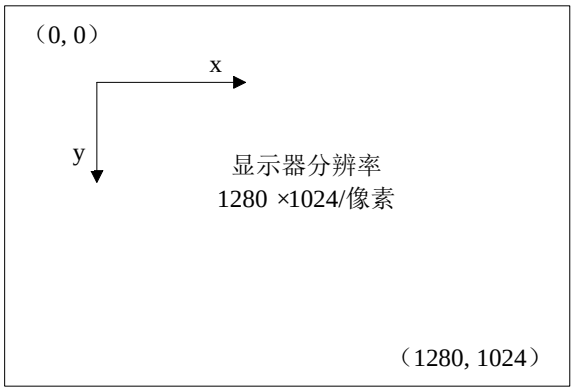


图 3-5 屏幕坐标示意图

3.3.2 用户输入行为模式的描述

本文将计算机用户的鼠标交互过程抽象为两个行为层次：

命令层：操作者控制鼠标，向操作系统或应用程序发出的一系列命令，如“光标定位”、“打开文件”、“执行程序”等；

操作层：操作者控制鼠标完成某个交互过程的逻辑步骤，如：首先移动光标到(x_1, y_1)附近，然后进行点击操作，其次移动光标到(x_2, y_2)附近，进行双击操作等；

本文研究用户输入行为模式是根据与应用程序相关的命令层行为，定义并分割出操作层的行为操作；进一步根据行为操作，定义并提取出用户在图形界面下人机交互的操作层特征，以及操作过程中所体现出的行为特征。

3.3.3 鼠标行为操作的定义与分割

1）鼠标行为操作的定义

根据对计算机用户使用指点输入设备与图形用户界面之间命令层交互行为的观察和研究，本文定义了以下的基本鼠标行为操作，包括

（1）单击操作（左/右/中键）Left/Right/Middle Click

鼠标左/右/中键一次按下到弹起的过程。如左键单击可能完成程序执行，文件图标选择等；右键单击可能完成图标选择，快捷菜单弹出等；

（2）双击操作（左/右/中键）Left/Right/Middle Double Click

鼠标左/右/中键连续两次完成按下到弹起的过程，其中第一次弹起和第二次按下的时间间隔小于操作系统中设定的阈值。如左键单击操作可能完成文件或程序的执行等。

（3）中键滚动操作 Middle Scroll

鼠标中键前后进行滚动的操作，如可以进行页面滚动浏览等操作。

（4）鼠标移动操作 Mouse Movement

光标从坐标(x_1, y_1)移动至坐标(x_2, y_2)处，随后进行点击等其他操作的过程。可以实现光标定位，完成后续动作，是主要的输入行为操作。

（5）鼠标拖拽操作（左/右/中键）Left/Right/Middle Drag and Drop

在按下鼠标左/右/中键的同时，将光标从坐标(x_1, y_1)移动至坐标(x_2, y_2)处，然后弹起按键的过程。如左键拖拽可以实现图标的移动，文本内容选择等操作；中键拖拽可以实现屏幕滚动操作。

（6）静止操作 Silence

鼠标未进行按键动作，光标停留在同一位置超过一定时间阈值的操作。

2）鼠标行为操作的分割

操作切分是指从原始的指点设备输入事件序列中分割出完整的有意义的操作层用户行为的过程。经过操作切分，我们把原始的设备输入事件序列，抽象为操作层中的用户操作序列。在切分过程中，不但要根据操作定义抽取完整的输入事件序列，而且要依据实际情况设定阈值，进行判断。下面列出了各类操作的分割判定条件，其中右键和中键的操作分割类似与左键。

（1）单击操作（左键）

对应鼠标事件编码序列为 513-(512)-514，操作分割判定条件为 514 后没有 515 出现（非双击操作），点击时间间隔小于一定阈值，坐标位移不变或小于一定阈值，

（2）双击操作（左键）

对应鼠标事件编码序列为 513-(512)-514-(512)-515-(512)-514，操作分割判定条件为点击时间间隔小于一定阈值。

（3）中键滚动操作

对应鼠标事件编码序列为 522-(512)-522，操作分割判定条件为连续 522 的间隔时间小于一定阈值，否则判断为一次新的滚动。

（4）鼠标移动操作

对应鼠标事件编码序列为 512-(512)-512-513 等。以某次点击或静止操作为起点，紧接着下一次的点击或静止操作为终点，分割判定条件为移动位移超过一定阈值，且移动过程中光标轨迹的方向在移动起点至终点方向的一定范围内连续变化，这样就可以切分出用户有意义的移动，过滤无目标的移动。

（5）鼠标拖拽操作（左/右/中键）

对应鼠标事件编码序列为 513-(512)-514，操作分割判定条件为左键按下到弹起的间隔时间和坐标位移均分别大于一定阈值。

（6）静止操作

对应鼠标事件编码序列为 512-…-512，操作分割判定条件为坐标位置保持不变，并且静止持续时间在一定范围内，如过小则可视为正常的操作间隔，过大则可能为用户离开等情况。

如经过操作分割后，下面的基本事件序列代表了一个完整的左键双击操作，总间隔时间为 328 毫秒。

513, 576, 372, 5724796, 1
512, 576, 372, 5724818, 1
514, 576, 372, 5724884, 1
512, 576, 372, 5724884, 1
515, 576, 372, 5724972, 1
514, 576, 372, 5725124, 1

图 3-6 描述了操作分割的状态转移过程。

3.4 鼠标交互行为数据库

由于基于鼠标交互行为的认证及监控研究起步不久，目前国际上还没有通用的鼠标交互行为数据集。因此，为了便于实验，我们创建了 XJTUMOUSE 鼠标交互行为数据库[①]。该数据库分别在身份认证和身份监控场景下采集了鼠标交互行为，并建立不同场景下的行为数据库。

3.4.1 身份认证场景下的数据库

在身份认证的场景下，本文设计了相应的固定模式。固定模式是指预先设定的用户行为模式，即在设计的图形交互环境下，在特定的时间之内，以特定的方式，完成特定的行为。采集的信息包括用户鼠标行为的 x 坐标、y 坐标、时间戳。固定模式包括压力测试，也可以说是负载测试，压力测试首先应该是较短时间的，其次是模拟巨大的工作负荷的，再次压力测试是要使用户操作行为达到峰值。身份认证场景下数据采集过程的详细说明见章节 4.3。

[①] http://nskeylab.xjtu.edu.cn/people/cshen/

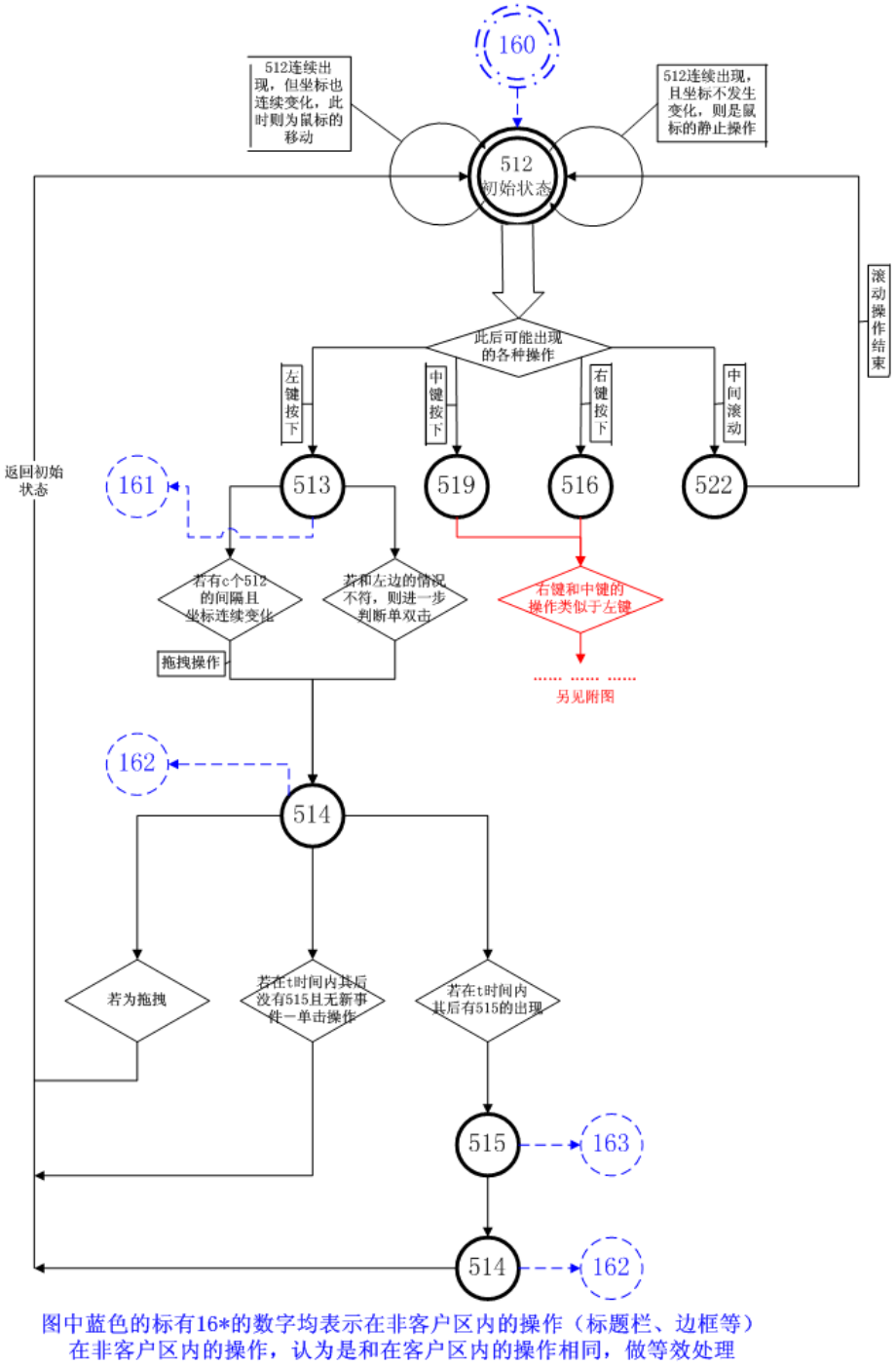


图 3-6 鼠标操作分割状态转移图

3.4.2 身份监控场景下的数据库

在身份监控的场景下，本文设计了相应的自由模式。自由模式下的鼠标行为数据采集采用基于消息钩子的数据采集技术，在用户个人计算机上将数据采集器安装为系统启动项，随计算机开机启动。采集用户在所有程序下的鼠标行为数据。采集的信息包括用户鼠标行为的 x 坐标、y 坐标、事件编号、时间戳、进程编号。而在进程编号上，将用户的进程按照场景分为几大类：网页浏览、文本编辑和其他类型。因为在相同类

型的场景下，用户往往有相似的鼠标行为模式。自然模式鼠标行为数据采集器在系统后台运行，不会影响用户的正常使用。另外，自然模式鼠标行为数据采集器采集用户在所有应用环境下的鼠标行为数据，采集的数据也最能体现用户鼠标行为的自然特征。身份监控场景下数据采集过程的详细说明将章节 6.3。

3.5 结论

本章首先介绍了 Windows 操作系统中鼠标输入的原理，分析了鼠标输入数据进入操作系统到最终被应用程序响应的过程，然后详细叙述了三种鼠标行为数据获取技术：消息钩子、原始输入和过滤驱动。从实现原理和时空信息对比分析了这三种技术的特点，选择了消息钩子技术进行数据的采集。随后将计算机用户操作指点设备与图形用户界面的交互过程抽象为命令层和操作层两个行为层次，研究用户输入行为模式，定义并实现了鼠标行为操作的分割。最后建立了不同应用场景下的鼠标交互行为数据集。

4 基于鼠标交互行为时空轨迹形态分析的身份认证

4.1 引言

针对人机交互行为的特征建模和认证问题，本章从鼠标交互行为的时空轨迹形态分析入手，提出了一种基于光标运动时空轨迹形态特征的身份认证方法。该方法解决了复杂人机交互过程的行为特征刻画问题，从鼠标交互行为的时空轨迹中捕捉轨迹形态变化的特征，获取的特征量间接体现了鼠标操作的习惯。在 XJTUMOUSE 数据库上的实验结果验证了算法的有效性。这在一定程度上也体现日常生活中遇到的一个普遍现象，即通常可以根据一个人的行为习惯来识别他的身份。

4.2 基本原理

鼠标交互行为特征不仅包含了光标操作的统计特性，而且包含了光标运动过程中轨迹的形态特性。理论上，光标操作过程中统计特性和轨迹形态的变化对于鼠标交互行为的身份信息是充分的。然而，如何从运动轨迹形态中提取出稳定的行为特征刻画量以进行身份信息的表示在模式识别和计算机安全研究中没有得到解决。经验上，鼠标交互行为的身份信息表示可以通过应用统计分析技术得到光标操作的频数信息来表示用户的身份信息，这些传统的技术不尝试匹配光标运动轨迹形态特性，而是通过对鼠标交互过程中光标操作统计描述量来表示用户的身份信息。因此，我们考虑将鼠标交互过程看作是光标轨迹的运动过程，由连续的光标轨迹运动所组成，通过分析它们的形态变化特性来获得可表示用户身份信息的特征向量。基于上述考虑，我们提出了一种基于鼠标交互行为时空轨迹形态分析的身份认证方法[36]。

图 4-1 给出了该方法的基本流程图。对于每个鼠标交互行为序列而言，提取描述鼠标交互行为时空轨迹形态特性的特征向量；利用距离度量和成分分析获取低维的特征量；引入单分类学习器构建身份认证和识别模型。实验结果表明该算法获得了令人鼓舞的认证和识别性能。

与过去大多数的算法不同，这个方法直接分析了鼠标交互行为的形态特性。它从时间和空间两个维度上分析运动轨迹形态的变化，得到描述运动轨迹形态特性的特征量，并用来表示用户的身份信息。也就是说，它本质上是描述性的，因为鼠标交互行为被间接地通过光标运动过程中轨迹形态变化所特征化。

4.3 认证模式

4.3.1 认证模式

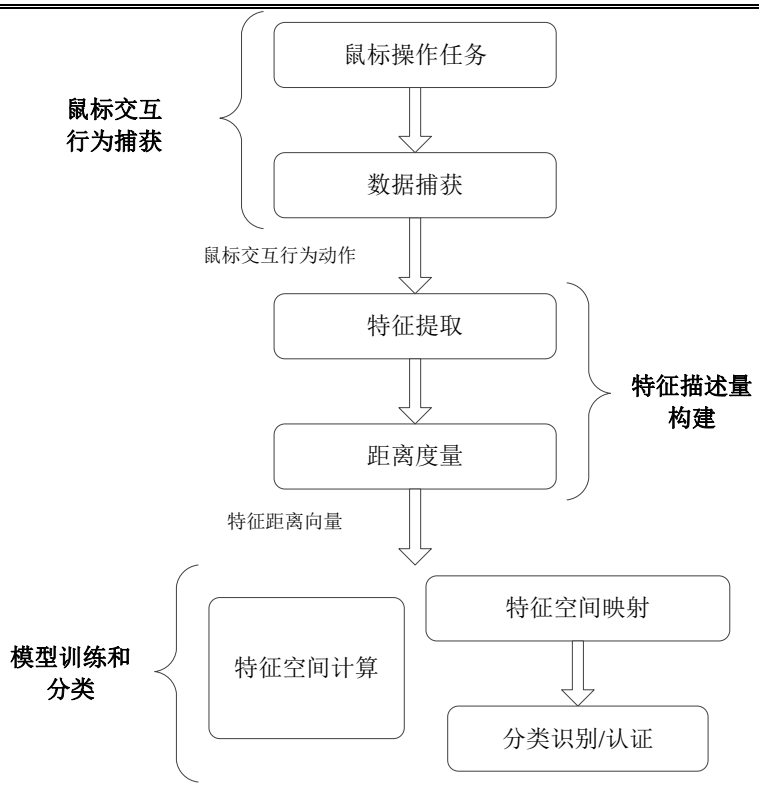


图 4-1 方法的基本流程图

和密码认证方式相似，基于鼠标交互行为的身份认证通常要求用户完成预先设定的鼠标交互操作模式。鼠标操作模式的设计需要考虑如下几个方面。首先，选择的操作是用户日常使用鼠标时经常出现的，以反应用户的习惯性操作。其次，模式中的操作不能太多，需要在用户可接受的范围内。此外，越多的操作意味着越长的认证交互时间，较少的操作次数可以减少用户认证时操作错误的几率。

本章设计了移动和点击相结合的操作模式。在一个矩形窗体上设置了 7 个固定位置，在这些位置依次出现方块提示用户单击或者双击。用户认证一次需要完成 16 次移动和 16 次点击，包括 8 次左键单击和 8 次左键双击。图 4-2 显示了该模式的数据采集环境，图中标出了前 8 次移动路径，后 8 次移动路径相同。

在这个模式中， 8 次移动代表了 8 个不同的移动方向（如图 4-3 所示），3 类不同的移动距离。表 4-1 显示了 8 次移动的方向和距离。4 条斜线与水平线之间的夹角是 45 °。

该操作模式的设计参考了文献[32,102]的研究结果，以及本文前期的实验分析。我们前期设计了几种不同的操作模式，通过大量的实验分析，发现该模式能够覆盖典型的日常鼠标操作，符合用户的操作习惯，具有一定的代表性。

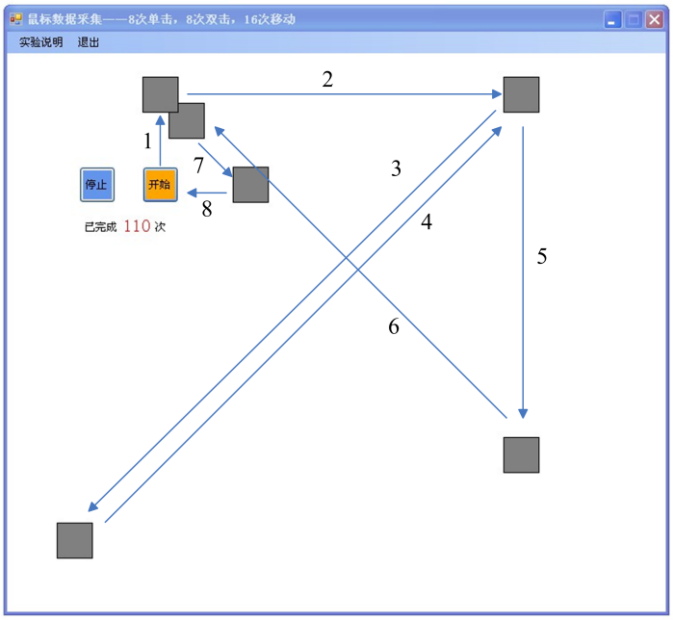


图 4-2　鼠标操作模式的前 8 次移动路径

表 4-1 鼠标操作模式中的移动方向和距离

移动编号	方向	距离/像素
1	竖直向上	100
2	水平向右	400
3	斜线向左下	700
4	斜线向右上	700
5	竖直向下	400
6	斜线向左上	524
7	斜线向右下	100
8	水平向左	100

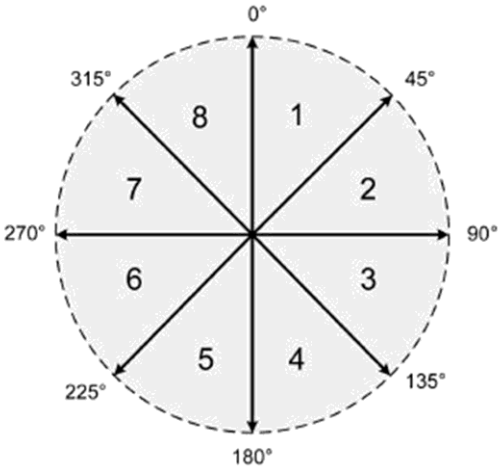


图 4-3　鼠标移动的 8 个方向[7]

从模式的设计和研究中我们可以得到如下结论：

1）不同用户在各方向上移动操作的出现比率不同，移动速度也各有差别，无法选定一个或者几个方向上的特征来区分用户。因此本文设计的模式包括了所有 8 个方向的移动。

2）若按距离把移动粗略地分为短距离移动、中距离移动和长距离移动，短距离移动出现的比率很高，但是不同用户的移动模式差别不大；长距离移动很少出现，但是不同用户的移动模式差别很大。中距离移动的出现比率和速度介于两者之间。因此本文设计的模式采用了 6 个短距离（100 像素），6 个中距离（400 像素和 524 像素）和 4 个长距离（700 像素）。

3）前期的实验使用顺序前进贪婪搜索算法在高维特征中选择最优特征组合，发现左键单击和双击时间间隔的均值对分类贡献最大。因此本文设计的操作模式包括了 8 次左键单击和 8 次左键双击。

4.3.2 参与用户

我们一共征集了 58 名用户参与了身份认证的实验，这些用户来自于西安交通大学智能网络与网络安全教育部重点实验室和西安交通大学其它的院系。58 名用户中有 46 名男性，12 名女性，每个用户都至少拥有 2 年的鼠标使用经验。

4.3.3 采集过程

所有的用户每天需要进行两轮的数据采集，并且等待至少 24 小时再进行下一次的数据采集，以确保时间序上的波动存在于数据中。在每一轮的采集中，所有的用户都被要求完成 10 次相同的鼠标认证模式。当一个用户第一次点击了屏幕上的开始按钮，然后依次移动鼠标点击由数据采集程序提示的按钮，直到最后的结束按钮，就完成了一次数据采集任务，记录下的鼠标行为数据就构成了一个鼠标操作样本。

用户被限制只使用鼠标这一种外接设备，键盘是不被建议使用的。如果用户需要休息或伸展他们的手臂，他们可以在完成一轮数据采集之后进行这些动作。这样的限制可以防止在一轮鼠标采集的过程中人为的数据干扰。用户必须将全部注意力集中在鼠标操作的任务中，就好像他们要登录到自己的账户上一样，避免在采集的过程中被分散注意力，比如与其他实验人员聊天。在操作过程中任意的错误（例如，当要求双击一个按钮的时候进行了单击操作）会要求用户重新开始相应的鼠标操作任务。

用户共花费 15 到 60 天左右完成鼠标数据采集。每个用户完成了 150 次无错的重复性的鼠标操作任务。一次数据采集大概要花费 6.2 秒到 21.3 秒，平均需要 11.8 秒。最后我们得到的数据集包含了 58 个用户总共 8700 组鼠标操作样本。

4.3.4 采集环境

采集环境的设定是固定的。包括

- 屏幕分辨率：1024×768；
- 鼠标参数（灵敏度、加速度、类型）

- 鼠标双击速度：Windows 默认设定（默认时间间隔 500ms，范围为 200-900ms）
- 移动：速度—windows 默认设定(Mouse Sensitivity=10，范围为 1-20)；
- 提高指针精确度—是（默认为选中此项，Mouse Speed=1，MouseThreshold1=6，MouseThreshold2=10）；
- 滚轮：一次滚动 3 行；
- 鼠标硬件：HP M-UAE96

在采集数据的过程中，所有实验人员需要在同一台电脑上使用同一个鼠标进行数据采集。这样可以在一定程度上减弱环境噪声对行为的干扰，以期在分析过程中将鼠标交互行为作为主要的因素。

4.4 特征提取

根据章节 3.4 所述的鼠标基本行为操作的定义和分割，可以在各种不同的操作或者操作的组合中提取出相应的鼠标行为特征，并对特征进行建模。

4.4.1 数据预处理

数据预处理的主要作用是去除冗余数据和无效数据，以及把原始数据转换成易于特征提取的形式。本章研究在数据预处理阶段完成了以下工作：去除冗余数据、剔除无效数据、分割移动和点击。

基于消息钩子的鼠标数据采集技术的时间精度为 8ms，则时间间隔小于 8ms 的两条消息类型编码相同的数据被认为是冗余数据，在处理的时候应剔除。原始数据中的移动和点击存放在一起，特征提取时需要将移动和点击分割开来，理想情况下应该分割出 16 次移动、8 次左键单击和 8 次左键双击。由于用户的误操作实际中可能切分出多于 16 次的移动和点击，这个原始数据就被认为是无效数据，会予以剔除。

经过数据预处理，原始数据序列 R 被分成了 18 个数据序列，记为 $S_i, i=1,2,...,18$。其中，$S_i, i=1,2,...,16$ 表示 16 次移动的数据，S_{17} 表示左键单击的数据，S_{18} 表示左键双击的数据：

$$S_i=\left\{(ncode_j, x_j, y_j, t_j, process_j)\right\},\quad j=1,2,...,J_i,\quad i=1,2,...,18 \qquad (4\text{-}1)$$

每个移动（$S_i, i=1,2,...,16$）的序列长度（以 $J_i, i=1,2,...,16$ 表示）通常有较大的差别，第一是由于移动距离不同，第二是由于移动速度不同。即使移动相同的距离，两次移动产生的数据量也有差别。在本章定义的认证模式下，一次移动的数据序列长度从十几到二百多不等。

4.4.2 鼠标行为特征的提取

以经过数据预处理的用户鼠标行为数据为基础，本章提取出的鼠标行为特征主要分为两类：行为轨迹曲线特征，即用户使用鼠标过程中所反映出光标运动轨迹的形态特性，如鼠标移动轨迹特性曲线等；行为轨迹统计特征，反映用户使用习惯的特性，

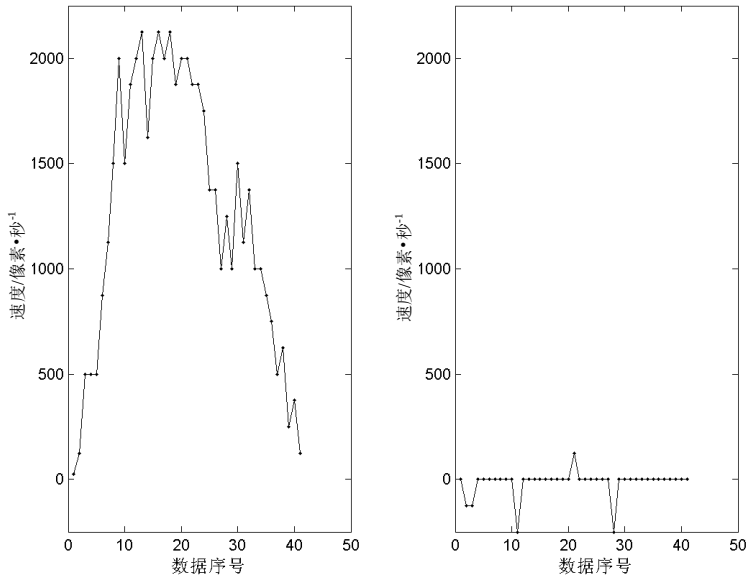
如用户经常进行哪些类型的操作。这些特征既包括基于统计的特征，也包括基于曲线的特征。

1）行为轨迹曲线特征

（1）移动速度曲线

本章计算移动速度的方法与其它文献不同。鼠标移动的轨迹通常不是直线，在移动方向和垂直移动方向都有位移。移动的瞬时速度方向并不总是和移动方向一致，有时甚至偏差很大。这里，我们将移动的瞬时速度v分解为移动方向的速度$v_{\parallel}$和垂直移动方向的速度$v_{\perp}$，考虑到$|v_{\parallel}| \gg |v_{\perp}|$，本文忽略$v_{\perp}$，仅计算$v_{\parallel}$。

考虑操作模式中的一次水平移动，如图 4-2 中的移动 2，鼠标移动过程中水平方向和垂直方向都有速度，如图 4-4 所示：



(a) 水平速度　　(b) 垂直速度

图 4-4 水平移动的水平和垂直速度曲线

注意到水平速度在数值上远大于垂直速度，并且垂直速度大多数情况下接近于 0。因此对于水平移动，只计算水平方向上的速度，第 j 个数据点的速度定义为：

$$v_j = \frac{x_j - x_{j-1}}{t_j - t_{j-1}}, \quad j = 2,3,...,J_2 \tag{4-2}$$

类似地，对于垂直移动，只计算垂直速度：

$$v_j = \frac{y_j - y_{j-1}}{t_j - t_{j-1}}, \quad j = 2,3,...,J_i, \quad i = 1,5,9,13 \tag{4-3}$$

本文的模式中还包含 8 次斜线方向的移动，计算这些移动的速度需要进行坐标变换，即将原先坐标系的水平方向旋转到该次鼠标移动的移动方向。坐标变换的示意图如图 4-5 所示：

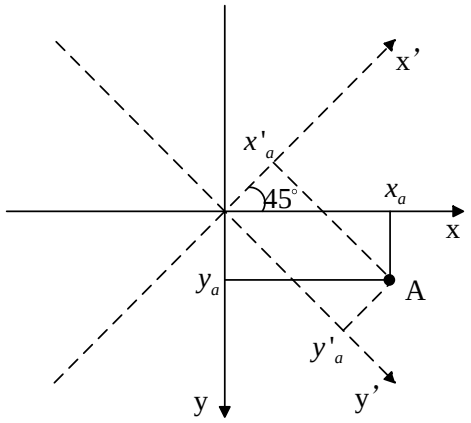
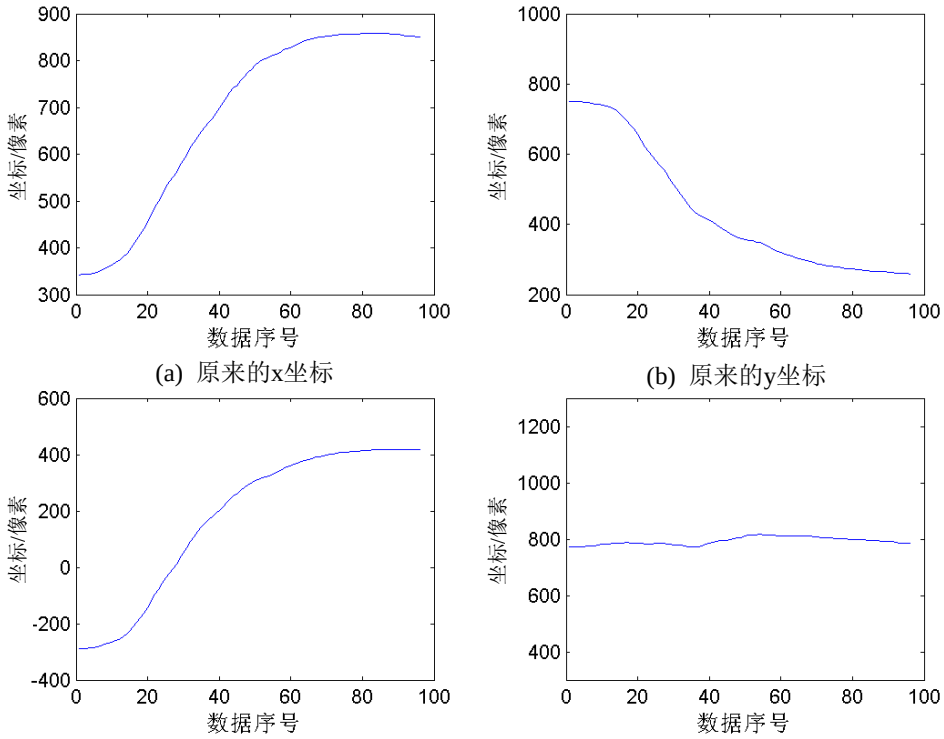


图 4-5　坐标变换示意图，点 A 的坐标(x_a, y_a)变换为(x'_a, y'_a)

将原来的屏幕坐标系逆时针旋转45°得到一个新的坐标系，比如点 A 在原来的坐标系中的坐标为(x_a, y_a)，在新坐标系中的坐标记为(x'_a, y'_a)，(x'_a, y'_a)和(x_a, y_a)的关系由下面的公式确定：

$$\begin{cases} x'_a = \dfrac{x_a - y_a}{\sqrt{2}} \\ y'_a = \dfrac{x_a + y_a}{\sqrt{2}} \end{cases} \tag{4-4}$$

以图 4-2 中的移动 4 为例，坐标变换前后的坐标如图 4-6 所示：



(a) 原来的x坐标　(b) 原来的y坐标

(c) 坐标变换后的x'坐标　(d) 坐标变换后的y'坐标

图 4-6　斜线方向移动数据的坐标变换

从图 4-6 可以看出，在原来的坐标系中，移动数据的 x 坐标和 y 坐标都有较大的变化范围；在新坐标系中，x'坐标的变化范围较大，y'坐标的变化范围很小。

斜线方向移动数据经过坐标变换后，可以按照前面所述的方法进行速度计算。以图 4-2 中的移动 4 为例，在新坐标系中沿 x'方向的速度远大于沿 y'方向的速度，因此第 j 个数据点的速度计算公式为：

$$v_j = \frac{x'_j - x'_{j-1}}{t_j - t_{j-1}}, \quad j = 2,3,...,J_4 \tag{4-5}$$

在新坐标系中沿 y'方向移动的速度计算公式为：

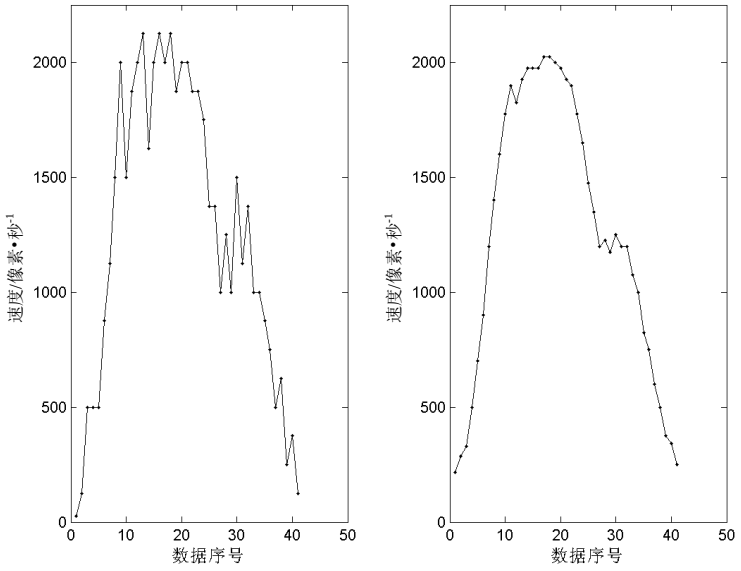
$$v_j = \frac{y'_j - y'_{j-1}}{t_j - t_{j-1}}, \quad j = 2,3,...,J_i, \quad i = 6,7,14,15 \tag{4-6}$$

在新坐标系下的移动速度相当于把原坐标系中的移动速度分解到移动方向上。

从图 4-4 我们可以观察到，由于噪声的影响，速度曲线在有些部位出现了明显的震荡，因此需要进行平滑处理以减少噪声的干扰。本章采用窗口尺寸为 $N=5$ 的平滑过滤方法[64]，依次处理移动序列中每个数据点，计算它与左右 $(N-1)/2$ 个相邻点的平均值：

$$v'_j = (v_{j-2} + v_{j-1} + v_j + v_{j+1} + v_{j+2})/5 \tag{4-7}$$

过滤前后的速度曲线如图 4-7 所示：



(a) 过滤前的速度　　(b) 过滤后的速度

图 4-7　使用平均过滤方法前后的速度曲线

第 i 次移动的速度序列为：

$$V_i = \{v'_j\}, \quad j = 2,3,...,J_i \tag{4-8}$$

最后，从移动数据序列$S_i, i=1,2,...,16$提取的速度曲线为：

$$V=\{V_i\},\quad i=1,2,...,16 \tag{4-9}$$

（2）移动加速度曲线

加速度的计算通过对已经计算出来的速度值求一阶导数，加速度方向和速度方向保持一致。第 j 个移动数据点的加速度定义为：

$$a_j=\frac{v'_j-v'_{j-1}}{t_j-t_{j-1}},\quad j=3,4,...,J_i,\quad i=1,2,...,16 \tag{4-10}$$

数据点的加速度值也使用移动平均过滤去除噪声。

$$a'_j=(a_{j-2}+a_{j-1}+a_j+a_{j+1}+a_{j+2})/5 \tag{4-11}$$

第i次移动的加速度序列为：

$$A_i=\{a'_j\},\quad j=3,4,...,J_i \tag{4-12}$$

最后提取出来的加速度曲线为：

$$A=\{A_i\},\quad i=1,2,...,16 \tag{4-13}$$

2）行为轨迹统计特征

（1）移动偏移量

在鼠标移动过程中，光标会在移动方向和垂直移动方向都产生位移，这个位移反映了鼠标轨迹偏移预定路径的程度。本章将这个量单独提取出来作为一个特征，称作偏移量，计算公式如下：

$$b_i=\begin{cases}\sum_{j=2}^{J_i}|y_j-y_{j-1}|, & x\text{方向的移动}\\ \sum_{j=2}^{J_i}|x_j-x_{j-1}|, & y\text{方向的移动}\end{cases},\quad i=1,2,...,16 \tag{4-14}$$

斜线方向的移动偏移量在变换后的坐标系中计算。对各次移动的偏移量求和，得到总偏移量b_{17}。最终提取到的移动偏移量特征为：

$$B=\{b_i\},\quad i=1,2,...,17 \tag{4-15}$$

（2）移动持续时间

一次移动的持续时间是首尾两个数据点的时间之差。即，

$$T_i=t_{J_i}-t_1, i=1,2,...,16 \tag{4-16}$$

移动持续时间特征为：

$$T=\{T_i\},\quad i=1,2,...,16 \tag{4-17}$$

（3）单击时间间隔统计量

左键单击的时间间隔是从左键按下到弹起的时间间隔。用t_{514}表示左键弹起的时刻，t_{513}表示左键按下的时刻，左键单击的时间间隔按下式计算：

$$t_l = t_{514} - t_{513} \tag{4-18}$$

（4）双击时间间隔统计量

左键双击有 4 个时刻$t_{513}, t_{514}, t_{515}, t'_{514}$，左键双击的时间间隔有 3 个内部时间间隔和 1 个总时间间隔：

$$t_{d1} = t_{514} - t_{513},\ t_{d2} = t_{515} - t_{514},\ t_{d3} = t'_{514} - t_{515},\ t_{d4} = t'_{514} - t_{513}, \tag{4-19}$$

本章采用点击时间间隔的均值和方差这两个统计量。用$\bar{t}$表示t的均值，var表示t的方差，点击时间间隔统计量为：

$$C = \{\bar{t}_l, \bar{t}_{d1}, \bar{t}_{d2}, \bar{t}_{d3}, \bar{t}_{d4}, var_l, var_{d1}, var_{d2}, var_{d3}, var_{d4}\} \tag{4-20}$$

4.5 特征空间表示

由于鼠标交互行为特征向量的高维性和较强的行为波动性，原始的行为特征量并不适合直接作为分类器的输入。因此，本章提出了一种基于距离度量的特征表示方法，生成特征距离向量来表示原始的行为特征空间。在距离度量的过程中，首先使用动态时间规整（Dynamic Time Warping, DTW）方法对轨迹形态特征进行距离特征的计算，其原因在于：1）两个样本的轨迹形态特征曲线（例如移动速度曲线）几乎不可能包含相同数量的移动点；2）DTW 方法能够直接对两个不等长移动序列进行比较而不需要进行降解或变换。其次采用了曼哈顿（Manhattan）距离来计算时空统计特征之间的距离，其原因在于：1）曼哈顿距离是和量纲无关的距离，能够保持特征之间的物理度量量；2）先前的相关领域的研究（Keystroke dynamics）表明应用曼哈顿距离度量统计相关特征能够达到较好的认证效果[112]。

基于上述讨论和分析，本章利用特征向量之间的距离作为分类器的输入，在接下来的描述中将特征向量之间的距离称为特征距离向量。设$\{V_s, A_s, B_s, T_s, C_s\}$为一特征向量，$\{V_t, A_t, B_t, T_t, C_t\}$是生成的参考特征向量，其中时空统计特征为 C，轨迹形态特征为 V, A, B, T，它们之间的特征距离向量记为d_{st}。下面详细描述特征距离向量的计算过程。

4.5.1 参考特征向量的生成

参考特征向量的生成流程如图 4-8 所示，具体的步骤如下：

第一步，分别计算两两训练特征样本的轨迹形态特征的距离向量和时空统计特征的距离向量。我们使用 DTW 方法计算两两训练样本 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 之间的轨迹形态特征，记为$d_{i,j}^{D}$，同时应用曼哈顿距离计算两两训练样本 $\mathbf{x}_i$ 和 $\mathbf{x}_j$ 之间的时空统计特征，记为$d_{i,j}^{S}$，

$$\mathbf{d}_{i,j}^{D} = DTW(\mathbf{x}_i^{D}, \mathbf{x}_j^{D}) \tag{4-21}$$

$$\mathbf{d}_{i,j}^{S} = \left|\mathbf{x}_i^{S} - \mathbf{x}_j^{S}\right| \tag{4-22}$$

其中，$\mathbf{x}_i^{D}$ 表示特征向量 $\mathbf{x}_i$ 中的轨迹形态特征成分，$\mathbf{x}_i^{S}$ 表示特征向量 $\mathbf{x}_i$ 中的时空统计特征成分。

第二步，将得到的轨迹形态特征和时空统计特征的距离度量组合在一起形成两两样本之间的特征距离向量。

$$\mathrm{d}_{ij} = [\mathrm{d}_{ij}^{D}, \mathrm{d}_{ij}^{S}] \tag{4-23}$$

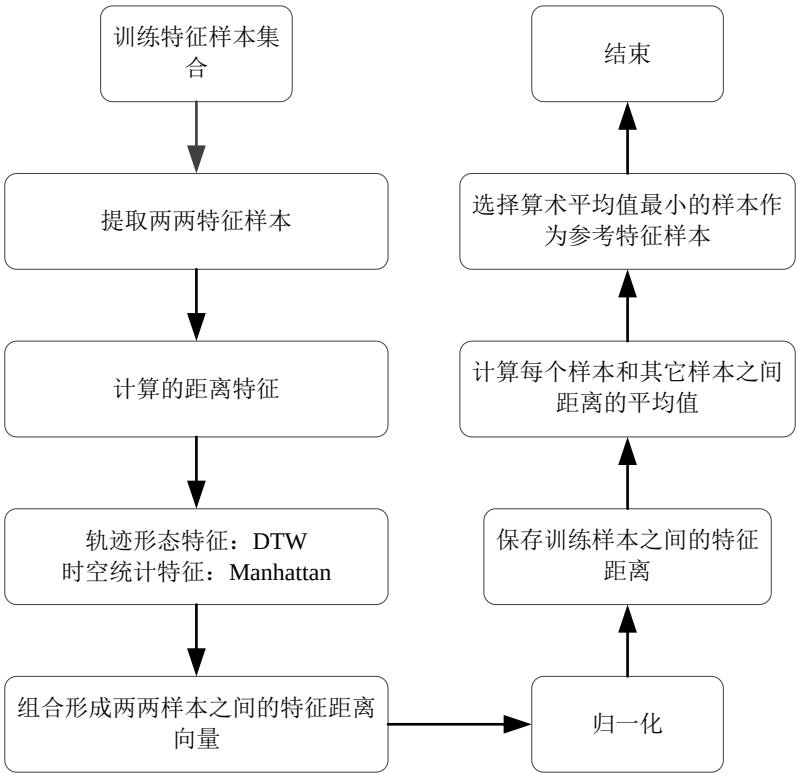


图 4-8 参考特征向量的生成流程

第三步，对得到的特征距离向量进行正则化处理，使其成为尺度无关的特征向量。

$$\bar{\mathrm{d}}_{i,j} = \{\bar{\mathrm{d}}_{i,j}^{l} \mid \bar{\mathrm{d}}_{i,j}^{l} = \frac{\mathrm{d}_{i,j}^{l} - \mu_l}{\sigma_l}, l = 1 \cdots d\} \tag{4-24}$$

其中，$\boldsymbol{\mu}=\{\mu_1,\mu_2,\ldots,\mu_d\}$是所有两两样本特征距离向量的平均值，$\boldsymbol{\sigma}=\{\sigma_1,\sigma_2,\ldots,\sigma_d\}$是所有两两样本特征距离向量的标准差。

第四步，针对每个训练特征样本，计算该样本和其它所有剩余样本之间的算术平均距离，然后选择算术平均距离最小的那个样本作为参考特征样本 $\mathbf{x}_{ref}$。

$$\mathbf{x}_{ref} = \mathbf{x}_k,\ k = \arg\min_i \frac{1}{K-1} \sum_{j=1, j\neq i}^{n} \sqrt{\sum_{l=1}^{d} (\bar{d}_{i,j}^{l})^2}. \tag{4-25}$$

4.5.2 特征距离向量的计算

得到每个用户对应的参考特征样本后，可以很容易的计算出任意特征样本与参考特征样本之间的距离作为该特征样本的特征距离向量。令 $\mathbf{x}_{ref}$ 表示某个用户的参考特征样本，对于任意的特征样本 $\mathbf{x}_i$（来自于合法用户或非法用户），可以通过公式（4-21）、（4-22）、（4-23）、（4-24）计算得到对应的特征距离向量。

图 4-9 表示了用户的两个样本之间的速度曲线特征 (V_i, V_j) 的动态时间规整计算过程，图中连接速度曲线的短线表示移动数据点对之间的距离。从图 4-9 中可以看出，利用 DTW 可以较好的刻画同一个用户速度曲线之间的差异，同时不同用户之间速度曲线有着明显的区分性。

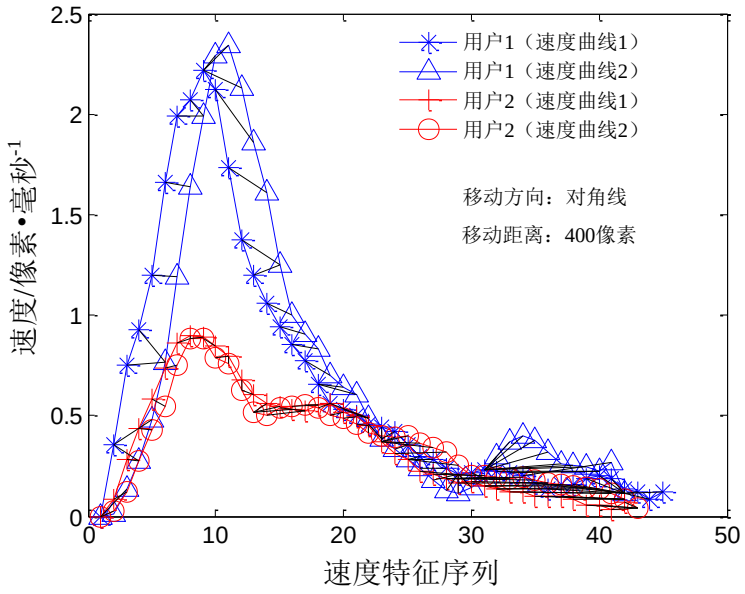


图 4-9 不同用户两个样本之间的速度曲线特征 DTW 计算对比图

在本章中，针对每个鼠标操作样本，我们提取了对应的时空统计特征和轨迹形态特征，并生成了相应的特征距离向量。其中共包括 10 个点击相关的特征，16 个距离相关的特征，16 个时间相关的特征，16 个速度相关的特征，16 个加速度相关的特征，这些特征距离成分被组合在一起，形成了 74 维的特征距离向量。

4.6 特征空间变换

在行为分析中，行为特征度量量常常会由于行为波动性的干扰包含一定程度的非线性噪声信息，不适用于直接作为分类器的输入。因此在这里我们对得到的特征距离向量首先进行核空间的变换，接着应用主成分分析方法选择特征距离空间的主要表征量对行为空间进行刻画，并将这些主要表征量作为分类器的输入。

4.6.1 核主成分分析的训练

与传统的主成分分析方法（Principal Component Analysis, PCA）相比，核主成分分析方法（Kernel Principal Component Analysis, KPCA）[113]是一种非线性的降维方法，能够抽取数据中的非线性特性。KPCA 的基本思想是将核函数的概念引入传统的线性主成分分析中，把数据从输入空间映射到高维特征空间，然后在高维特征空间中利用线性主成分分析方法计算主成分。本章使用 KPCA 的目的在于获得特征距离空间的主要表征量，其计算流程如图 4-10 所示，具体的过程如下：

对于某一个用户，其训练样本集表示从其所有的数据样本中提取出的部分特征距离向量样本的集合。假定 $\mathbf{D}_i$ $(\mathbf{D}_i \in \Re^d, i=1,2,\ldots,n)$ 为训练样本集中的第 i 个特征距离向量，n 表示特征距离向量的个数。首先使用非线性的核函数 $\Phi:\mathbf{D}_i \in \Re^d \to \mathbf{Z}_i \in \Re^h$ 将被测量的向量映射到高维的核特征空间中。接着获得训练样本集合在高维空间的均值向量和协方差矩阵：

$$\mathbf{m}_\Phi = \frac{1}{n}\sum_{i=1}^{n}\Phi(\mathbf{D}_i) \tag{4-26}$$

$$\Sigma_\Phi = \frac{1}{n}\sum_{i=1}^{n}(\Phi(\mathbf{D}_i)-\mathbf{m}_\Phi)(\Phi(\mathbf{D}_i)-\mathbf{m}_\Phi)^T \tag{4-27}$$

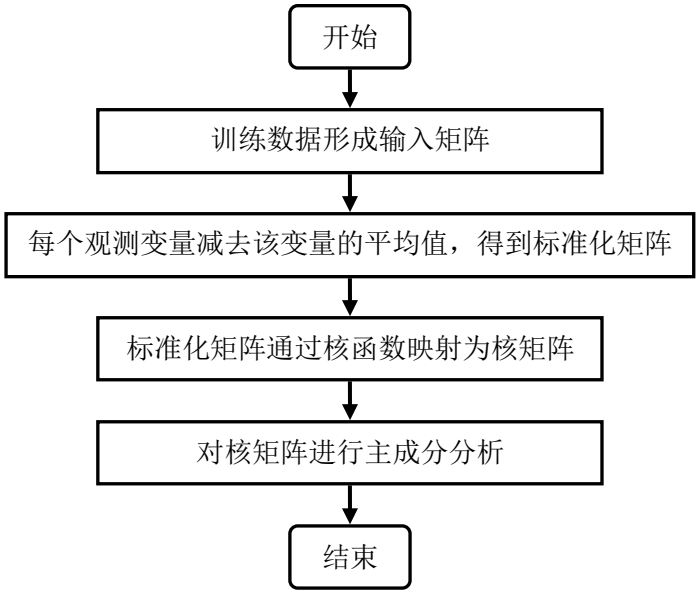


图 4-10 基于 KPCA 的特征距离空间变化的训练流程

在这里我们利用得到的高维空间的均值向量对映射的数据点进行中心化处理 $\bar{\Phi}(\mathbf{D}_i)=\Phi(\mathbf{D}_i)-\mathbf{m}_\Phi$。该特征距离空间的主成分表征量可以通过求解下面的特征值问题获得，

$$\lambda\mathbf{V} = \Sigma_\Phi\mathbf{V} = \frac{1}{n}\sum_{i=1}^{n}\bar{\Phi}(\mathbf{D}_i)^T\mathbf{V}\bar{\Phi}(\mathbf{D}_i) \tag{4-28}$$

其中$\lambda>0$并且$\mathbf{V}\neq\mathbf{0}$。接着，通过定义相应的核空间的变化矩阵，

$$K_{ij} := (\bar{\Phi}(\mathbf{D}_i)\cdot\bar{\Phi}(\mathbf{D}_j)) = \mathbf{k}(\mathbf{D}_i,\mathbf{D}_j) \tag{4-29}$$

我们从特征值问题的求解中可以获得系数α_i，该系数依赖于所定义的核空间函数：

$$\lambda\boldsymbol{\alpha} = K\boldsymbol{\alpha} \qquad (\boldsymbol{\alpha} = (\alpha_1,\cdots,\alpha_n)^T) \tag{4-30}$$

关于高维核空间函数的详细构造过程，可参见 B. Schölkopf *et al.* [114]。

通过上述特征值问题的求解，可以得到对应的特征值和特征向量，从而进一步生成特征向量的投影矩阵。一般来说，少数的从高维空间得到的特征向量就可以表示训练样本集的信息，这些特征向量对应着较大的特征值。因此，为了得到在低维的行为特征距离空间的主成分表征量，本文利用一个阈值 T_s 来选择较大的特征量并利用对应的特征向量构建投影变换矩阵，其流程如图 4-11 所示。其计算过程为，

$$R_k = \sum_{i=1}^{k}\lambda_i \Big/ \sum_{i=1}^{n}\lambda_i > T_s \tag{4-31}$$

其中，R_k 表示前 k 个较大的特征量在整个特征空间中的累加贡献度，该值可以表现出前 k 个特征量在原始特征空间中所能够覆盖的信息量。本文根据经验将阈值 T_s 设定为 0.95（变化范围从 0 到 1）。需要注意的是，我们针对所有用户都设定了相同的阈值 T_s，因此对于不同的用户，k 的取值会不同。在实验中，我们观察到对于不同的用户，主成分表征量的个数从 12 到 20 变化不等。

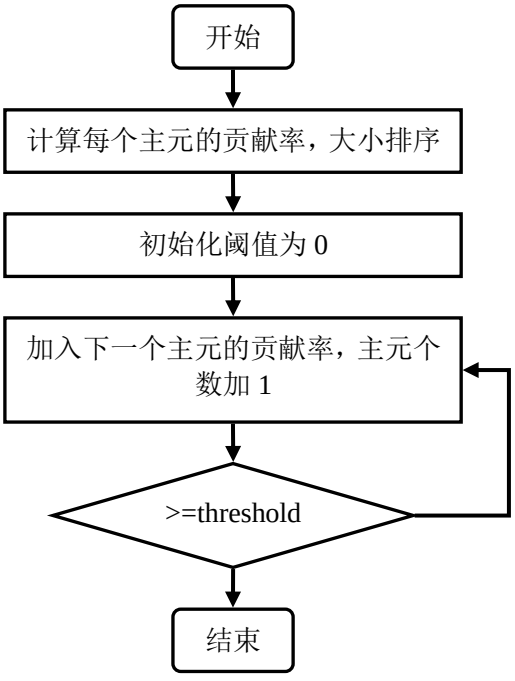


图 4-11 低维空间的行为特征距离空间的主成分表征量个数计算

4.6.2 核主成分分析的投影

针对某个选定的用户，选取该用户的 k 个特征量及其对应的特征向量，构建特征

空间的投影变换矩阵，

$$\mathbf{V}^k = [V_1\ V_2\ \ldots\ V_k] \tag{4-32}$$

对于需要进行特征空间变换的数据生成其特征距离向量 **D**，在投影变换矩阵的基础上对特征距离向量 **D** 进行投影映射，得到低维空间的特征距离向量 **P**，

$$\mathbf{P} = \mathbf{V}^k \cdot \bar{\Phi}(\mathbf{D}) = \sum_{i=1}^{n} \alpha_i^k \mathbf{k}(\mathbf{D}_i, \mathbf{D}) \tag{4-33}$$

基于上述的过程，每个用户的鼠标交互行为数据都可以被映射到对应参数空间的流形轨迹上。在实验分析中，我们发现 k 值往往要远远小于原始特征空间的维数，也就是说，基于 KPCA 的特征空间分析方法能够在很大程度上减小鼠标输入空间的维数。如图 4-12 所示，我们以用户 7 为例对比分析了 KPCA 和传统的 PCA 在鼠标行为特征距离空间的作用效果。从该图可以观察到，当使用传统的 PCA 时，在设定的阈值下（0.95）低维空间的主成分表征量的个数为 25，这意味着原始空间的维数从 78 下降到了 25；当使用 KPCA 进行相似的分析时，获得了 19 维的低维空间的主成分表征量，原始空间的维数从 78 下降到 19，维数降低的效果强于传统的 PCA。这说明在原始的行为空间中确实存在着非线性噪声或相关量，使用 KPCA 可以有效地降低这些噪声或相关量的干扰。

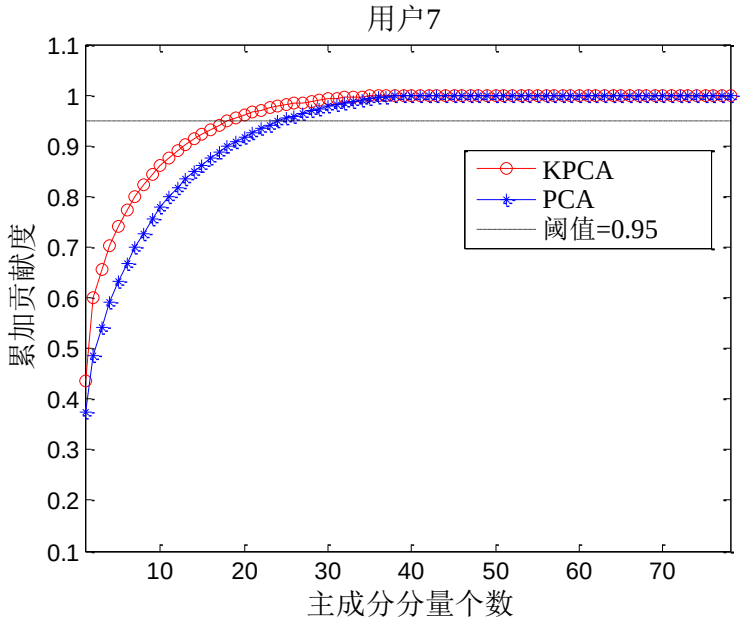


图 4-12 KPCA 和 PCA 贡献度的对比分析

基于上述的计算过程，在下面的分析中我们使用特征距离空间的主成分表征量作为行为分类器的输入。

4.7 身份认证分类器

本节描述了用于身份认证的单分类支持向量机分类器，并介绍了另外两种广泛使用的分类器。每个分类器经过学习后用于合法用户和非法用户区分。

4.7.1 单分类学习器概述

从模式分类的角度来说，用户身份认证是一项具有挑战性的任务，是一个二分类（合法 vs. 非法）问题。在利用鼠标交互行为进行用户身份认证的场景下，用户需要在认证过程中完成一系列鼠标行为的操作，每个用户都拥有自己的鼠标操作模式（像计算机登录密码一样），并且不会和别人分享。当为合法用户建立其对应的身份模型时，该用户的训练样本来源于该用户本身，而其他用户（在认证场景下被视为入侵者）的样本是很难获取到的。因此在身份认证场景下，一种更合适的解决方案是建立只基于合法用户数据样本的身份模型，并且使用这个模型来对用户身份的合法性进行判别。这类问题被称为单分类或者异常检测[115-117]。

4.7.2 主分类器：单分类支持向量机

传统的单分类方法经常无法达到令人满意的效果，比如常常遗漏正确的合法样本或产生较多错误的非法样本。在本章的研究中，我们使用由 Scholkopf 等人提出的单分类支持向量机[118,119]。该方法已经被成功地应用在了许多的实际分类问题中，例如，人脸识别，签名识别以及击键身份识别。

如图 4-13 所示，首先给定属于某个用户的 l 个训练样本$\{\mathbf{x}_i \in \Re^d\}$，$i$=1,…$l$,每个样本有 d 维特征（对应于此用户的特征距离向量的主成分表征量）。其目标在于在最大边缘化的条件下找到一个超平面来划分数据点。为了以原点为轴心划分数据点，需要解决如下的二次规划问题，

$$\begin{aligned} \max_{\beta} \quad & W(\beta)=\sum_{i=1}^{l}\beta_i\beta_j k(\mathbf{x}_i,\mathbf{x}_j) \\ \text{s.t.} \quad & 0\le\beta_i\le\frac{1}{vl},\ i=1,\ldots,l; \quad \sum_{i=1}^{m}\beta_i=1 \end{aligned} \tag{4-34}$$

这里$\beta=\{\beta_i\}$是待定的 l 个非负的拉格朗日算子，其作用是最大化被超平面包含的数据点的个数和超平面到原点的距离；$k(\mathbf{x}_i,\mathbf{x}_j)$是核函数。这里我们允许非线性决策边界，对应的决策函数为，

$$f(\mathbf{x})=\text{sign}(\sum_{i=1}^{l}\beta_i k(\mathbf{x}_i,\mathbf{x}_j)-\rho) \tag{4-35}$$

ρ 是决策函数的偏移量。

我们把用户身份认证问题看作是一个单分类问题。在训练阶段，学习任务是基于合法用户的特征样本建立一个分类器。在测试阶段，测试样本被映射到对应的高维空

间中，决策函数的输出被记录下来。基于训练精度对线性核、多项式核、放射基核以及 sigmoid 核进行比较之后，这里我们采用了放射基函数 $k(\mathbf{x}_i,\mathbf{x}_j)=\exp(-\gamma\left\|\mathbf{x}_i-\mathbf{x}_j\right\|^2),\gamma>0$。支持向量机的参数 v 和核参数 γ（使用 libsvm[120]）分别设定为 0.06 和 0.004。如果输入的是合法用户的测试集，决策函数输出为"+1"，否则则作为一个误拒的实例。相反，如果输入的是非法用户的测试集则决策函数输出为"-1"，否则则作为一个误纳的实例。

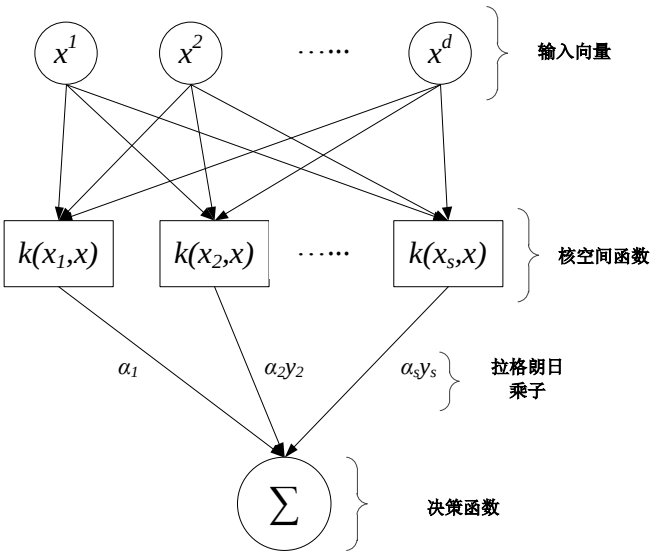


图 4-13 单分类 SVM 的建模过程

4.7.3 对比 1：单分类最近邻分类器

最近邻(k-Nearest Neighbor，KNN)分类算法[121]，是一个理论上比较成熟的方法，也是最经典的机器学习算法之一。该方法的思路是：如果一个样本在特征空间中的 k 个最相似（即特征空间中最邻近）的样本中的大多数属于某一个类别，则该样本也属于这个类别。在 KNN 算法中，所选择的邻居都是已经正确分类的对象。该方法在分类决策上只依据最邻近的一个或者几个样本的类别来决定待分样本所属的类别。

在单分类最近邻距离分类器的训练阶段，首先在训练数据集上计算出协方差矩阵，同时保存训练数据的对应的特征向量。经过在训练集上的多次测试，我们选择最近邻 k 的数目为 3。在该分类器的测试阶段，对于每个测试样本，首先计算出该样本到训练样本的马氏距离（Mahalanobis distance），然后将该测试样本到最近邻样本的距离作为该样本的检测值。

由于 KNN 方法主要依靠周围有限的邻近样本，而不是依靠判别类域的方法来确定所属类别的，因此对于类域的交叉或重叠较多的待分样本集来说，KNN 方法较其它方法更为适合。

4.7.4 对比 2：单分类神经网络分类器

BP（Back Propagation）神经网络[121]是一种按误差逆传播算法训练的多层前馈网络，

是应用最广泛的一种神经网络模型。BP 神经网络的基本原理是利用输出后的误差来估计输出层的直接前导层的误差，再用这个误差估计更前一层的误差，如此一层一层的反传下去，就获得了所有其它各层的误差估计。BP 神经网络使用激活函数描述层与层输出间的关系，从而模拟各层神经元之间的交互。其中，激活函数需要满足处处可导的条件，经常用到的激活函数是 S 型函数。

$$net = x_1 w_1 + x_2 w_2 + ... + x_n w_n$$
$$y = f(net) = \frac{1}{1 + e^{-net}} \quad (4\text{-}36)$$

BP 神经网络的学习过程是 1) 正向传播，输入样本分别经过输入层、各隐层和输出层得到输出值；2) 判断是否反向传播，如果输出层的输出值和期望的输出不符合，则转入反向传播阶段；3) 误差反传，误差以前面所述的形式在各个层表示并修正各层单元的权值以减小误差。当网络的输出误差减小到可接受的范围或者学习次数大于设定的最大次数时结束算法，否则选取下一个学习样本及对应的期望输出进入下一轮学习。

在单分类神经网络训练阶段，我们建立了三层学习网络，第一层有 p 个输入节点，最后一层有 1 个输出节点，第二层有$\lfloor 2p/3 \rfloor$个隐节点。网络中节点的权值随机地初始化为 0 到 1 之间的值，对于每一个训练样本的输出都设定为 1.0。我们使用 0.001 的学习率进行了 1000 个循环的训练。在测试阶段，测试样本被输入网络，并记录下网络的输出。设 s 为网络的输出值；若 s 接近于 1.0，则该测试样本与训练样本较为相似，若 s 接近于 0.0，则该测试样本与训练样本不相似。

4.8 评估方法

本节介绍了用于鼠标行为身份认证的评估方法。首先简述了该实验的数据集，接着建立了认证模型的训练和测试流程，然后介绍了认证结果的评估指标。最后引入了一种统计分析的方法用于认证结果的统计分析。

4.8.1 数据集

如章节 4.3 所述，用户操作固定的鼠标行为模式进行交互行为样本的采集。58 个用户参与了该认证实验，每个用户采集了 150 个行为样本，总共提供了 8700 个行为样本。我们针对每个样本计算了特征距离向量，并从中提取了低维的主成分表征量用作分类器的输入。

4.8.2 训练和测试过程

在章节 4.7.1 所述的身份认证场景下，我们首先指派 58 个用户中的 1 个作为合法用户，其他用户作为非法用户。按照如下的步骤训练并且测试分类器对合法用户和非法用户的识别能力：

第一步，建立合法用户的身份模型。从合法用户的数据中随机抽取 75 个样本（总

共 150 个样本）建立该用户的身份认证模型；

第二步，测试该模型对合法用户的识别能力。将该合法用户剩余的 75 个样本作为身份模型的输入，计算这些样本的分类分数，记为合法分数。

第三步，测试该模型对非法用户的识别能力。将非法用户的所有样本（57×150=8550）作为身份模型的输入，计算这些样本的分类分数，记为非法分数。

第四步，依次指定其余用户作为合法用户，并重复上面的步骤得到每个用户对应的合法分数和非法分数。

在训练的过程中，我们采用了 10 折交叉验证计算模型的参数[122]。此外，由于在训练过程中使用了随机选择的方法获得用于生成身份模型的训练样本，为了解释这个随机因素，我们将上述实验重复了 50 次，每次重复独立地从样本池中选择合法用户的训练样本。

4.8.3 评估指标

为了将测试过程中得到的合法和非法分数转化成身份模型的评测值，我们计算了误纳率（False-Acceptance Rate, FAR）和误拒率（False-Rejection Rate），同时利用这两个指标得到了受试者工作特征曲线（Receiver Operating Characteristic curve，简称 ROC 曲线）[123]。在本研究中，FAR 是指进行身份检测时被判为合法用户的非法用户样本数占测试的非法用户样本总数的百分比，用来衡量入侵的非法用户被错误地判别为合法用户通过验证的概率；FAR 越小，则非法用户被错误地接受的概率越小，系统的安全性越高，其数值大小与系统设定的判定相似度的阈值呈负相关，即相似度阈值定得越高，FAR 的数值越低。FRR 是指进行身份检测时被判为非法用户的合法用户样本数占测试的合法用户样本总数的百分比，用来衡量合法用户被错误地判别为非法用户拒绝通过验证的概率。FRR 越小，则合法用户被错误地拒绝的概率越小，系统更容易被普通用户接受，其数值大小与系统设定的判定相似度的阈值呈正相关，即相似度阈值定得越高，FRR 的数值也越高。我们首先计算了每个用户的 FAR 和 FRR 值，然后针对所有用户得到了 FAR 和 FRR 的平均值。

一个鼠标操作样本被判定为非法或合法依赖于检测阈值的设定。身份检测分数超过检测阈值时用户被判定为非法用户，低于检测阈值时用户被判定为合法用户。在实际操作中，为了使一个认证系统更易于在现实中部署，降低合法用户被拒绝的概率（即降低 FRR 以增加模型的可用性）比降低非法用户被接受的概率（即降低 FRR）重要[78]。然而如前所述，FAR 和 FRR 是一对折中值。这里我们通过在训练过程中调整 FRR 的值得到相应的身份检测阈值，其原因是 FRR 的计算只需要合法用户的数据。具体来讲，身份检测阈值的变化区间为[-1, 1]，该阈值的选择通过在训练集上产生较小的 FRR 得到。进行多次测试之后，我们将检测阈值设定为 0.1。在本章的后续研究中，FAR 和 FRR 值都是在身份阈值为 0.1 下得到的。

4.8.4 统计分析指标

为了进一步评价方法的有效性，我们采用了一种基于 HTER（Half Total Error Rate）和置信区间（Confidence Interval, CI）的统计检测评估方法[124]。HTER 检测的目的在于统计性地分析和评估身份认证效果的优劣，该指标的计算如公式（4-37）所示，

$$HTER = \frac{FAR + FRR}{2} \tag{4-37}$$

认证结果置信区间的计算可以通过 $HTER \pm \sigma \cdot Z_{\alpha/2}$ 得到，其中 σ 和 $Z_{\alpha/2}$ 可通过公式（4-38）和（4-39）计算得到，

$$\sigma = \sqrt{\frac{FAR(1-FRR)}{4 \cdot NI} + \frac{FRR(1-FAR)}{4 \cdot NG}} \tag{4-38}$$

$$Z_{\alpha/2} = \begin{cases} 1.645 & for\ 90\%\ CI \\ 1.960 & for\ 95\%\ CI \\ 2.576 & for\ 99\%\ CI \end{cases} \tag{4-39}$$

其中 *NG* 是合法分数集的个数，*NI* 是非法分数集的个数。

4.9 实验结果与分析

本章进行了多个实验以分析该方法的有效性。首先我们进行了身份认证实验，并将实验结果与其它两类分类器进行了比较。其次，我们检验了特征空间变化方法对认证识别结果的影响。接着，我们检验了样本长度对认证结果的影响，同时讨论了该技术在可用性和安全性之间的折中。最后，我们将该方法同文献中相关方法进行了比较。

4.9.1 实验 1：身份认证实验结果与分析

图 4-14 和表 4-2 展示了身份认证实验的 FAR、FRR 及 ROC 曲线，括号内的数值表示相关 FAR 和 FRR 值的标准差。表 4-2 也包含了平均的认证时间，该时间值是通过对所用用户样本的平均采集时间和平均决策时间加和得到的（由于后者的数值总小于 0.003 秒，因此我们在这里忽略平均决策的时间）。

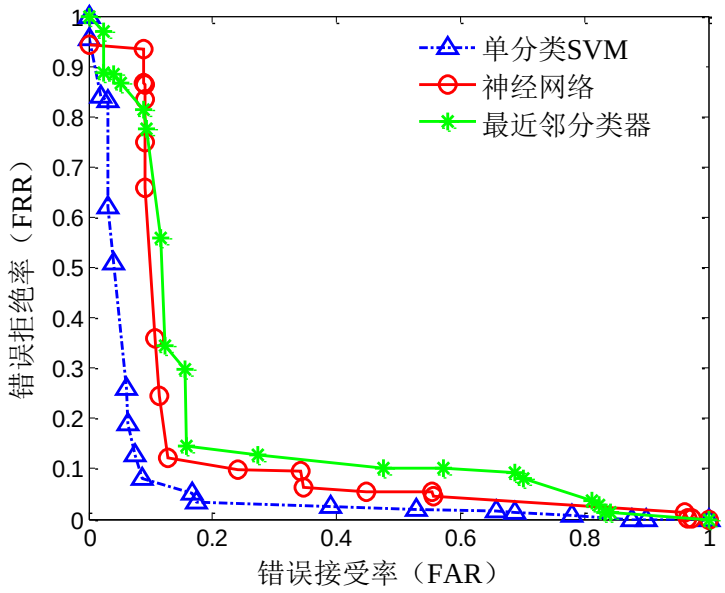


图 4-14 身份认证结果的 ROC 曲线

从图 4-14 和表 4-2 的实验结果中，可以观察到最好的认证结果为 8.74%的 FAR 和 7.96%的 FRR，该结果是非常有效且很有竞争力的。此外，该方法对鼠标交互行为的观察时间要明显短于文献中的其它方法。需要指出的是，这个结果还没有达到欧洲标准对商业生物行为特征的要求（0.001%的 FAR 和 1%的 FRR）[125]。但该结果证实了鼠标交互行为中确实含有能够对用户身份进行认证的信息。我们相信经过一系列的增量式的改进方法，鼠标交互行为特征能够成为一种身份认证的辅助技术，例如一种对传统密码认证技术的加强手段。

表 4-2 身份认证结果的 FAR 和 FRR 值（括号内为对应的标准差）

分类器	FAR/%	FRR/%
单分类支持向量机	8.74 (4.26)	7.96 (4.23)
BP 神经网络	12.78 (5.67)	12.22 (5.12)
最近邻分类器	15.67 (10.74)	14.53 (10.62)
平均认证时间: 11.8 秒		

我们还观察到基于单分类支持向量机得到的身份认证结果明显优于其它两种广泛使用的分类算法。其原因是支持向量机在先验知识不足的条件下能够将分类问题转化为二次优化问题，并且能够保持较高的精度和稳定性。此外，对应的身份认证结果的标准差也明显小于其它两种方法。这一结果表明结合单分类支持向量机的身份认证模型对不同的参数选择方法和行为波形性具有一定的鲁棒性。

我们方法的平均认证时间为 11.8 秒，该时间长度达到了现实应用的程度。文献中的一些方法常常需要较长的观察时间对用户身份的合法性进行检测（12.55 分钟[32]），然而，我们的方法能够在 11.8 秒之内对用户完成身份认证。这表明鼠标交互行为能够

完成快速的身份认证，可适用于大部分的登录需求。我们推测认证时间的大幅度降低是由于我们使用的轨迹形态的特征刻画量，该类特征能够提供更加详细和细粒度的运动轨迹的描述。

最后，我们使用了 HTER 和置信区间对得到的认证结果进行了统计分析。表 4-3 呈现了不同置信区间下的统计分析的结果。三类分类方法的实验结果对比分析表明结合单分类支持向量机的方法能够得到最低的 HTER。在 95%的置信区间下，该方法的认证错误率为 8.35% ±3.24%。

表 4-3 身份认证结果的统计分析值

分类器	HTER/%	置信区间/%		
		90%	95%	99%
单分类支持向量机	8.35	±2.72	±3.24	±4.25
BP 神经网络	12.50	±3.21	±3.83	±5.03
最近邻分类器	15.10	±3.50	±4.17	±5.48

4.9.2 实验 2：特征空间变换对认证的影响

本实验检验了特征空间变换方法对认证效果的影响。借助于单分类支持向量机构建的身份模型，我们分别使用三个不同的特征空间作为输入：原始的特征空间、经过 KPCA 变换的特征空间以及经过 PCA 变换的特征空间。图 4-15 和表 4-4 展现了三种不同的特征空间作为输入得到的 FAR、FRR 及 ROC 曲线，表 4-4 括号内的数值表示相关 FAR 和 FRR 值的标准差。

如图 4-15 和表 4-4 所示，经过 KPCA 变换的特征空间的认证效果最佳，经过 PCA 变换的特征空间的认证效果次之，最后是原始特征空间上的认证结果。具体来讲，在原始空间上的直接认证得到了 15.45%的 FAR 和 15.98%的 FRR。与先前的研究相比较，这个结果并不是很好。然而，正如实验 1 所述，我们的数据样本含有更大的行为波动性，因为我们进行认证时所观察的鼠标交互时间较短。此外，我们也发现经过 PCA 和经过 KPCA 变化的特征空间的认证结果可以分别达到 10.57%的 FAR，10.12%的 FRR，以及 8.74%的 FAR，7.96%的 FRR，这个结果明显优于未经变换的原始特征空间。这进一步证实了特征空间变换在处理波动的行为数据时的可行性和有效性。进一步分析可以看到 KPCA 的认证结果要略优于 PCA 的认证结果。其原因可能是由于鼠标交互行为中存在非线性的行为波动，使用 KPCA 的特征空间变换能有效地减弱这种非线性的行为波动（通过使用核空间变换）[126]。同时需要注意的是，结合 KPCA 和 PCA 的认证结果的标准差也明显的小于原始空间，表明特征空间变换能够加强方法的稳定性和鲁棒性。

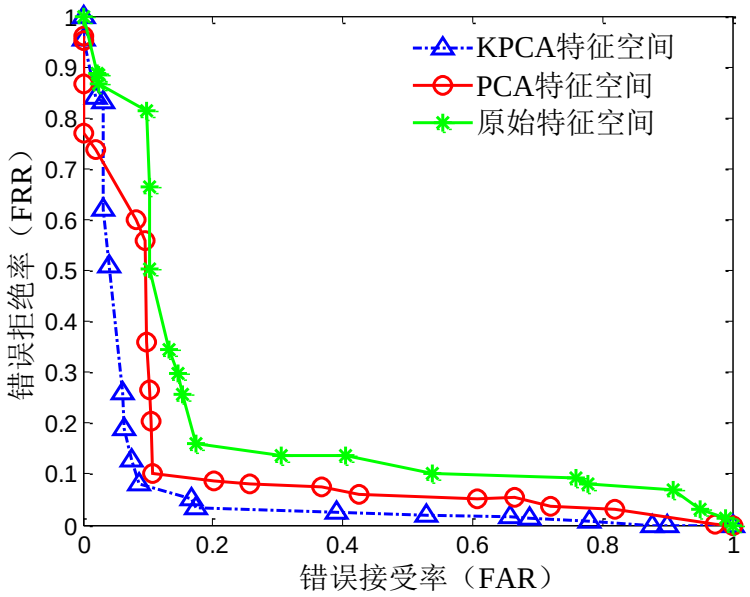


图 4-15 不同特征空间下身份认证结果的 ROC 曲线

表 4-4 不同特征空间下身份认证结果的 FAR 和 FRR 值

身份模型	FAR/%	FRR/%
单分类支持向量机+KPCA	8.74 (4.26)	7.96 (4.23)
单分类支持向量机+PCA	10.67 (6.67)	10.12 (7.45)
单分类支持向量机	15.45 (11.46)	15.98 (10.53)

4.9.3 实验 3：样本长度变化对认证的影响

本实验检验了样本长度的变化对认证效果的影响，其目的在于研究该方法的安全性（认证精度）和可用性（认证时间）的折中。在基于鼠标交互行为的身份认证中，样本长度对应着鼠标操作模式中包含的鼠标操作的个数。在身份认证场景下，每个原始的鼠标交互样本包含了 32 个鼠标操作。为了研究样本长度对认证结果的影响，我们首先导出不同样本长度 s_n 对应的数据集，以原始数据集为基础应用可重复采样的方法[127]使新生成数据集和原始的数据集拥有相同数量的样本。新数据样本是根据原始数据集中多个连续的样本组合而成的。根据上述的方法，我们可以将身份认证的精度看成是样本长度的函数。基于此，我们生成了 6 个数据集，这些数据集中单个样本的长度分别为：s_n = 32, 80, 160, 320, 480, 800，然后在这些数据集上进行了身份认证实验（使用单分类支持向量机）。

表 4-5 呈现了不同样本长度下身份认证的 FAR 和 FRR 值，表中也展示了不同样本长度所对应的认证时间。我们可以看到在样本长度为 32 时，身份认证的 FAR 为 8.74%，FRR 为 7.96%，对应的认证时间为 11.80 秒。当样本长度的增加到 80 时，FAR 值减少到 6.97%，FRR 值减少到 6.68%，对应的认证时间为 29.88 秒。因此身份认证的精度会随着样本长度的增加而提升。需要注意的是，用户可以接受认证时间长度的上

限大概为 60 秒左右，但是对应的 FAR 为 4.69%，FRR 为 4.46%，这样的认证精度并不能达到欧洲标准对商用的生物特征身份认证的要求。我们同时也发现当样本长度增加到 800 时，我们的方法能获得 0.87%的 FAR 和 0.69%的 FRR，这样的结果非常接近于前面所述的欧洲标准，但是对应的认证时间却为 588.62 秒（约为 10 分钟），这在现实应用中是不能接受的。因此，在身份安全和可用性之间存在于一个折中，我们期待更多的研究来改进这个折中，以提高这种技术的可应用性。

表 4-5 不同样本长度下的身份认证结果 FAR 和 FRR 值

样本长度 (鼠标操作的数量)	FAR/%	FRR/%	认证时间/秒
32	8.74	7.96	11.80
80	6.97	6.68	29.88
160	4.69	4.46	59.49
320	3.33	2.12	118.14
480	1.67	1.27	295.14
800	0.87	0.69	588.62

4.9.4 比较

基于鼠标交互行为的身份认证已经吸引了相关领域大量研究者的兴趣。然而，在这个领域中还没有公开的数据集和基准化的评价算法。缺失可靠性的公开数据集（例如人脸识别领域的 FERET 数据集[15]）和标准的评测方法极大地限制了该技术的发展。先前绝大多数的研究者都在自己提供的数据集上测试自己的方法，选用不同的特征，但是没有人对不同的特征集和不同的结果进行比较。在这里我们进行了两个比较实验将我们的方法与文献中相关的方法进行深入的比较。

1）比较 1：不同特征的比较

如前所述，在本章中我们基于鼠标点击和移动构建了相应的特征空间，包括时空统计特征和轨迹形态特征。为了进一步检验这些特征的有效性，我们和文献中的特征进行对比实验。我们选择了 Gamboa 等人[55]、Aksari 和 Artuner [63]、Hashia 等人[101]、Bours 和 Fullu [64]、Ahmed 和 Traore [32]使用的行为特征集，因为这些特征集都从不同的方面对鼠标交互行为进行了刻画。我们首先从身份认证场景下的数据集中提取了本文和前述文献中的特征集，然后使用基于单分类支持向量机的身份模型进行了身份认证实验。最后我们对不同特征集的身份认证结果进行了比较。

图 4-16 和表 4-6 呈现了不同特征集下身份认证实验的 ROC 曲线和 FAR 及 FRR 值。表 4-6 中的括号内是对应 FAR 和 FRR 的标准差。可以观察到使用本章所定义的特征的平均错误率要明显优于使用其它方法定义的特征。这是由于我们的方法所用轨迹形态特征，这类特征能够对光标运动轨迹形态变化进行准确和细粒度的描述。但也有可能是因为 1）不同方法的采集环境导致特征提取的不完备性；2）在认证过程中使用不同的检测阈值；3）在模型建立时使用较少的数据样本。认证精度的提升也说明相

比于文献中其它方法定义的特征，我们所定义的特征能够更加有效和准确的刻画用户的行为。从表 4-6 中我们也可以观察到使用我们的特征得到的认证结果的标准差要小于使用其它特征得到的标准差，这也说明了我们的特征对于行为数据中的波动性呈现了一定的稳定性和鲁棒性。

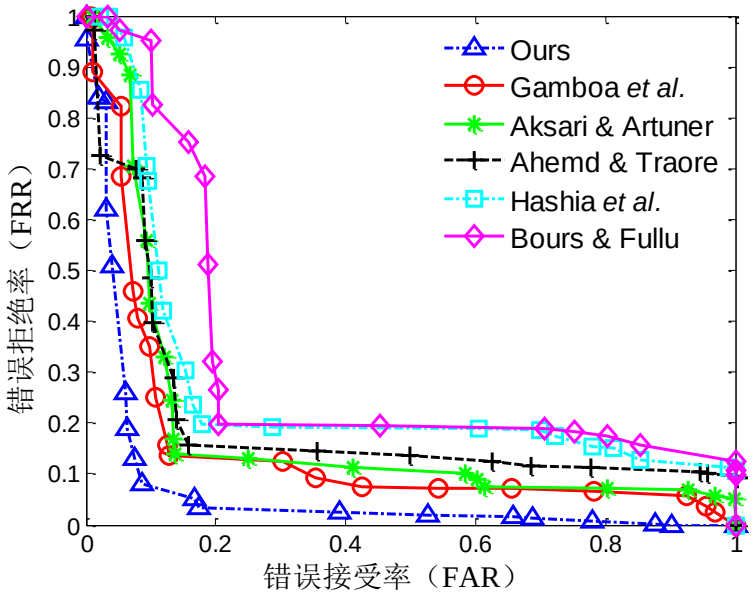


图 4-16 不同特征集下身份认证的 ROC 曲线

此外，针对我们所定义的两类特征，分别以每类特征作为输入进行了相应的身份认证实验。实验结果表明轨迹形态特征的认证结果要优于时空统计特征。具体来讲，基于轨迹形态特征的身份认证精度为 10.32%的 FAR 和 9.78%的 FRR，而基于时空统计特征的身份认证精度为 19.58%的 FAR 和 17.96%的 FRR。

表 4-6 不同特征集下身份认证的 FAR 和 FRR 值

身份模型：单分类支持向量机		
特征集来源	**FAR/%**	**FRR/%**
Our work	8.74 (4.26)	7.96 (4.23)
Gamboa *et al.* [55]	12.87 (9.46)	13.63 (9.73)
Aksari and Artuner [63]	13.76 (11.24)	13.85 (10.35)
Ahmed and Traore [32]①	15.89 (7.63)	15.67 (6.92)
Hashia *et al.* [101]	17.85 (12.35)	19.86 (13.56)
Bours and Fullu [64]	20.32 (15.68)	19.65 (13.48)

需要指出的是，这个对比实验只是呈现了初步的结果，因此并不能下结论说某类特征总是强于其它类的特征。每种类别的特征从不同的侧面刻画了鼠标交互行为，因

① 由于文献[32]中方法的应用为身份监控，这里我们提取了和我们数据集中的鼠标操作相关的特征。我们的目的是检验应用于身份监控中的特征是否也能用在静态认证中。

此更加深入的实验和评估才能得出相关的结论。

2）比较 2：相关工作的比较

大多数先前的方法要么会导致较低的身份认证效果（较低的认证精度或较长的认证时间），或使用了较小的数据集。在这里，我们对相关方法的实验设置和实验结果进行比较分析，如表 4-7 所示。

表 4-7 相关工作的定性比较

方法来源	实验结果			Data Collection			训练数据来源
	FAR /%	FRR /%	认证时间	计算机硬件	用户数目	实验环境	
Our work	8.74 4.69 3.33	7.69 4.46 2.12	11.8 秒 59.49 秒 118.14 秒	相同	58	可控	合法用户
Hashia *et al.* [101]	15	15	20 秒	相同	15	不可控	合法用户
Gamboa *et al.* [55]	6.2	6.2	N/A	N/A	50	不可控	合法和非法用户
Bours and Fulla [64]	26.8	26.8	N/A	不同	28	不可控	合法和非法用户
Revett *et al.* [62]	4	4	39.7 秒	N/A	6	不可控	合法和非法用户
Aksari and Artuner [63]	5.9	5.9	N/A	相同	10	可控	合法和非法用户

Revett 等人[62]和 Aksari 等人[63]将鼠标交互行为看作独立的生物特征，并且达到了 4%和 5.9%的 EER（相等错误率），然而他们所采用的行为数据集过小（Revett 等人收集了 6 个用户的数据，Aksari 等人收集了 10 个用户的数据），因此并不能够有力的支持他们的结论。Hashia 等人[101]和 Bours 等人[64]能够在较短的时间内对用户身份进行认证，但是他们的认证错误率却过高（Hashia 等人的方法的 EER 为 15%，Bours 等人方法的 EER 为 26.8%）。

我们的方法能够在相对短的时间内对用户身份进行认证且保持了较好的认证精度。我们采用了单分类的分类器，这更贴切于真实的身份认证场景。我们能够在小于 60 秒的认证时间内达到 4.49%的 FAR 和 4.46%的 FRR。虽然这个结果还没有达到欧洲标准，但在当前的适用范围内，基于鼠标交互行为的身份认证方法能够作为一种传统认证方法的辅助手段。

4.10 结论

本章针对人机交互行为的特征建模问题，从鼠标交互行为的时空轨迹形态分析入手，提出了一种基于光标运动时空轨迹形态特征的身份认证方法。解决了复杂人机交互过程的行为特征刻画问题，建立了用户独特的人机交互行为模型。对于每个交互序列而言，提取描述鼠标交互行为时空轨迹形态变化的特征向量；利用距离度量和成分分析获取低维的鼠标特征量；引入单分类学习器构建身份认证和识别模型。实验结果表明该算法获得了令人鼓舞的认证性能，并对文献中的相关方法进行了比较。

尽管该方法的身份认证结果令人鼓舞，但是样本规模仍然较小，我们正计划创建

一个更大的数据库，以拥有更多的用户、操作和模式等。对于鼠标交互行为，用户间运动轨迹的部分相似性必定会减弱身份认证的效果。因此如何更加细分运动轨迹有可能会进一步提升身份认证的效果。

5 融合鼠标交互轨迹形态特征和运动过程特征的身份认证

5.1 引言

第四章的基于鼠标交互行为时空轨迹形态分析的身份认证方法捕捉了鼠标交互行为的整体化的时空形态特性（比如统计性的操作频数，整体轨迹的速度曲线），特别是运动轨迹的整体形态信息，然而它忽略了交互行为随时间动态变化的过程性信息。鼠标运动轨迹是一种过程性的模式，因此，这里我们有必要进一步探索鼠标交互行为运动轨迹的过程性特性。

鼠标交互过程是一个非常复杂的动态行为，涉及到手部许多基元的运动以及基元之间或手部与计算机之间的交互。是否能够对鼠标运动轨迹进行结构化的刻画决定着鼠标交互行为建模的准确性和有效性。对于鼠标运动轨迹可使用的特性，我们可以将其归类为轨迹形态特征和随时间变化的运动过程特征。形态特征反映了基于几何结构的度量（Geometry-based Measurement），比如运动轨迹长度、偏移量等。相对而言，过程特征对于行为的时间变化比较敏感，比如运动轨迹的加速度变化曲线。前面我们已经对交互行为的形态特性（如第四章）进行了分析，在这里为了进一步提高身份认证的有效性（身份认证精度）和可用性（身份认证时间），我们以鼠标运动轨迹为分析对象，旨在从形态和过程两方面分别对鼠标运动轨迹进行细粒度的、更加准确的刻画，对鼠标交互行为进行更加准确的刻画。

同时，为了获得最优认证性能，一个认证算法应当结合尽可能多的可获得的观察，并且提取尽可能有意义的线索。本章旨在对运动轨迹形态和过程信息分别建模的基础上，提出一种融合鼠标运动轨迹的形态与过程信息的身份认证方法[35,77]，并期望获得更好的性能。

5.2 基本原理

鼠标交互行为的运动轨迹既包含运动轨迹的形态信息，也包含移动过程中的光标运动的细粒度过程性信息。直观上，通过鼠标交互行为进行身份认证很大程度上依赖于鼠标运动轨迹的形态信息；而理论上，基于光标运动轨迹变化的过程性信息进行身份认证是更加充分的。因此，我们期望能够对这两方面的信息分别进行结构化的描述和建模，并融合这两种从不同侧面描述鼠标交互行为的信息，以更加全面和有效的对鼠标交互行为进行表示和刻画。基于上述考虑，我们提出了一种融合鼠标交互轨迹形态特征和运动过程特征的身份认证方法。

图 5-1 给出了该方法的原理图。对于每个鼠标交互行为序列而言，根据运动轨迹的形态特性获得相关的形态信息；形态特征刻画量从这些形态信息提取出来，并且通

过 Box-Cox 特征变换分析方法来获得对形态信息的稳定度量量，即形态特征，它反映了运动轨迹的形态信息。另外，在运动轨迹细粒度过程性信息刻画的思想下，基于近邻传播（Affinity Propogation）的方法进行运动轨迹的动态切分，以获得细粒度的运动轨迹表示；然后从切分的轨迹片段中提取运动过程信息的刻画量，即过程特征，它反映了鼠标运动轨迹的过程性信息。形态特征和过程特征可以分别用来进行身份认证，使用不同的融合规则，我们在判决级上融合它们来提高系统的认证性能。

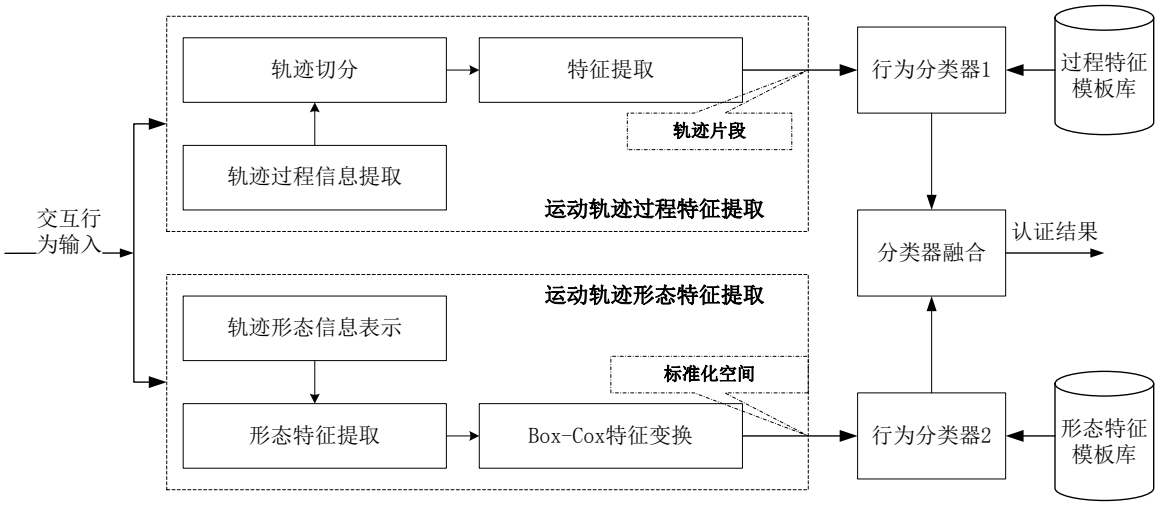


图 5-1 方法的基本流程图

5.3 形态特征提取与建模

5.3.1 形态信息表示

鼠标交互行为一般被描述为在图形用户界面下用户使用鼠标同计算机进行交互所产生的鼠标事件流。在前述认证模式的场景下（见章节 4.3.1），我们首先根据章节 3.4 所述的鼠标输入行为描述方法将鼠标事件流转换为相应的鼠标操作，并根据操作类型分割出了鼠标移动的信息。每一段的移动是由移动点构成的序列，每个移动点由坐标轴和时间戳构成的三元组 (x,y,t) 所表示。例如，一段采样点数目为 N 的鼠标移动可以表示为 $Movement=\{(x_1,y_1,t_1),(x_2,y_2,t_2)...,(x_N,y_N,t_N)\}$。在此基础上，我们定义了不同的鼠标形态特性，这些形态特性包括：距离、偏移量、持续时间。并在这些特性的基础上，对运动轨迹的形态特征进行了提取。

5.3.2 形态特征提取

根据上述的运动轨迹形态特性，提取了如下的运动轨迹形态特征：

移动距离：一段鼠标移动从起始点到结束点之间的距离。令 s 作为认证模式中某段移动的移动距离，我们通过累加在这段移动中每两个相邻的移动点之间的欧式距离得到该距离值。

$$s=\sum_{i=2}^{N}\sqrt{(x(i)-x(i-1))^2+(y(i)-y(i-1))^2} \quad (5\text{-}1)$$

移动偏移量：一段鼠标移动实际移动轨迹和理想移动轨迹（指得是起始点和结束点之间的直线距离）之间的差异距离，表示的是鼠标实际轨迹偏移预定路径的程度。该特征的具体计算过程见章节 4.4.2。

移动持续时间：一段鼠标移动起始点和结束点之间的时间差。该特征的具体计算过程见章节 4.4.2。

5.3.3 特征变换

早期的研究工作表明鼠标的形态特征的分布近似于一种对数正态分布。此外，由于很多行为特征的模型都是以数据的近似正态分布为前提假设，所以对形态特征进行相应的特征变换使其分布近似一种正态分布，能够更好的适应相应的模型并减弱类内的波动。因此，我们采用了一种指数式的特征变换方法以获得鼠标轨迹形态特征的稳定的、近高斯的表征量。

1）特征变换：构建

我们采用 Box-Cox 特征变换方式对形态特征进行变换以提升特征的行为刻画性能。对于某一个用户，她的训练样本集表示从她所有的形态特征向量样本中随机选择出的部分样本的集合。令 $F=\{f_{ij}\}_{n\times m}$ 作为该用户的训练样本，其中 f_{ij} 表示第 i 个特征向量的第 j 个分量，m 和 n 分别表示该向量中特征分量的个数和训练样本中特征向量样本的个数。Box-Cox 特征变换构建的目的是利用训练数据推理出参量 $\boldsymbol{\lambda}=\{\lambda_1,\lambda_2,\ldots,\lambda_{m-1},\lambda_m\}$，在这里我们采用最大似然估计的方法（Maximum Likelihood Method）。Box-Cox 变换的方式有很多种，我们定义了如下的变换模型：

$$y_{ij}=\begin{cases}\dfrac{f_{ij}^{\lambda_j}-1}{\lambda_{ij}}, & if\ \lambda\neq 0\\ \log(f_{ij}^{\lambda_j}) & if\ \lambda=0\end{cases},\ i=\{1,2,...,n\},\ j=\{1,2,...,m\} \quad (5\text{-}2)$$

令 $f_j=\{f_{ij}\}_{n\times 1}$ 和 $y_j=\{y_{ij}\}_{n\times 1}$ 分别表示第 j 个特征和对应于第 j 个特征的变换量。

假设变换的特征服从如下的分布：

$$y_j(\lambda)\sim N(\mathrm{X},\beta_j,{\sigma_j}^2\mathrm{I}_n) \quad (5\text{-}3)$$

我们的目的是获得设计矩阵 X 和相应的参数 $(\lambda_j,\beta_j,{\sigma_j}^2)$。令 $J(\lambda,y_j)$ 作为从 f_j 变换到 y_j 的 Jacobian 矩阵，那么 y_j 的似然估计如下：

$$L(\lambda_j,\beta_j,{\sigma_j}^2\mid y_j,\mathrm{X})=\frac{\exp(-\frac{1}{2\sigma^2}(y_j-\mathrm{X}\beta_j)'(y_j-\mathrm{X}\beta_j))}{(2\pi\sigma^2)^{\frac{n}{2}}}J(\lambda_j,y_j) \quad (5\text{-}4)$$

接着，对参数(β_j,σ_j^2)计算其最大似然估计量：

$$\tilde{\beta}_j = (\mathrm{X}'\mathrm{X}) - \mathrm{X}y_j$$
$$\hat{\sigma}_j^2 = \frac{y_j'(\mathrm{I}_n - G)y_j}{n} \quad (5\text{-}5)$$

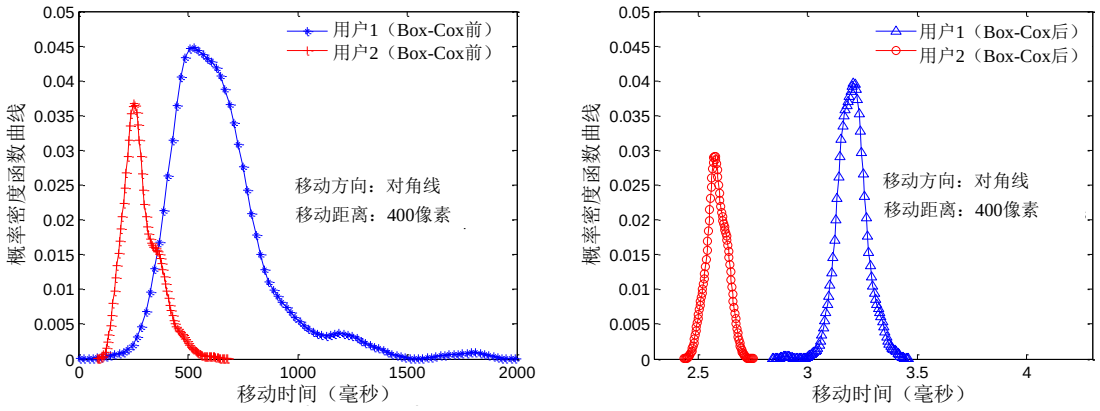
其中$G = \mathrm{X}(\mathrm{X}'\mathrm{X}) - \mathrm{X}'$。

然后通过求解使公式（5-4）最大化的参量 $\boldsymbol{\lambda}$。关于参量 $\boldsymbol{\lambda}$ 的详细求解过程，可参见[131]。

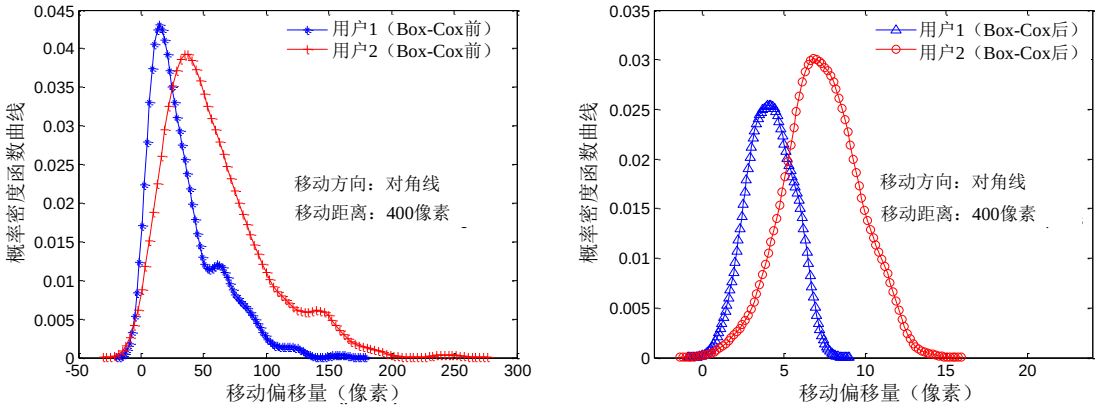
2）特征变换：投影

根据得到的该用户的特征变换参数 $\boldsymbol{\lambda} = \{\lambda_j\}_{1\times m}$，对于新的特征向量 f_{new}，我们通过公式（5-2）可以计算其投影变换向量。需要说明的是，对特征向量中所有 m 个特征进行变换的计算复杂度仅为 $O(mn)$，这是因为使用了似然函数对 Box-Cox 变换的参数 $\boldsymbol{\lambda}$ 进行最优求解，该步骤的算法复杂度为 $O(m)$。

5.3.4 形态特征变换的实验分析



(a) Box-Cox 变换前后移动时间的概率密度函数估计



(b) Box-Cox 变换前后移动偏移量的概率密度函数估计

图 5-2　Box-Cox 变换前后运动轨迹形态特征的概率密度函数估计

为了进一步分析经过特征变换后形态信息刻画量的稳定性和区分性，我们使用了一种非参数的随机变量的概率密度估计方法-核密度估计（Kernel Density Estimation）的方法-来计算经过变换得到的形态特征表征量的概率密度函数[128]。我们从数据集中随机选取了 150 个样本对每个特征的概率密度函数进行计算。图 5-2 展示了两个用户的几个典型特征的概率密度函数对比情况。

从上图可以观察到经过 Box-Cox 变换得到的形态特征表征量的概率密度函数表现的更为紧凑，这说明变换后的特征表征量能够提供更为稳定的运动轨迹形态特性描述。此外，我们也观察到不同用户的变换后的特征表征量的概率密度函数之间存在在明显的区分。这说明变换后的形态特征具有更好的区分能力。作为对比，图示的两个不同用户的变换前的形态特征概率密度曲线有着较大的重叠区域，这意味着较难对两个用户进行区分。

结合上述对形态特征稳定性和区分性的分析，这些结果说明 Box-Cox 变换后的形态特征空间优于原始的形态特征空间。同时我们可以看出变换后形态特征的概率密度曲线能够展现出更加明显的正态特性，这说明 Box-Cox 变化将可能对基于统计的分类器产生更好的适应性，以建立更加准确的身份认证模型。

5.4 过程特征提取与建模

5.4.1 运动轨迹过程特性分析

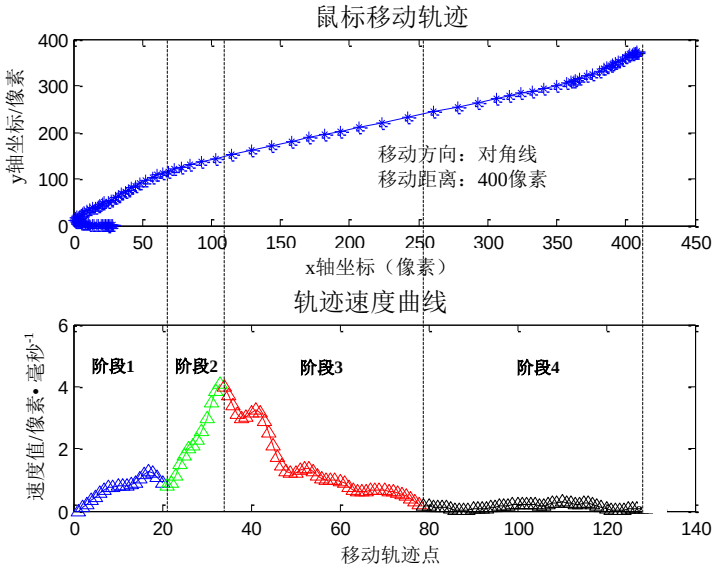


图 5-3 一段鼠标移动的切分过程

通过对鼠标运动轨迹的初步分析，我们发现用户的一些鼠标移动片段（来自于某段移动的一部分）在该用户的不同样本之间呈现出一定的连续性和稳定性。通过对鼠标移动产生的物理过程的深入分析，我们发现鼠标移动在时间上具有保序性的特点，

一段完整的鼠标移动可以被分割为若干个小的移动阶段。如图 5-3 所示，以用户的鼠标对角线移动为例（移动距离为 524 像素），我们可以将这段鼠标移动轨迹划分 4 个移动片段（对应于 4 个移动阶段）：第一阶段，用户从开始位置出发，速度从零开始增加，称为启动阶段；第二阶段，用户开始加速移动，速度增加到某一个值，称为加速阶段；第三阶段，用户开始减速，逐渐接近目标，称为减速阶段；第四阶段，用户调整光标位置以到达指定区域或点击区域内的目标，最后速度降为 0，称为结束阶段。

更进一步，我们发现从用户移动片段中提取出的特征测量量相比于从整体移动中提取出的特征测量量具有更好的稳定性和可区分性。这是由于对鼠标移动的物理过程进行了分析而得到更加细粒度的行为片段，对鼠标整体移动进行了更加准确的刻画，形成了一种对鼠标运动轨迹的过程性描述方法。

5.4.2 运动轨迹切分

输入: 一段任意的鼠标移动$P = \{p_i\}_{1\times n}$, 其每个移动点的移动距离为s_i, 移动速度为v_i.
输出: 一个样板点集合C_P^*和该移动的移动片段集合.
方法: *MouseMovmentSegmentation*()

调用 *MouseMovementSegmentation* (<>, *S*, ξ)
begin
(1) 针对移动*P*中每对数据点计算出测地距离矩阵D_p
(2) 生成相似度矩阵Sim_p，它是测地距离矩阵的负值
(3) 对所有的数据点，初始化数据点之间的两种传递信息$r(i,k) = 0$, $a(k,i) = 0$
(4) **for** *time* = 1 to *m* do (m是迭代的最大次数)
(5) 更新责任度信息$r(i,k)$和可用度信息$a(k,i)$
(6) 识别出样板点集合和相应的移动分段集合
(7) **if** $|a_{time+1} - a_{time}| < \varepsilon_a$ and $|r_{time+1} - r_{time}| < \varepsilon_r$
(8) 返回样板点集合和相应的移动分段集合
(9) **else if** 样板点集合和相应的移动分段集合在T_p迭代中保持不变
(10) 返回样板点集合和相应的移动分段集合
(11) **else**
(12) 继续下次迭代 *time* ← *time* + 1
(13) **end if**
(14) **end for**
(15) **for** 在该移动中的移动片段
(16) **if** 两个数据点在某个移动片段分界出的两边并且在时间上是不连续的
(17) **if** 其中只有一个点的S_{il} **(**轮廓宽度测量量) 值为负
(18) 重新归类这个点到另一个最近邻的片段
(19) **else if** 两个点的S_{il} (轮廓宽度测量量)都为负值
(20) 归类S_{il}值小的数据点到另一个最近邻的片段
(21) **end if**
(22) 计算修订后的移动片段的S_{il} 值
(23) **if** S_{il} 值变小
(24) 拒绝这次修订
(25) **end if**
(26) **end if**
(27) **end for**
end begin

图 5-4 鼠标移动轨迹切分算法

现有的研究在描述鼠标运动轨迹的过程性特性时都是对整体的移动轨迹进行刻画，从而致使稳定的和可区分的测量量淹没在整体移动行为中，这会导致较低的认证精度。因此，基于章节 5.4.1 的分析，我们提出一种基于近邻传播的相似移动轨迹片段聚类方法[129]来对鼠标移动轨迹进行切分，从而获得细粒度的移动轨迹表示方法。该方法的基本思想是迭代利用数据点之间的相似度距离来对数据类别进行划分，直到得到高质量的样板点集合。所提出的算法如图 5-4 所示，下面我们详述了该方法。

1）轨迹切分方法

令 $P=\{p_1,p_2,...,p_n\}$ 表示一段鼠标移动，其中 p_i 是该移动中的第 i 个数据点，n 是该段移动中数据点的数目。轨迹切分算法流程图如图 5-5 所示。

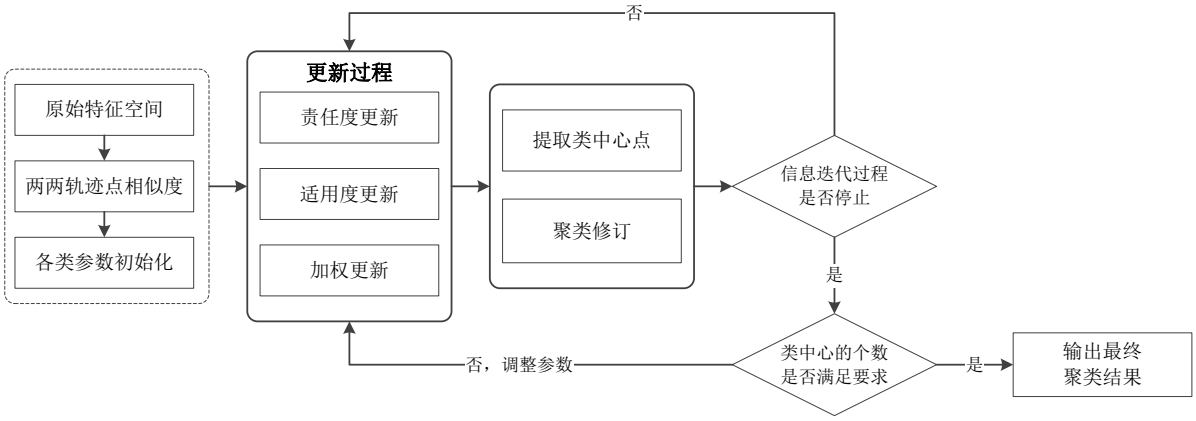


图 5-5 轨迹切分方法流程图

第一步是计算每两两移动点之间的相似度值。首先根据简单性、有序性和计算有效性采用了移动距离 s_i 和移动速度 v_i 对每个移动点进行刻画（移动距离和移动速度的计算可参见章节 4.4.2）。然后计算了每两两点之间的测地距离，在这里我们定义的测地距离是由移动 P，距离函数 $d_{ISO}(.,.)$和近邻参数 k 构成的，如下式所示：

$$D(p_u,p_v)=\min_{q}\sum_{i=1}^{|q|-1}d_{ISO}(q_i,q_{i+1}) \tag{5-6}$$

其中 q 是一个长度 $|q|=l\geq 2$ 的数据点序列，其中 $q_1=p_u$，$q_l=p_v$，$q_i\in P,$，$\forall i\in\{2,...,l-1\}$。此外 (q_i,q_{i+1}) 是彼此的 k 近邻点。

接下来设定两两点之间(p_i, p_k)相似度 $Sim(i,k)$ 值为测地距离的负值，这个值反映了点 p_k 作为点 p_i 的样板点的合适度程度的大小。生成的相似度矩阵的对角线上的数值表示该数据点的自相似系数，也称为偏向参数（*preferences*）。对每一个数据点来说，偏向参数刻画了该点能够成为一个移动片段的样板点的倾向度，同时移动分段的数据也会受到偏向参数值大小的影响。在这里，将所有的移动点能够作为聚类中心点的概率设定为同一个固定的值。

接下来，使用两类聚类结构信息进行移动数据点之间的信息传递以形成不同的移动分段，这两类信息是：责任度信息（Responsibility）和适用度信息（Availablity）。责任度 $r(i,k)$ 是从一个类中成员 i 传送到候选的聚类中心点 k 的信息，表示数据点 i 选择数据点 k 作为聚类中心的合适程度。适用度 $a(i,k)$ 是从候选的聚类中心点 k 传送到可能的类成员 i 的信息，表示候选的聚类中心点 k 作为点 i 的聚类中心点的合适程度。

首先对这两类信息进行初始化，将责任度矩阵 R 和适用度矩阵 A 都赋值为 0：

$$a(i,k)=0, r(i,k)=0,\ \ i,k \text{ 为任意点} \tag{5-7}$$

然后对这两种结构化信息进行迭代式的更新，移动点点 i 的责任度 $r(i,k)$ 的更新综合利用相似度信息和其他点对 i 的适用度信息，

$$r(i,k) \leftarrow Sim(i,k) - \max_{k',k' \neq k} \{a(i,k') + Sim(i,k')\} \tag{5-8}$$

在第一次迭代中，因为适用度 $a(i,k)$ 是 0， $r(i,k)$ 被设置为点 i 和聚类中心点 k 之间的相似度减去数据点 i 和其他候选聚类中心点的相似度的最大值。这个信息更新的过程是由相似度和适用度信息决定的，没有考虑各点自身作为聚类中心点的偏向参数。下一次迭代中，当某些点被分配给其他聚类中心点，按照近邻传播的更新规则，它们的适用度 $a(i,k)$ 将会减小到小于 0。按照上述规则，这些负的适用度将会减小输入相似度 $s(i,k')$，降低对应的候选聚类中心点 k 被选中为 i 的聚类中心点的合适程度，

$$r(k,k) = p(k) - \max_{k' \neq k} \{a(k,k') + s(k,k')\} \tag{5-9}$$

对于 $k=i$ 的情况，责任度 $r(k,k)$ 设置为输入的 k 被选择为聚类中心点的预置偏向参数 $p(k)$ 减去点 k 和其他候选聚类中心点间的相似度的最大值。这个责任度反映了点 k 是聚类中心点的累积信息，它基于输入的偏向参数，并在后续信息更新过程中作为调整点 k 被分配给其他聚类中心点的合适度的依据。

在一次信息更新中，使用了适用度信息更新责任度信息后，接着使用责任度来更新适用度，

$$a(i,k) = \min\{0, r(k,k) + \sum_{i' \neq i} (\max\{0, r(i',k)\})\} \tag{5-10}$$

适用度 $a(i,k)$ 设置为自责任度 $r(k,k)$ 加上候选聚类中心点 k 从其他点接收的正的责任度之和。这里只加上了正的责任度，因为聚类中心点只要能够很好地代表一些数据点（正责任度），那它就是一个好的聚类中心点，不管它和其他的点如何无关（负责任度）。如果自责任度 $r(k,k)$)是负的，说明点 k 属于其他的聚类中心点代表的类别比它自己作为一个聚类中心点要合适。在有些点对于数据点 i 作为他们的聚类中心点有正的责任度的情况下，k 作为聚类中心点的适用度会增加。为了限制正责任度的影响，对两部分数据的总和设置一个阈值，使得它不会变得大于 0。自适用度的更新规则如下，

$$a(k,k) = \sum_{k' \neq k} \max\{0, r(k',k)\} \tag{5-11}$$

在该方法的任意一次迭代过程的最后，可以综合适用度和责任度信息来识别基于当前的信息下的聚类中心点和类的划分。停止信息传递的过程可以使用以下判定条件：达到事先规定的最大迭代次数；或者信息的改变下降到一个阈值以下；或者聚类中心点和聚类的划分在收敛迭代次数的迭代中保持不变。对于点 i，使得 $a(i,k)+r(i,k)$ 最大的 k 的值，如果 $k=i$，那么 i 就是一个聚类中心点；如果 $k\neq i$，那么 k 就是点 i 的聚类中心点。

$$c_i^* \leftarrow \arg\max_k \{r(i,k)+a(i,k)\} \qquad (5\text{-}12)$$

2）轨迹片段边界修订

在上述的轨迹切分完成之后，我们发现有些处于分段边界处数据点会产生错误的划分，因此它们在原始轨迹中是明显不应属于这个分段的。分析其原因可能是由于轨迹划分时的依据是点和样板点之间的相似度，而没有考虑每个移动片段整体的聚类特性及分段完成后相邻点之间的相似度，因此会导致不准确和不稳定的划分。针对这个问题，提出了一种轨迹片段边界点的修订方法。采用了一个简单和有效的测量量-轮廓宽度（Silhouette Width[130]）-对每个移动数据点在当前分段中的合适度进行度量。若测试的移动点的轮廓宽度值为 1 时，指明该数据点以接近于 1 的概率划分到这个类别中；若测试的移动点的轮廓宽度值为-1 时，指明该数据点以接近于 1 的概率不应被划分到这个类别中。对于每个移动数据点 p_i，其轮廓宽度值被定义为，

$$S_{il}(p_i)=\frac{b(p_i)-g(p_i)}{\max\{g(p_i),b(p_i)\}},$$
$$b(t)=\min\{d(p_i,C_j^*)\}$$

其中 $g(p_i)$是点 p_i 针对于其它与其属于同一个类别 $p^{C_i^*}$ 中的数据点的平均不相似度值，$d(p_i,C_j^*)$ 点 p_i 针对于其它与其不属于同一个类别 $p^{C_j^*}$ 中的数据点的平均不相似度值。

根据对轨迹片段边界的移动点得到的轮廓宽度值，设计了如下的边界点修订方法：

第一步，对位于一个边界两边的数据点 p_i 和 p_{i+1}（例如，p_i 位于边界左边，p_{i+1} 位于边界右边），如果只有其中一个点的 S_{il} 值为负，那么将这个点重新划分到边界的另一边；如果两个点的 S_{il} 值都为负，那么就将 S_{il} 值小的那个数据点划分到边界的另一边。

第二步，重新计算经过修订的整个移动片段的 S_{il} 值，如果 S_{il} 值增加，接受这次修订；反之，拒绝这次修订。

第三步，对边界两旁的新的数据点重复上述的步骤，直到修订被拒绝。

第四步，对所有的边界重复上述步骤，完成之后就可以获得最终的移动轨迹分段。

3）参考样板点的生成和比较

当应用该方法进行鼠标移动轨迹切分时，需要使用训练样本对每个用户生成一个参考样板点集来表示其每段移动的分段中心点，具体的步骤如下：

第一步，将该用户一个鼠标行为样本中的所有移动按照上述的方法进行切分，得

到相应的移动分段集合；

第二步，从每个移动分段中识别出该分段的样板点，形成样板点集；

第三步，对该用户的所有鼠标行为样本重复上述的步骤得到平均样板点集，并以此作为该用户的参考样板点集。

需要注意的是该方法可以自动得到每个用户样板点的数目，不需要预先进行指定。具体来说，对于实验的所有 58 个用户，每段移动的样板点个数在 3 到 7 之间。

接着，根据生成的参考样板点集，针对新的鼠标行为样本，使用如下的步骤获得该行为样本的移动分段集：

第一步，对样本中的每段移动，计算移动数据点和参考样板点之间的相似度；

第二步，对每个移动点，根据每个数据点与样板点之间的相似度的最大值对数据点进行划分；

第三步，对划分的数据点进行组合，形成新的行为样本的移动分段集。

5.4.3 过程特征提取

针对每个行为样本，我们从行为样本对应的移动分段集中提取出了相应的过程性特征，相比于整体行为的动态特征（见章节 4.4.2），该特征更加细粒度和准确的对鼠标运动轨迹进行了描述。针对每个行为分段提取了如下的特征：

水平方向速度：行为分段中每个数据点的水平方向移动速度；

垂直方向速度：行为分段中每个数据点的垂直方向移动速度；

运动方向速度：行为分段中每个数据点的运动方向移动速度

水平方向加速度：行为分段中每个数据点的水平方向移动加速度；

垂直方向加速度：行为分段中每个数据点的垂直方向移动加速度；

运动方向加速度：行为分段中每个数据点的运动方向移动加速度；

水平方向路程速度：水平移动距离与累积移动距离的比值；

垂直方向路程速度：水平移动距离与累积移动距离的比值；

路程平均速度：平均移动距离与累积移动距离的比值；

水平方向路程加速度：水平移动速度与累积移动距离的比值；

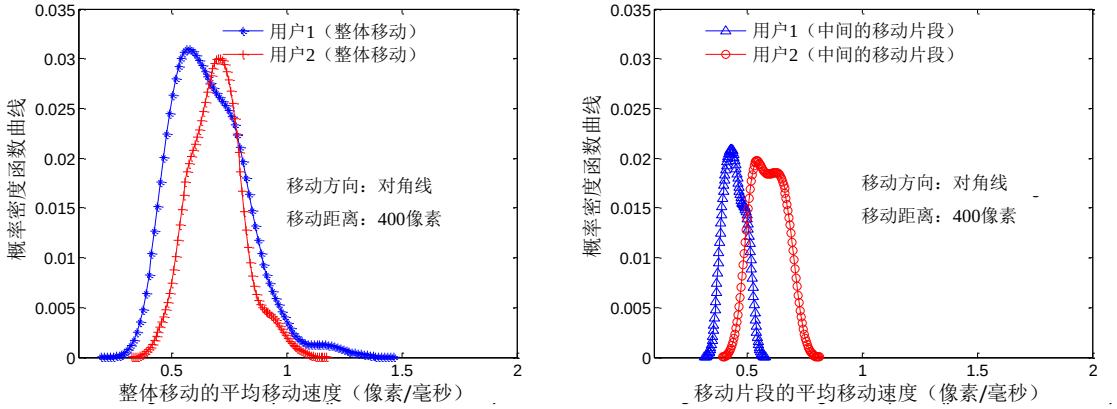
垂直方向路程加速度：水平移动速度与累积移动距离的比值；

路程平均加速度：平均移动速度与累积移动距离的比值。

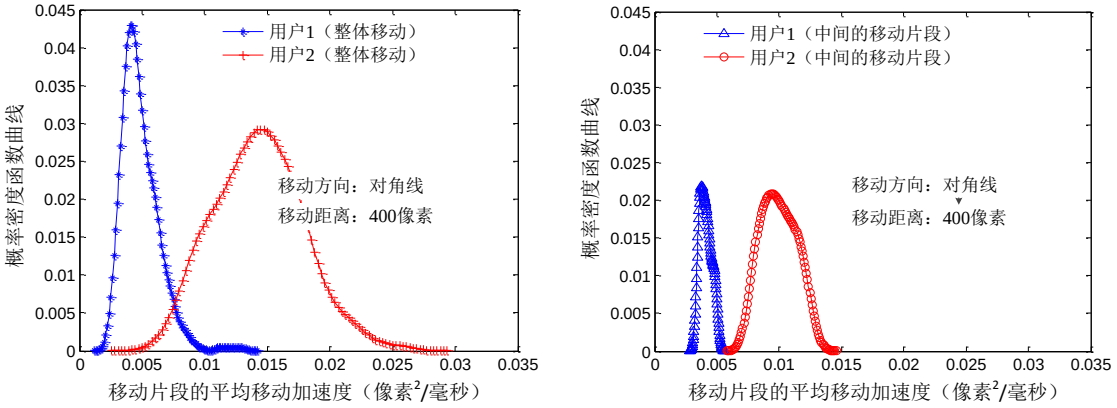
5.4.4 运动轨迹切分的实验分析

为了进一步验证行为轨迹切分方法的有效性从移动轨迹分段中提取出的行为刻画量的稳定性和可区分性，这里我们采用了核密度估计（Kernel Density Estimation）[128]的方法计算从轨迹行为分段中提取的过程特征的概率密度函数，并将其与整体轨迹中提取出的过程特征的概率密度函数进行对比分析。我们从数据集中随机选取了 150 个样本对每个特征的概率密度函数进行计算。图 5-6 展示了两个用户几个典型特征的概率密度函数对比情况。

通过比较在（a）或（b）中的两幅图形，我们发现从移动轨迹片段中提取的特征概率密度曲线相比于从整体轨迹中提取出的特征概率密度曲线表现的更加集中，这说明轨迹切分方法能够更加准确和稳定地对运动轨迹的过程特性进行刻画。我们也观察到两个不同用户的整体移动提取出的特征概率密度曲线有着较大的重叠区域，这会使得分类器难以对两者进行区分。相比之下，两个不同用户的轨迹分段提取出的特征概率密度曲线之间有着明显的不重合，这说明从轨迹分段中提取的过程特征具有更好的区分能力。上述结果说明轨迹切分方法能够生成更准确和稳定的运动轨迹刻画量，可能会提高身份认证的准确率。



(a) 整体移动和移动分段下移动速度的概率密度函数估计



(b) 整体移动和移动分段下移动加速度的概率密度函数估计

图 5-6 整体移动和移动分段下运动轨迹过程特征的概率密度函数估计

5.5 分类器

5.5.1 形态信息的分类器：最近邻分类器（马氏距离）

相关领域的研究结果表明使用 Box-Cox 变换和最近邻分类器结合的方法可以产生较好的分类识别结果[131]，因此我们采用了基于马氏距离的最近邻分类器对经过 Box-Cox 变换后的形态特征进行建模。

在训练过程中，我们在训练数据集上计算出协方差矩阵，同时保存训练数据的每组行为特征向量。经过在训练集上的多次测试，我们选择最近邻参数 k 的数值为 3。在测试阶段，计算出测试样本到训练样本的马氏距离（Mahalanobis distance），然后将该测试样本到最近邻样本的距离作为该样本的检测值。

5.5.2 过程信息的分类器：单分类支持向量机

类似于章节 4.7.2 所述，我们采用单分类支持向量机对从轨迹分段集提取出的过程特征进行建模。在训练阶段，学习任务是基于合法用户的特征样本建立一个分类器。在测试阶段，测试样本被映射到相应的高维空间中，决策函数的输出被记录下来。这里我们使用放射基函数（RBF） $k(\mathbf{x}_i,\mathbf{x}_j)=\exp(-\gamma\left\|\mathbf{x}_i-\mathbf{x}_j\right\|^2),\gamma>0$ 进行高维空间的映射，支持向量机的参数 ν 和核参数 γ 被分别设定为 0.01 和 0.02。如果输入的是合法用户的测试集，决策函数应输出”+1”，否则将作为一个误拒的实例。相反，如果输入的是非法用户的测试集则决策函数应输出”-1”， 否则将作为一个误纳的实例。

5.6 融合规则

5.6.1 信息融合研究

信息融合是通过对多源信息的综合处理来得到更完整、可靠、客观的有用信息。信息融合按其处理的层次不同可分为特征级（Feature-based）和决策级（Decision-based）两个层次。特征级融合需要先提取特征，然后再对特征信息加以综合分析和处理。其优点是能够保留一定的原始信息，且有利于实时处理。决策级融合是最高层次的融合，它需要以各个信源关于目标的确定性结论为依据来做出最后的决策。

这里我们简单回顾一下在身份认证中的信息融合研究。通过多生物特征或者生物自身的多个特征融合，可在提高准确率和扩大应用范围两方面提高身份认证系统的性能。融合系统是用一定的算法将不同的生物特征识别结果结合起来进行决策。在分类器融合研究中，一个有意思的课题就是它们被组合的方法。如果仅仅标号是可获得的话，那么投票规则可以被使用。如果后验概率输出可以获得的话，均值或者线性组合可以被考虑。许多不同的分类器组合规则已被设计，并且实验上已经验证其中部分规则一致上远胜过任何单一的最好的分类器[132-135]。例如 Srisuk 等人[132]将人脸的形状和纹理信息结合起来进行身份认证，在提高身份认证准确率的同时缩短了认证时间；Kittler 等人在结合人脸的侧面、正面以及声纹识别时，提出了融台理论框架并将其分为三层，同时比较了加法准则和乘法准则等算法在融合中的优缺点[134]。可以用来进行身份识别的融合算法除了一般通用的融合算法，如 Bayes 理论和模糊积分等以外，模式识别中的分类器也可以用来进行信息融合，如决策树和神经网络等[135]。

5.6.2 分值变换

在给定每个模态的观察下，可以获得了每个模型的匹配分值，但一般而言是不能直接用一种统计意义上的方式直接将这些分值进行组合[134]。鼠标行为认证的分类器产

生的分值通常不是后验概率的直接估计，而是测试样本与合法用户匹配的参考特征向量的距离度量。这些匹配分值，拥有不同的范围和分布，因此必须被转换。

我们采用了 Logistic 变换进行分值变换，该变换是单调函数，所以不会影响分类器的 Rank 次序。这是一个理想的特性，因为任何 Rank 次序的修改都只应当发生在组合阶段。Logistic 变换可描述为：

$$\hat{x} = \frac{e^{(\alpha+\beta x)}}{(1+e^{(\alpha+\beta x)})} \tag{5-13}$$

5.6.3 融合规则

在鼠标交互行为的身份认证过程中，当给定一个测试样本时，根据前述的模型，会得到两个身份认证的结果：形态信息的认证结果 $F_{hol}(k)$和过程信息的认证结果 $F_{pro}(k)$。应用不同的融合规则 $f(.,.)$，我们可以得到最终的认证结果：

$$\begin{aligned} &f(F_{hol}(k), F_{pro}(k)) \approx P(\omega_1 \mid (F_{hol}(k), F_{pro}(k))), \\ &f(F_{hol}(k), F_{pro}(k)) \geq \zeta_k \Rightarrow accepted. \end{aligned} \tag{5-14}$$

在这里，我们观察了如下几种不同的组合方式来进行分类器的融合：常用的分类器融合规则[135]（例如乘法规则和加法规则），加权的加法规则，基于神经网络的规则。我们将上述融合规则应用于鼠标行为的身份认证问题，其形式如下：

1）常用的分类器融合规则

乘法规则：

$$f(F_{hol}, F_{pro}) = F_{hol} \times F_{pro} \tag{5-15}$$

加法规则：

$$f(F_{hol}, F_{pro}) = F_{hol} + F_{pro} \tag{5-16}$$

最大值规则：

$$f(F_{hol}, F_{pro}) = \max(F_{hol}, F_{pro}) \tag{5-17}$$

最小值规则：

$$f(F_{hol}, F_{pro}) = \min(F_{hol}, F_{pro}) \tag{5-18}$$

2）加权加法规则

在鼠标交互行为的身份认证中，运动轨迹的形态信息和过程信息所表示的用户身份信息可能会有不同，所以我们对不同的分类器结果赋予不同的权值。我们结合每个分类器得到的 FAR 和 FRR 值，提出了如下的加权加法规则：

$$\begin{aligned} &f(F_{hol}, F_{pro}) = W_{hol} F_{hol} + W_{pro} F_{pro}, \\ &W_{hol} = \frac{1-(FAR_{hol} + FRR_{hol})}{2-(FAR_{pro} + FRR_{pro} + FAR_{hol} + FRR_{hol})}, \\ &W_{hol} + W_{pro} = 1. \end{aligned} \tag{5-19}$$

3）基于神经网络的融合规则

在基于神经网络的融合规则中，我们将每个单独的分类器的输出组合在一起，形成了一个新的特征向量 $F=(F_{hol},F_{pro})$，作为神经网络的输入，将神经网络的输出作为最终的身份认证结果。这里采用了三层神经网络结构，包含 2 个输入节点，1 个输出节点和 4 个隐层节点。

5.7 实验结果与分析

5.7.1 数据集

与章节 4.3.1 所述的鼠标行为模式不同的是，在这里的操作模式由前 8 次的鼠标移动构成。在每次行为模式的采集中，我们要求用户只完成前 8 次的鼠标移动操作，形成一个行为交互样本。58 个用户参与了该认证实验，每个用户采集了 300 个行为交互样本，总共提供了 17400 个行为交互样本。

5.7.2 实验 1：单一特征的身份认证

在本实验中，我们分别使用运动轨迹的形态特征和过程特征进行身份认证。图 5-7 和表 5-1 展示了身份认证实验的 FAR、FRR 及 ROC 曲线，表 5-1 括号内的数值表示相关 FAR 和 FRR 值的标准差。表 5-1 也包含了平均的认证时间。

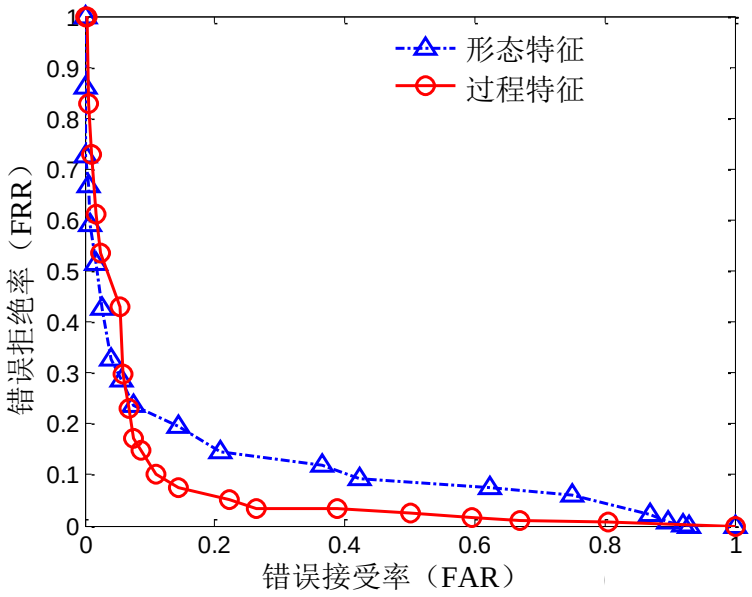


图 5-7 分别使用形态和过程特征的身份认证结果的 ROC 曲线

表 5-1 分别使用形态和过程特征身份认证结果的 FAR 和 FRR 值（括号内为对应的标准差）

特征类别	FAR/%	FRR/%
形态特征	15.83 (9.79)	16.92 (10.76)
过程特征	7.71 (5.64)	8.43 (6.21)
平均认证时间： 6.1 秒		

从图 5-7 和表 5-1 中我们观察到使用形态特征的身份认证结果为 15.83%的 FAR 和 16.92 %的 FRR，而使用过程特征的身份认证结果为 7.71%的 FAR 和 8.43 %的 FRR。虽然没有达到很好的认证结果，但这些结果再次证明了鼠标交互行为中确实存在可用于身份认证的信息。此外，我们发现过程特征的身份认证结果要优于形态特征的身份认证结果。我们推测这是由于经过切分的轨迹分段的过程特征能够更加细粒度和有效的对原始轨迹进行表示和描述，从而准确的刻画用户交互行为习惯的细节信息。我们也同时观察到过程特征身份认证结果的标准差要远小于形态特征认证结果的标准差，这也从另一个侧面反映了轨迹分段中过程特征的稳定性和鲁棒性。

5.7.3 实验 2：融合特征的身份认证

在本实验中，我们使用了不同的融合规则对交互行为运动轨迹的形态信息和过程信息进行了融合并进行了相关的身份认证实验。图 5-8 和表 5-2 展示了身份认证实验的 FAR、FRR 及 ROC 曲线，表 5-2 括号内的数值表示相关 FAR 和 FRR 值的标准差。表 5-2 也包含了平均的认证时间。

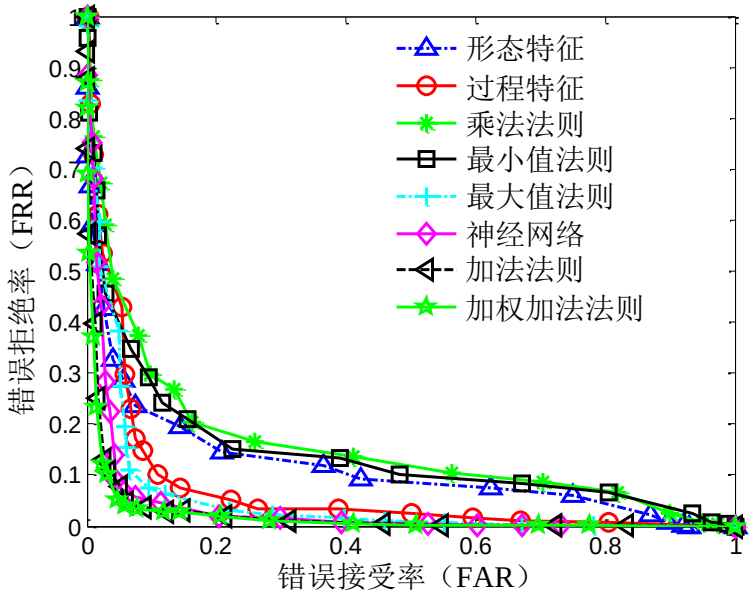


图 5-8 不同融合规则的身份认证结果的 ROC 曲线

从图 5-8 和表 5-2 的实验结果中，我们可以看出最好的认证结果为 4.18%的 FAR 和 4.96%的 FRR，认证时间为 6.1 秒，是基于加权加法规则得到的。对比于第四章得到的身份认证结果，身份认证性能提高了一倍以上（第四章所述方法的认证精度为 8.74%的 FAR 和 7.96%的 FRR，认证时间为 11.8 秒），明显优于现有文献中的基于鼠标交互行为的认证结果。

我们观察到基于加权加法融合规则的身份认证性能要明显优于单独使用任何一种

信息。这是由于我们对运动轨迹信息进行了细粒度的刻画，从形态和过程信息对其分别进行建模，同时结合了融合规则，有效的提升了认证性能。在四个融合规则中，“和”规则也是最好的，这在文献[135]中已经指出：“和”规则能够最为有效地对估计误差进行抵制。

表 5-2 不同融合规则的身份认证结果的 FAR 和 FRR 值（括号内为对应的标准差）

融合规则	FAR/%	FRR/%
乘法规则	17.83 (11.86)	19.35 (13.21)
最小值规则	17.01 (11.75)	18.91 (12.69)
最大值规则	6.52 (5.48)	7.23 (6.02)
神经网络	5.85 (5.26)	6.42 (5.72)
加法规则	4.33 (4.58)	5.32 (5.12)
加权加法规则	4.18 (3.87)	4.96 (4.83)
平均认证时间: 6.1 秒		

此外，不同信息之间的相关性越低，融合后的身份认证准确率就越好。我们的两种特征分别从形态和过程两个侧面对鼠标运动轨迹进行了刻画，因为运动轨迹的整体形态信息和轨迹切分后的过程信息的关联度很小，这是基于融合规则的方法能得到很好的认证性能的首要原因。

对于最差性能的乘积规则而言，它比相对不敏感的均值和加法规则更易受分值分配噪声的影响。总之，这些现象表明了合理选择组合规则的重要性。当然，我们也相信，对于两个模式分类器而言，如果有足够的数据来建模分值的概率分布，统计规则会得到更好的识别结果。

最后，我们使用了 HTER 和置信区间对得到的认证结果进行相应的统计结果分析。实验结果的对比表明基于加权加法规则融合形态和过程信息的方法能够得到最低的 HTER。在 95%的置信区间下，该方法能够达到的认证错误率为 4.57% ±1.62%。

5.7.4 实验 3：Box-Cox 对认证结果的影响

本实验检验了 Box-Cox 变换的应用对认证精度的影响。我们使用章节 5.5.1 所述的最近邻分类器建立身份模型，对采用和不采用 Box-Cox 变换的身份认证结果进行了分析。表 5-3 呈现了相应的身份认证结果。我们可以观察到采用 Box-Cox 变换的身份认证精度及其对应的标准差都要明显优于不采用 Box-Cox 变换的结果。这个结果证实了 Box-Cox 变换在鼠标运动轨迹的形态特征建模中的有效性。Box-Cox 变换降低了鼠标交互行为误差的不可加性，并增强了数据的正态性。

表 5-3 采用和不采用 Box-Cox 变换基于形态特征的身份认证结果的 FAR 和 FRR 值

形态特征	FAR/%	FRR/%
不采用 Box-Cox 变换	19.72 (13.58)	22.78 (15.67)
采用 Box-Cox 变换	15.83 (9.79)	16.92 (10.76)

5.7.5 实验 4：行为切分对认证结果的影响

本实验检验了轨迹切分方法的应用对认证精度的影响。我们使用了章节 5.5.2 所述的单分类支持向量机建立身份模型，对采用和不采用轨迹切分的身份认证结果进行了对比分析。表 5-4 呈现了相应的身份认证结果。我们可以观察到采用轨迹切分方法的身份认证结果及其对应的标准差都要明显的优于不采用轨迹切分的方法，并且其对应的 FAR 和 FRR 有很大的提升。将鼠标移动轨迹依据其物理运动过程切分为多个阶段的短距离移动能够更加有效和细粒度的对鼠标运动轨迹的过程性信息进行准确的刻画，从而提取出区分性更好的过程特征量。

表 5-4 采用和不采用轨迹切分的基于过程特征的身份认证结果的 FAR 和 FRR 值

过程特征	**FAR/%**	**FRR/%**
不采用轨迹切分	15.24 (12.63)	15.38 (11.79)
采用轨迹切分	7.71 (5.64)	8.43 (6.21)

5.8 结论

针对人机交互行为的行为结构化描述问题，本章旨在从鼠标移动轨迹的形态和过程两个方面对运动轨迹进行细粒度的分析和建模。此外，为了获得最优认证性能，提出了一种融合鼠标移动轨迹形态和过程信息的身份认证方法。形态和过程特征线索可以分别进行身份认证。我们也在判决级上融合它们以提高身份认证和验证性能的准确度。实验结果验证了方法的有效性。尽管实验结果是令人鼓舞的，大量的工作仍需要进行，如提高轨迹切分算法的可靠性、设计更好的组合规则、创建更大的评估数据库等。

6 基于鼠标频繁交互行为模式挖掘的身份监控

6.1 引言

前两章分别介绍了两种在计算机系统登录场景下的基于鼠标交互行为的身份认证方法，然而鼠标交互行为的更大优势在于鼠标能够在用户成功登录系统后持续性的进行交互，因此可以利用鼠标交互行为在计算机系统的使用过程中对用户的身份信息进行验证，从而实现无干扰的、全程的身份跟踪与监控。研究者们已经开始探讨利用鼠标交互行为进行身份监控的可行性。尽管监控场景下的鼠标交互行为的描述方法及波动性分析方法仍是非常困难的问题，部分研究者们已经开始了这方面的努力。

针对监控场景下人机交互行为的表示和波动性问题，本章从鼠标交互行为中存在的交互模式入手，尝试提出了一种基于鼠标频繁交互行为模式挖掘的身份监控方法[34,86]。首先，结合计算机用户日常操作鼠标进行交互的特性，利用基于模式生长的序列模式挖掘方法获取交互行为的频繁子序列；然后从频繁子序列中提取稳定的特征刻画量；以这些特征刻画量作为身份模板对用户身份进行监控。

6.2 基本原理

鼠标作为一种能够无缝融入人机交互过程的指点设备，其在交互的过程中会产生大量的行为操作。在这些大量的行为操作中，会包含重复的操作模式，比如用户反复刷新计算机屏幕的操作，而重复的操作往往会形成较为稳定的操作模式。故我们可以从大量的交互行为操作中提取重复的操作模式，然后在认证过程中使用从这些模式中从提取出的特征刻画量。另外，模式挖掘（Pattern Mining）技术是行为分析和异常检测中强有力的工具。因此借助于模式挖掘分析的方法，我们提出了一种基于鼠标频繁交互行为模式的身份监控方法。该方法不仅分析了监控场景下的鼠标交互行为，而且从行为序列中衍生出操作模式的描述，间接捕获了鼠标交互行为的结构化特性。

整个方法的流程图如图 6-1 所示，它包括四个主要的模块，即鼠标行为分析、行为模式挖掘、特征提取、行为模型建立或检测。第一个模块用于行为的表示和描述。对于所捕获到的鼠标行为数据，按照不同的属性对数据进行划分。第二个模块用来提取出行为序列中的频繁操作模式，利用基于模式增长的序列模式挖掘方法来进行用户频繁操作的提取。第三个模块用来进行特征提取，从频繁的操作行为模式中提取刻画行为的特征量。第四个模块应用单分类学习器构建正常行为模型，进行用户身份监控和异常行为检测。实验结果表明该方法能够提取稳定的行为刻画量，获得了非常有效的身份监控和检测精度。

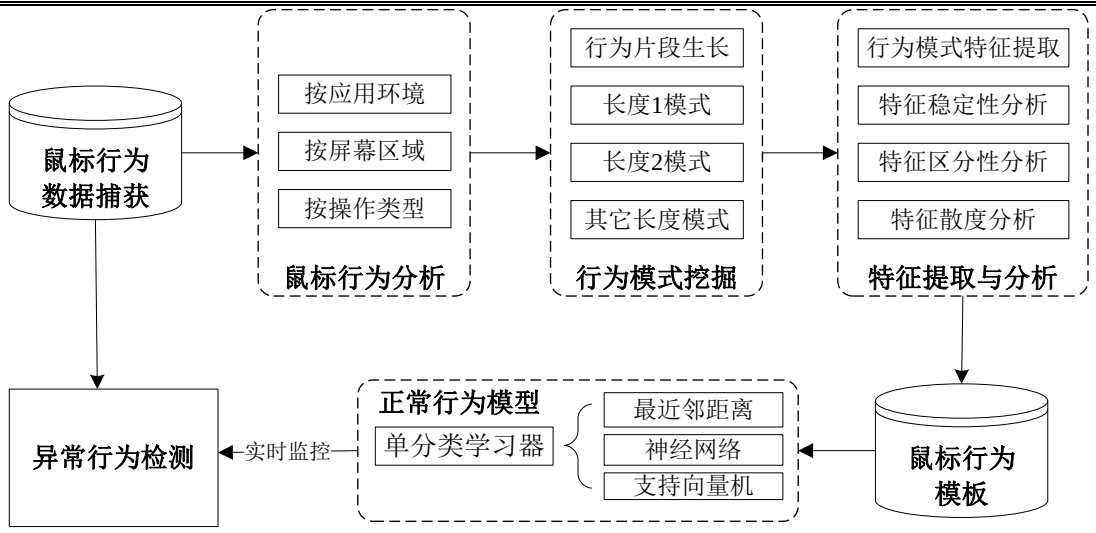


图 6-1 方法的基本流程图

6.3 监控模式

6.3.1 监控模式下的数据采集

我们建立了一个监控模式下的数据采集环境来捕获用户的鼠标交互行为。首先开发了一个数据采集软件，该软件以后台作业的形式运行在计算机之中。在用户登录计算机系统之后该软件开始记录用户的鼠标交互行为，在用户登出计算机系统之后该软件停止数据采集，该软件对用户来说是完全透明的且不影响其它程序的运行。用户的在不同应用场景下日常鼠标交互行为被记录下来，这些场景主要包括网页浏览，字处理应用，在线聊天，业务工作和游戏。在数据采集的过程中，用户被要求使用鼠标进行日常的操作，持续时间大约为半个小时，形成一个鼠标交互行为块。采集到的数据格式为<鼠标行为事件，应用类型，屏幕坐标，时间戳>。

6.3.2 参与用户

我们一共征集了 28 名用户参与身份监控模式下的数据采集，这些用户来自于西安交通大学智能网络与网络安全教育部重点实验室和西安交通大学其它的院系。在每次数据采集的过程中，每名用户完成一个数据块的采集，并且在每两次数据采集之间至少间隔 24 小时。这样做的目的是使数据样本中包含有不同天之间的变化特性。每个数据块中包含大概有 3000 个操作，每名用户用了 30 天到 60 的天的时间完成了 30 个数据块的采集。该数据库公开在我们的网站上[①]。

6.3.3 采集环境

我们在多个计算机系统上部署了该采集软件，这些计算机系统通过 Internet 连接到一台服务器上，用以存储采集到的交互行为数据。计算机系统为 HP 工作站，其配置为

[①] http://nskeylab.xjtu.edu.cn/projects/mousedynamics/monitoring/

Core 2 Duo 3.0 GHz 双核处理器和 2.0GB 的内存，和一个 17 寸的液晶显示器（分辨率设置为：1280×1024）。每个工作站配备着一个光学的 HP USB 鼠标，其上运行着 Windows XP 操作系统。服务器是一台 Dell PowerEdge 服务器，其配置为 Intel Xeon X5677 3.46 GHz 四核处理器和 12.0GB 的内存，其上运行着 Windows Sever 2003 操作系统。

6.4 行为模式分析

在本章的研究中，首先根据章节 3.4.3 中鼠标操作的定义重新对鼠标操作事件进行组合，形成了更加具有实体意义的鼠标操作事件。每个鼠标操作事件都由一个五元组进行表示：<鼠标动作类型，应用程序类型，屏幕区域，屏幕坐标，时间戳>。详细的五元组信息如表 6-1 所示。

表 6-1 鼠标操作事件五元组

操作属性	描述
鼠标动作类型	鼠标单击、双击、一般移动、点击移动、拖拽移动、鼠标静止
应用程序类型	鼠标动作发生的场景，包括浏览器应用，字处理应用，聊天程序应用以及游戏应用
屏幕区域	鼠标光标所在的屏幕区域，在本研究分为类似九宫格的 9 个区域
屏幕坐标	鼠标光标坐标
时间戳	鼠标动作发生的时间

在对不同应用程序类型的鼠标操作事件分析的过程中，我们发现一些鼠标行为片段中包含一系列连续的、重复的鼠标操作，我们定义这样的行为片段为**行为模式**。本章研究将这样的行为模式分为两类：微习惯模式和任务导向模式。微习惯模式刻画了用户下意识的和习惯性的鼠标操作过程。例如大部分的计算机用户重复刷新计算机屏幕，在此过程中，用户先在桌面空白区域点击鼠标右键，然后从弹出菜单中选择“刷新”，这样的模式对应着一系列的鼠标操作：右键单击->鼠标移动->左键单击。任务导向模式刻画了在指定应用下用户鼠标动作的习惯和操作能力，例如经常性的在某些特定应用中使用某些功能。当用户在字处理软件中想要创建一个新的文档时，用户首先使用鼠标左键点击字处理软件的菜单栏，接下来在菜单栏中选择“新建”，并在弹出的窗口中选择“空白文档”，这样的操作对应着一系列的鼠标操作：左键单击->鼠标移动->左键单击->鼠标移动->左键双击。

6.5 行为模式挖掘

本章首先描述了鼠标交互行为模式挖掘的问题，接着提出了一种基于模式增长的序列模式挖掘方法以抽取出相应的行为模式。

6.5.1 行为模式挖掘问题

我们的主要目的是从鼠标操作的整体行为当中提取出频繁的行为模式。首先定义

鼠标行为模式挖掘问题。令 $I=\{i_1, i_2, \ldots, i_n\}$ 为鼠标操作的一个集合，是整体鼠标操作行为的一个子集。令 $s=\{s_1 s_2 \ldots s_l\}$作为一个鼠标操作序列，且这个操作序列是根据用户名和时间戳进行排序的，s_j 是一个操作集合，$s_j \subset I, 1 \le j \le l$。$s_j$ 也称作该序列中的一个元素，定义为$\{x_1, x_2, \ldots, x_m\}$，$x_k$ 是一个鼠标操作。操作序列中鼠标操作的实例个数定义为序列的长度。例如，l 长度的序列就被称为是一个 l-序列。鼠标操作序列数据库是一个三元组的集合，该三元组表示为<*ID, sid, s*>，在这里 *ID* 指用户 ID，*sid* 指序列的 ID 编号，*s* 指一个鼠标操作序列。序列 α 在数据库 S 中的支持度指的是数据库中包含 α 的子项发生的频数，在这里被定义为 $support(\alpha)$。给定一个正整数 ξ 作为支持度的阈值，如果序列 α 包含最少 ξ 个三元组，$support_S(\alpha) \ge \xi$，则序列 α 被称为数据库 S 中的序列模式。l 长度的序列模式就称为 l-模式。

问题描述：给定鼠标操作序列数据库 S 和最小值尺度 ξ，序列模式挖掘的问题就是从数据库中找寻并构建行为模式集。

6.5.2 行为模式挖掘算法

本章基于前缀投影序列模式挖掘算法提出了一种新颖的鼠标行为模式挖掘算法。该算法采用分治的思想，将简单的操作模式作为投影向量，不断从鼠标操作数据库中产生多个更小的投影数据库，然后在各个投影数据库上进行深入的序列模式挖掘。本研究定义的鼠标行为模式前缀，后缀及投影数据库如下。

前缀：给定序列 $\alpha=\langle e_1 e_2 \cdots e_n \rangle$，一个序列 $\beta=\langle e_1' e_2' \cdots e_m' \rangle (m<n)$ 被称为 α 的前缀当且仅当 (1)对于 $(i \le m-1)$，$e_i'=e_i$；(2) $e_m' \subseteq e_m$。

后缀：给定序列 $\alpha=\langle e_1 e_2 \cdots e_n \rangle$（在这里 e_i 对应于 S 中的一个频繁子项）。令 $\beta=\langle e_1' e_2' \cdots e_m' \rangle (m<n)$ 作为 α 的前缀。序列 $\gamma=\langle e_m'' e_{m+1} \cdots e_n \rangle$ 被称为 α 相对于 β 的后缀，定义为 $\gamma=\alpha/\beta$，在这里 $e_m''=(e_m-e_m')$。

投影数据库：令 α 作为序列数据库 S 中的一个序列模式。我们定义 α-投影数据库为 $S|_\alpha$，指的是在 S 中相对于前缀 α 的所有后缀序列的集合。

根据图 6-2 所示，鼠标行为模式被增量式的从鼠标操作序列数据库中提取出来。该算法首先扫描整个行为数据库去寻找长度为 1 的鼠标行为序列模式，然后将搜索空间分成多个前缀投影，构建相对应的投影数据库，最终在得到的投影数据库中迭代式的找寻序列行为模式的子集。

6.5.3 参考行为模式的生成和匹配

在对鼠标交互行为进行异常检测或身份监控之前，我们需要根据每个合法用户的训练数据生成对该用户的参考行为模式集。我们从每个训练数据块中挖掘出相应的行为模式，再增量式的将这些行为模式集结起来形成一个参考行为模式集合。

在检测过程中，针对未知的行为数据块，根据生成的参考行为模式集，我们可以很简单的对行为模式进行匹配：

第一步，对给定数据块中的每个行为序列，依次在参考行为模式集中进行匹配；
第二步，输出所有的匹配的行为模式来表示这个数据块。

输入: 鼠标操作序列数据库 *S*, 和最小值尺度阈值ξ.
输出: 完整的频繁行为模式集*P*.
方法: *MouseBehaviorPatternMining*()

调用 *MouseBehaviorPatternMining* (<>, *S*, ξ)
Begin
(1) 令 α 表示序列化的鼠标操作模式;
(2) **if** $\alpha \neq$ <>
(3) 令$S|_\alpha$ 表示 α-投影的数据集;
(4) **else**
(5) $S|_\alpha = S$;
(6) **end**
(7) 令 *l* 表示α的长度;
(8) **for** $S|_\alpha$ 的每个鼠标操作**do begin**
(9) 找寻频繁项的集合*b*;
(10) **if** 在$S|_\alpha$ 中频繁项*b*的结果以及 (*l*+1) 是大于ξ **then begin**
(11) **if** *b* 能够被组合
(12) 形成新的集合$B = B \cup \{b\}$;
(13) **end**
(14) **end**
(15) **end**
(16) **for** *B*中的每个频繁项*b* **do begin**
(17) $\alpha' = \alpha \cup \{b\}$;
(18) 形成新的α'-投影的数据集$S|_{\alpha'}$;
(19) **Call** *MouseBehaviorPatternMining* (α', $S|_{\alpha'}$, ξ);
(20) **end**
end

图 6-2 行为模式挖掘算法

6.5.4 行为模式分析

本研究利用 28 名用户 420 个行为会话作为训练数据并据此生成训练行为模式集（每个会话中包含约 3000 个鼠标操作行为），同时基于这个模式集，我们提取了相应的行为特征刻画量并构建了合法用户的正常行为模型。

表 6-2 行为模式中鼠标操作相对于整体行为的覆盖率

最小支持度	长度 1 模式	长度 2 模式	其他模式	所有模式
2%	23.64%	32.15%	25.22%	81.01%
5%	16.08%	22.06%	24.90%	63.04%
8%	12.29%	17.65%	17.34%	47.19%
20%	0.95%	1.26%	0%	2.21%

表 6-2 显示了行为模式中鼠标操作相对于整体行为的覆盖率。从表中可以看出随着最小支持度的增加，所有模式对应的覆盖率都有所下降。由于最小支持度反应了行

为模式发生的频率，而从高频率的行为模式中可以提取出更加稳定的行为特征。因此，在覆盖率和最小支持度之间存在一个折中。这里我们设定最小支持度为 8%。在此支持度下，长度 1 模式，长度 2 模式，及长度 n 模式的覆盖率分别为 12.29%，17.65%及 12.29%。对应的模式个数如表 6-3 所示：

表 6-3 不同支持度下行为模式的个数

最小支持度	长度 1 模式	长度 2 模式	其他模式	所有模式
2%	2127	1445	482	4054
5%	1447	992	329	2768
8%	1106	794	130	2030
20%	85	57	7	149

6.6 特征提取

6.6.1 特征提取

行为特征向量包含了用户鼠标行为模式中的所有操作的特征，这里定义特征如下：

点击持续时间：用户进行鼠标单击时按键按下和弹起的时间间隔。点击类型选取一般用户常用的点击：左中右键单击、左键双击、左键拖拽、中键滚动等，共 6 种。

移动速度：不同类型鼠标移动的平均速度。需要注意的是移动类型由离散化的移动方向和长度划分，方向分为 8 种，长度分为 3 种，共 24 种。

移动加速度：不同类型鼠标移动的加速度。

移动速度极值的相对位置：一次鼠标移动中极值速度点在移动中的相对位置。如极值速度点在移动的中间位置，则取值 0.5。

如章节 6.3 所述，鼠标交互行为数据是以数据块为单位进行采集的。故特征从每个数据块中进行提取，在本章的研究中，我们提取了 20 个点击相关的特征，24 个移动速度相关的特征，24 个移动加速度相关的特征，和 24 个移动速度极值的相对位置相关的特征，这些特征经过组合形成了 92 维的特征向量，来表示每个数据块。

6.6.2 特征评价

我们对从行为模式中提取的特征进行系统性的评价，来检验相比于整体行为中行为模式对特征稳定性、区分性、散布性的提升。

1）特征稳定性评价

鼠标交互行为分析中一个重要的问题就是行为的稳定性。行为数据可能会受到各种环境因素或人为因素的影响，从而变得不稳定。因此从原始行为数据中直接提取的特征往往不能够很好的刻画用户的行为。具体来说，点击时间相关的特征高度依赖于用户手指的灵活性和用户的操作目的；移动速度相关的特征与用户的移动习惯或应用场景密切相关。因此，从不同操作属性的行为模式中提取出的特征刻画量将能够较为准确的表示交互行为。

我们使用了核密度函数估计的方法分别计算行为模式中和整体行为中特征的概率密度函数曲线。每个特征的概率密度曲线是由对应用户的 300 个鼠标操作得到的。图 6-3 展示了两个用户的一些特征的对比结果。

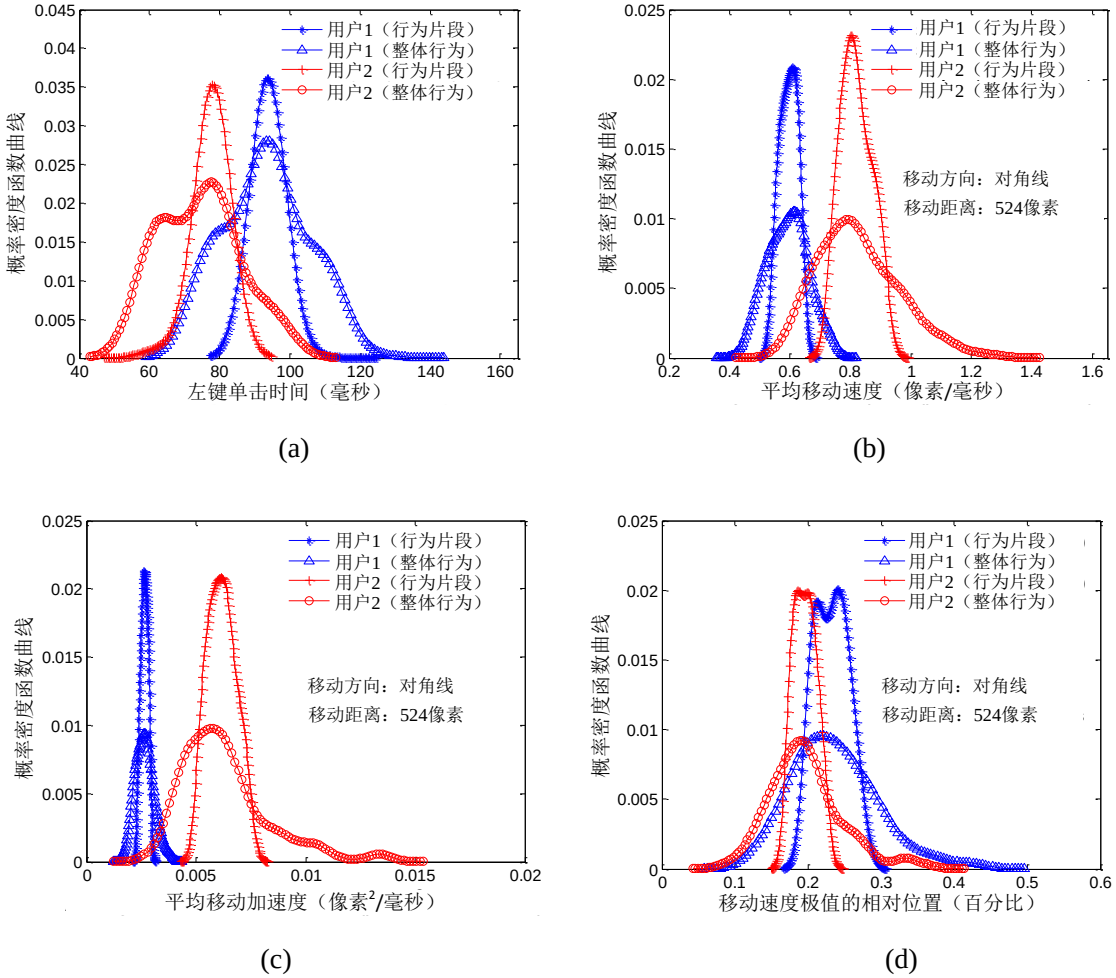


图 6-3 两个用户部分鼠标特征在行为模式和整体行为下的概率密度曲线对比图。其中(a) (b) (c) (d)分别展示了左键单击时间、平均移动速度、平均移动加速度及移动速度极值的相对位置的概率密度曲线。

从图中我们可以观察到从行为模型中提取的特征的概率密度曲线明显比从整体行为中得到的概率密度曲线更加紧凑和集中，这表明行为模式中的特征刻画量可以更加稳定和准确的对鼠标交互行为进行刻画。重复发生的行为模式在一定程度上能更准确的表示用户的习惯和稳定性行为，因此能够从中提取出更为稳定的特征刻画量，更加准确对用户身份信息进行表示。

2）特征区分性评价

鼠标交互行为分析中另一个重要的属性是特征的区分性。经过实验分析发现，从行为模式中提取的特征刻画量不但对于同一个用户表现出相对的稳定性，而且对于不同的用户表现出较高的区分性。如图 6-3 所示，从整体行为中提取的特征的概率密度曲线对于两个用户拥有较大的重叠区域，这意味着较难对两个用户的行为进行区分。

相比之下，在行为模式中两个用户的特征概率密度曲线有着明显的区分，表明从行为模式中提取的特征具有更好的区分能力，能够对不同用户的行为进行较好的区分。具体来说，平均速度（图（b））和平均加速度（图（c））的概率密度曲线在行为模式下能够将两个用户的行为完全区分，而在整体行为下却有着明显的重合。

上述对于特征稳定性和区分性的实验结果表明，从行为模式中提取的特征刻画量明显优于整体行为中的刻画量。需要注意的是，在这里只呈现了部分用户的对比图。然而，对于其它的用户也得到了相似的结果。

3）特征散布性评价

为了进一步对行为模式的有效性进行评估，我们基于基尼平均差（Gini's Mean Difference）[136]定义了一个简单且有效的散布指标对行为模式下特征量的统计散布性进行分析。该测量量的数值为 0 时表明所有的数据都相同（数据很稳定），该数值的增加表明数据的分布变得更加散布。这里，针对行为模式下提取的每个特征 $f_k=\{x_i^k\}_{1\times n_k}$，其散布指数可定义为：

$$DM(f_k)=\frac{1}{n_k(n_k-1)}\sum_{i=1}^{n_k}\sum_{j=1}^{n_k}\left|x_i^k-x_j^k\right| \qquad (6\text{-}1)$$

我们首先计算每个用户的每个特征的散布指数，数据来源是每个用户的 300 个鼠标操作。然后在所有 28 个用户的数据上得到了平均散布指数，如表 6-4 所示，其中第三列的括号内的百分比表示了行为模式下特征的散布指数相比于整体行为下的减弱程度。

表 6-4 行为模式和整体行为下特征的散布指数

特征	整体行为下	行为模式下
左键单击时间	0.1450	0.0121 (-91.7%)
左键双击时间	0.0632	0.0214 (-66.2%)
右键单击时间	0.1247	0.0347 (-72.2%)
右键双击时间	0.1683	0.0652 (-61.3%)
平均移动速度②	0.1872	0.0703 (-62.4%)
平均移动加速度②	0.3106	0.1198 (-61.4%)
移动速度极值的相对位置②	0.3650	0.1645 (-54.94%)

从表中我们可以看到行为模式下的特征的散布指数要明显小于整体行为下的度量量。同时，对比于整体行为下的度量量，表中所有的特征在行为模式下的散布指数都降低了超过 50%，左键单击时间特征更是降低了 91.7%。这些结果表明行为模式下的特征刻画量拥有更强的稳定性和可区分性，将能够在身份监控和检测的过程中更好的

② 本章研究中基于 8 种移动方向和 3 种移动距离提取了 24 种类型的移动。在这里我们以对角线方向、移动距离为 524 像素为例计算了对应特征的散布指数。然而，对于其它类型的移动也能得到相似的结果。

表示用户的身份信息。

6.7 分类器

6.7.1 分类器的部署

本文采用了三个单分类分类器进行身份监控模式的构建：单分类支持向量机，单分类神经网络和单分类最近邻距离。具体的描述请参见章节 4.7。

6.7.2 评估方法

在身份监控的场景下，我们首先指派 28 名用户中的 1 名作为合法用户，其他用户作为非法用户。根据如下的步骤训练并且测试分类器对合法用户和非法用户的识别能力：

第一步，从合法用户的数据中随机抽取 15 个会话（总共 30 个会话）建立该用户的身份监控模型；

第二步，测试该模型对合法用户的识别能力。将该合法用户剩余的 15 个会话作为身份监控模型的输入，计算这些样本的检测分数，记为合法分数。

第三步，测试该模型对非法用户的识别能力。将非法用户的所有会话（27×30=810）作为身份监控模型的输入，计算这些样本的检测分数，记为非法分数。

第四步，依次指定其余用户作为合法用户，并重复上面的步骤得到每个用户对应的合法分数和非法分数。

在训练的过程中，我们采用了 10 折交叉验证计算模型的参数[122]。此外，由于在训练过程中使用随机选择的方法获得用于生成身份监控模型的训练数据，为了解释这个随机因素，我们将上述实验重复了 20 次，每次独立地从数据池中选择合法用户的训练数据。

本章所采用的评估指标为误纳率（False-Acceptance Rate, FAR），误拒率（False-Rejection Rate）和受试者工作特征曲线（Receiver Operating Characteristic curve，简称 ROC 曲线）。详细描述请参见章节 4.8.3。

6.8 实验结果与分析

6.8.1 身份监控实验

图 6-4 和表 6-5 展示了应用不同分类器的身份监控实验的 FAR、FRR 及 ROC 曲线，表 6-5 括号内的数值表示相关 FAR 和 FRR 值的标准差。

从图 6-4 和表 6-5 的实验结果中，可以观察到最好的身份监控的检测结果为 0.37% 的 FAR 和 1.12%的 FRR，该结果是令人鼓舞的且很有竞争力。此外该方法对鼠标交互行为的观察时间要短于文献中的其它方法。我们还发现使用行为模式得到的平均错误率要明显低于使用整体行为得到的结果，这是由于行为模式对交互行为中所包含的身份信息的稳定及准确的刻画，也从另一个侧面证实了利用行为模式表示身份信息的有

效性。此外，我们的结果非常接近欧洲商用生物特征认证的要求（0.001%的 FAR 和 1%的 FRR[125]）。虽然该结果还不能支持鼠标交互行为作为单一的生物特征对用户的身份有效性进行检测，但是它再一次证实了鼠标交互行为中所反映出的用户身份信息。平均错误率的标准差也表明了利用行为模式进行身份监控检测的稳定性和鲁棒性。

通过比较三种分类器的检测结果，我们发现单分类支持向量机要优于其它两种方法。这可能是由于支持向量机在先验知识不足的情况下能够将身份检测中的分类问题转换为最优化问题，并且能够保持较高的准确度和稳定度。此外，对应检测结果的标准差也说明了单分类支持向量机的鲁棒性。我们还发现应用最近邻分类器得到的 FAR 为 2.73%，FRR 为 3.67%，这一结果要明显差于其它两种方法。我们分析其原因可能是由于最近邻分类器对噪声数据的敏感并且缺少自我学习的能力。

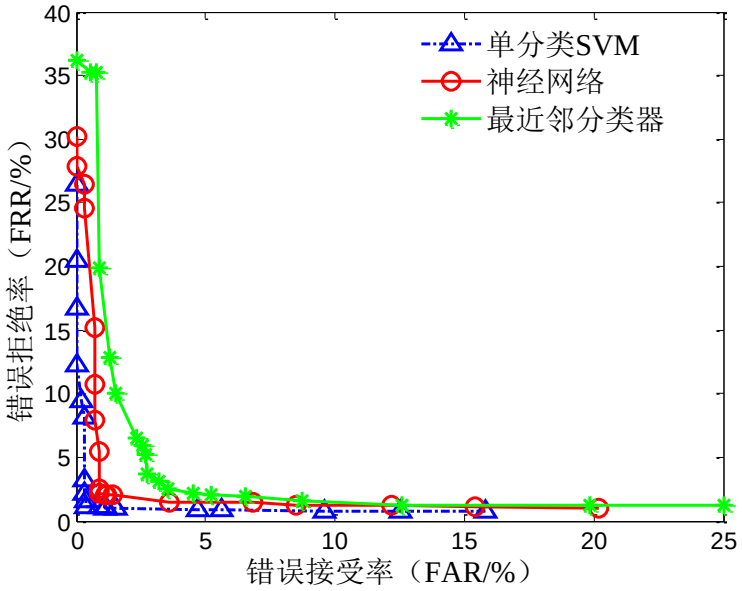


图 6-4 不同分类器下身份监控结果的 ROC 曲线

表 6-5 不同分类器下身份监控结果的 FAR 和 FRR 值

	行为模式		整体行为	
分类器	FAR/%	FRR/%	FAR/%	FRR/%
最近邻分类	2.73(1.24)	3.67 (0.89)	8.87 (9.36)	9.63 (9.23)
神经网络	0.89 (0.57)	2.15% (0.65)	6.36 (5.34)	6.95 (6.53)
单分类支持向量机	0.37 (0.62)	1.12% (0.67)	5.57 (5.02)	6.73 (4.93)

最后，我们使用了 HTER 和置信区间对得到的认证结果进行相应的统计结果分析。三类方法的实验结果对比表明结合单分类支持向量机的方法能够得到最低的 HTER。在 95%的置信区间下，该方法能够达到的身份监控检测错误率为 0.75%±1.15%。

6.8.2 比较

这里，我们将本章研究的实验结果与文献中的身份监控检测方法的结果进行了比较，如表 6-6 所示。Pusara 等人[100]将鼠标交互行为作为一种单独的生物行为特征，提出了一种身份再认证的方法，得到了较高的认证精度结果和较少的检测时间。但是该研究只采集了 11 个用户的数据并且没有考虑到行为波动的问题。我们的方法采集了更多用户的数据并提出了一种改进的方法，使用行为模式发现的方法有效的降低了行为波动性并提取了稳定的特征刻画量。另一方面，Schulz[102]所提出的方法能在较短的时间内对用户进行检测，但是其检测错误率高达 24.3%（EER）。在我们的方法中，身份的检测可以在 10 分钟内进行，并且相应的 FAR 为 2.75%，FRR 为 3.39%。虽然这个精度还不能达到欧洲标准对商用生物特征的要求，但这个结果可以支持基于鼠标交互行为的身份监控作为一种辅助的身份监控和检测手段。

表 6-6 与文献中方法的比较

文献	身份监控检测结果			数据采集	训练数据
	FAR/%	FRR/%	检测时间/分钟	用户	来源
本方法	7.78 2.75	9.45 3.39	5 10	28	合法用户
Pusara *et al.* [100]	0.43	1.75	1 to 14.5	11	合法和非法用户
Ahmed *et al.* [31,32]	2.46	2.46	17.22	22	合法和非法用户
Schulz [102]	24.3	24.3	未说明	72	合法和非法用户
Zheng *et al.* [78]	1.3	1.3	37.37	30	合法和非法用户

6.9 结论

本章针对监控场景下人机交互行为的表示和波动性问题，提出了一种基于鼠标频繁交互行为模式挖掘的身份监控方法。我们详细的介绍了监控模式下的鼠标行为分析、行为模式挖掘、特征提取、行为模型建立等问题。该方法不仅分析了监控场景下的鼠标交互行为，而且从行为序列中衍生出频繁的行为模式，间接捕获了监控模式下鼠标交互行为的结构化特性。从检测结果中，我们可以看到从行为模式中能够提取稳定的特征刻画量，获得了非常有效的身份监控和检测性能。

未来工作需要进一步研究行为模式在总体行为中的覆盖率、开发身份检测方法的鲁棒性以及寻求更有效的行为特征和分类器等。

7 基于多种人机交互行为的身份隐私属性分析

7.1 引言

随着社会信息化、网络化大潮的推进，在计算机及移动网络中对用户信息的感知分析变得越来越重要。一方面，在电子商务、网络银行等网络虚拟化经济活动中，商家迫切希望能够尽量充分地了解客户，以提供针对性的商品或服务从而提高商业活动的成功率；另一方面，计算机网络和移动网络信息犯罪活动也越来越严重，提取和分析存在于计算网络系统中的电子证据进而确定操作者的性别、年龄、种族、语言等身份属性能够为网络犯罪活动的发现和遏制提供重要的帮助。

近年来，有研究人员提出基于生物特征检测用户的信息或身份属性，他们根据人脸、指纹、虹膜、掌纹等生理特征对用户的性别、年龄、种族等信息进行检测，但是，此类方法需要使用特定的生物信息采集设备，如摄像头、指纹传感器等，不适用于现有的计算网络环境。目前还没有可以在现有的计算网络环境中大规模应用的分析检测用户身份属性的技术或方法。

针对上述需求，本章提出一种基于多种人机交互行为（鼠标和键盘）的身份隐私属性的分析方法[107]。分析在取证分析场景下根据这些交互行为对计算机操作者的身份隐私信息进行推理，尤其是对计算机操作者的“软身份”特性进行识别（例如性别/年龄/种族/左右手使用习惯等）。

7.2 基本原理

使用生物特征信息在信息取证场景下进行身份隐私属性的分析自从20世纪初就开始了。生物特征识别可以被看成是1893年Bertillon所提出的人类学的一种扩展，来源于人体的一些测量量。在当前计算环境下，生物特征信息在信息取证场景下的应用主要为如何从大量的候选数据（或候选嫌疑人）中过滤出潜在的数据（或嫌疑人），以为后续的专家分析提供一种自动化的、可靠的分析手段。

近些年来，有很多生物特征（例如语音[137,138]、人脸[139,140]、指纹[141,142]、步态[143,144]）被用来在信息取证分析中进行候选用户的过滤（通过推测候选用户的身份属性比如年龄、性别），虽然这些方法取得了一定的成功，但是它们也存在一些缺陷致而限制相关技术在计算机犯罪相关领域的应用：1）有些技术的数据捕获需要用户的配合；2）有些技术需要额外的设备；3）有些技术容易被攻击和模仿。

因此，本章在前三章研究的基础上（证实的鼠标交互行为中含有充分的身份信息），提出了一种基于多种人机交互行为（鼠标和键盘）的身份隐私属性分析方法。该方法不需要特殊硬件设备，可在现有的计算环境下实现无干扰的信息捕获及身份隐私属性

分析，可以为计算机信息取证提供一种新的解决思路。

方法的流程图如图 7-1 所示。首先捕获人机交互行为（鼠标和键盘行为），对行为进行标识和分析，提取多模态的交互行为特征。接着借助于随机森林学习框架，基于这些特征进行软身份建模的建立，最后采用多决策融合的方法对计算机操作者的身份隐私属性信息识别。

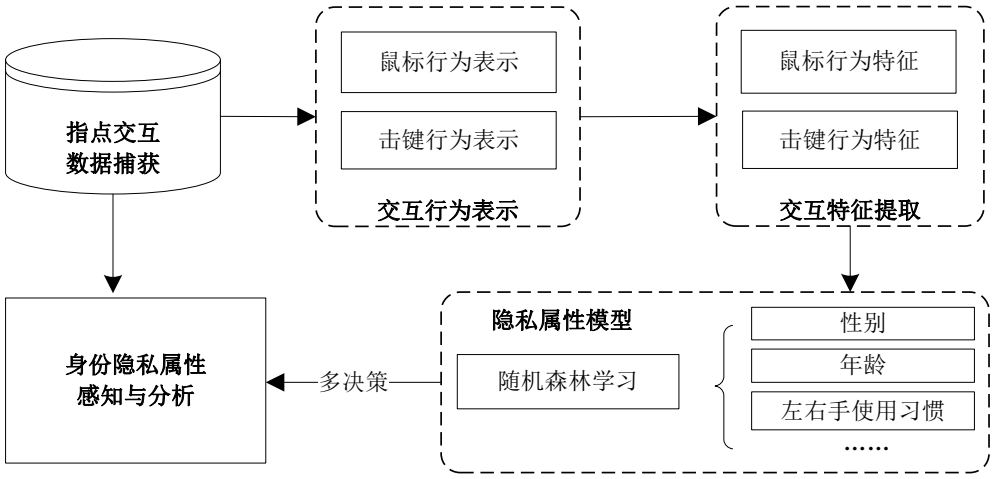


图 7-1 方法的基本流程图

7.3 基于人机交互行为的身份隐私属性研究

利用人机交互行为进行身份隐私属性的研究是一个全新的领域，至今为止还未见有学者进行该领域的探索。近年来只有 2012 年 Giot 和 Rosenberger[145]在所提出的一种加强身份认证的方法中采用了键盘交互行为对用户的信息进行性别识别，作为身份认证的一个额外特征。但是由于他们的目的是进行身份认证，因此在进行性别识别时的训练和测试数据都来源于同一组用户。而取证分析的场景下要求的训练数据来自任意用户的收集，测试数据是来自取证场景下的采集，因此训练和测试数据往往是来自不同用户。尽管如此，Giot 和 Rosenberger 还是展现了利用键盘交互行为进行性别识别的可行性。

7.4 数据采集

总体来说，利用人机交互行为进行身份隐私属性的可行性分析需要对数据采集过程加以控制，以将本质的行为特征作为分析中的首要因素，同时也可以减少其它环境因素产生的影响。基于这样的考虑，本章扩展了我们先前研究所得到的鼠标[36]和键盘交互行为数据[112]。下面我们对这两个数据集进行简单的描述。

7.4.1 键盘交互行为数据采集

在键盘交互行为数据的采集过程中，51 个用户参与并完成了数据采集过程。每个用户被要求键入一个 10 字符长度的密码（.tie5Roanl）400 次。采集共分 8 次完成，每

次要求用户完成 50 次的数据采集。简单来说，数据采集平台由一个外接键盘、一台笔记本、一个外接的时钟计数器组成。时钟计数器用来记录生成击键事件的时间戳（精度为 100 微秒）；数据采集软件提示用户进行密码的键入，同时记录键盘的按下和弹起事件。详细的数据采集方法和过程请参见[112]。

7.4.2 鼠标交互行为数据采集

在鼠标交互行为数据采集的过程中，58 个用户参与并完成了数据采集过程。每个用户被要求完成一个固定的鼠标移动序列 300 次。该移动序列包含 8 个连续的移动，两个移动间由鼠标点击隔开。该移动序列定义了 8 个移动方向，每个移动代表一个 45 度区域内移动方向（共 360 度）；同时定义了 3 种移动距离，分别代表短、中、长距离的移动。数据采集平台包括数据采集软件、一个台式机和一个 USB 鼠标；Windows 事件时钟用来生成鼠标事件的时间戳（精度为 15.625 毫秒）；数据采集软件提示用户进行鼠标移动序列的操作，并记录下相应的鼠标行为事件。详细的采集方法和过程请参见[36]。

7.5 身份属性

在基于鼠标和键盘交互行为的身份隐私属性分析中，一个重要的步骤是对参与数据采集的用户的身份属性信息进行标记。因此，我们在数据采集开始之前对每个用户进行了一次身份隐私信息的问卷调查。此次问卷调查共收集了每个用户 25 个身份隐私属性，比如性别、年龄、种族等。在本章的研究中，我们选择了 5 个和计算机取证分析最相关的属性，包括性别、年龄、种族、左右手使用习惯和主要使用的语言。

对于键盘交互行为数据，共有 51 名用户参与了问卷调查，每个用户的键盘使用年龄大于 5 年。我们根据所选择的身份隐私属性对用户进行了类别划分（主要分为 2 类，对于年龄划分为 3 类），如下所示（括号中表示每个类别中用户的数目）：

性别：第一类=男性（30），第二类=女性（21）；

年龄：第一类<=30 岁（24），第二类>30 岁并且<=60 岁（25），第三类>=60 岁（2）；

种族：第一类=白种人（41），第二类=非白种人（10）；

左右手使用习惯：第一类=右手（43），第二类=左手（8）；

主要使用的语言：第一类=英语（45），第二类=非英语（6）。

对于鼠标交互行为数据，共有 58 名用户参与了问卷调查，每个用户的鼠标使用年龄大于 2 年。在进行问卷调查的过程中，我们发现进行鼠标行为数据采集的用户都是来自于西安交通大学的学生，因此难以在诸如种族和年龄的属性上产生多样性。考虑到这样的局限性，我们根据相关的身份隐私属性对用户进行类别的划分，如下所示（括号中表示每个类别中用户的数目）：

性别：第一类=男性（46），第二类=女性（12）；

年龄：都是小于 30 岁，年龄分布在 19 岁到 25 之间；

种族：都是非白种人；
左右手使用习惯：都是右手；
主要使用的语言：都是非英语。

7.6 特征提取

击键行为特征从原始的击键事件中进行提取。这里，我们提取了 3 类典型的击键事件特征，包括：（1）击键持续时间（表示一个按键的按下和弹起之间的间隔时间）；（2）连键延迟时间（表示相邻两个按键按下的间隔时间）；（3）连键间隔时间（表示相邻两个按键第一个按键弹起和第二按键按下的间隔时间）。针对我们使用的密码，共提取了 31 个时间特征，包括 11 个击键持续时间，10 个连键延迟时间和 10 个连键间隔时间。这 31 个特征组成了 31 维的特征向量用来表示一次采集的密码样本。详细的特征定义及提取过程可以参见[112]。

鼠标行为特征从鼠标移动的基本属性（距离、时间、速度和加速度）进行提取。我们基于每个属性对行为进行细分，得到相应的行为特征。这里，我们将这些特征分为两类：移动形态特征，反映了鼠标运动轨迹的几何结构的度量，比如运动轨迹长度、偏移量；移动动态特征，反映鼠标运动轨迹的随时间变化的特性，比如运动轨迹的加速度变化曲线。针对我们的鼠标操作序列，生成了 104 维的特征向量来刻画一次采集的鼠标操作序列样本。详细的特征定义及提取过程可以参见章节 5.3 和 5.4 以及[36]。

7.7 分类器

7.7.1 加权随机森林分类器

在身份隐私属性标记的过程中，我们发现根据不同属性划分而产生的类别会表现出较强的偏向性。例如，在对参与键盘交互行为采集的用户根据种族属性进行划分时，我们有 41 个白种人和 10 个非白种人，因此该数据的分布明显偏向于白种人的类别。这会导致模型训练和识别时的不平稳偏差[146]。为了解决这个问题，在这里本章提出了一种基于加权的随机森林分类方法，通过在算法的节点分割和决策阶段引入权值来平衡模型的不平稳偏差，其原理示意图如图 7-2 所示。

原始随机森林由 Leo Breiman(2001)[147]提出，它通过自助法(bootstrap)重采样技术，对每个 bootsrap 样本进行决策树建模，然后组合多棵决策树的预测，通过投票得出最终预测结果。下面我们详细描述基于加权的随机森林分类方法的构建过程。

第一步，初始化训练特征集中特征样本的个数为 N，每个特征样本中特征分量的个数为 M，决策树的个数为 P，每个决策树的决策特征的个数为 m (m 远小于 M)；在整个随机森林的构造过程中 m 是一个常数，我们选取 $m=\text{int}(\log_2 m+1)$，其中 int 是取整函数。

第二步，为了消除不同的特征量纲的影响，对各维特征向量进行归一化处理，将其取值限制在[0, 1]之间；

第三步，使用 Bagging 算法对 N 个特征样本取样 P 次，得到 P 个特征集合；

第四步，对每一个随机树随机选取一个特征集合，并对该决策树进行评估及误差分析。对于树中的每一个节点，随机选择 m 个基于此点的特征分量，并针对不同类别的特征样本，赋予不同的权值以寻找最佳的分割方式。为了找到最佳的分割方式，在每棵决策树构造的过程中，其生成遵循自顶向下的递归分裂原则，即从根节点开始依次对训练集进行划分。对于每个节点，按照节点不纯度最小原则，分裂为左节点和右节点，它们分别包含训练数据的一个子集，按照同样的规则使节点继续分裂，直到分支停止生长。若节点 i 上的分类数据均来自于同一类别，则该节点的不纯度 $I(i)=0$。不纯度的度量方法是基于 Gini 不纯度准则的，即假设 $P(w_j)$是节点 i 上属于 w_j 类样本个数占训练样本总数的频率，则 Gini 不纯度准则表示为

$$I(n)=\sum_{i\neq j}P(w_i)P(w_j)=1-\sum_{j}P^2(w_j) \qquad (7\text{-}1)$$

第五步，根据分类效果最好的特征节点将节点划分为两个分支，再递归调用第四步直到这棵树能够准确分类训练样本集，或所有属性都已经被使用过；决策树完整成长之后，不对其进行剪枝；

第六步，重复第三步、第四步、第五步直到建立了全部 P 棵决策树；

第七步，采用基于加权的多数投票的方法来综合决定多个决策树的分类结果，即得到了加权随机森林分类器的分类结果。

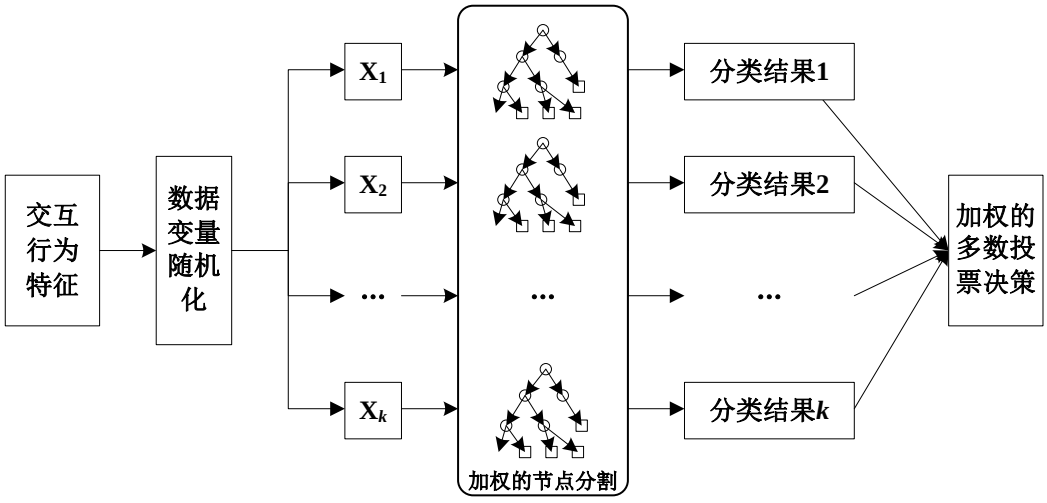


图 7-2 加权随机森林算法的示意图

7.7.2 评估方法

在方法的评估过程中，我们将所有用户的数据分成了训练数据集和测试数据集，并确保两个数据集中的数据来自不同的用户。这是为了测试我们的方法在取证分析场景下的可应用性。取证分析的场景下要求的训练数据来自任意用户的收集，测试数据是来自取证场景下的采集，因此训练和测试数据往往是来自不同用户。我们使用了 10

折交叉检验的方法对分类器进行训练和测试，计算出身份隐私属性的识别率。具体来说，针对于每个身份隐私属性，我们把所有用户分成 10 份，其中 9 份中包含的用户的交互行为数据用来进行训练分类器，剩余 1 份中包含的用户的交互行为数据用来进行测试；我们对上述过程进行了 10 次重复，每一次指定 1 份不同的用户交互行为数据作为测试数据。然后针对其它的身份隐私属性重复上述的步骤。

因为采用了随机采样的方法将用户分成 10 份，为了解释由这个步骤引起的随机性，我们将上述评估过程重复 20 次。在每次重复过程中都使用上述的 10 折交叉检验的方法，因此针对每个身份隐私属性的识别，我们都产生了 200 个识别准确率，通过求取均值和标准差得到了最终的识别结果。此外，本章还使用了卡巴统计量（Kappa Statistic）来反映该识别结果是否是所提出的方法的真实体现（卡巴统计量的数值从 0 变化到 1，其中 0 表示识别结果是由所建立的方法随机产生的，1 表示识别结果完全是所提出的方法的性能体现）。

7.8 实验结果与分析

7.8.1 身份属性识别

图 7-3 和表 7-1 展示了身份隐私属性的识别结果。从实验结果我们可以观察到利用鼠标或键盘交互行为进行身份隐私属性的识别率均高于 82%，这个结果是非常令人鼓舞的，同时也表明鼠标和键盘交互行为中包含了用户的身份隐私信息，可以用在信息取证场景下进行隐私信息的识别和推测。具体来说，针对于性别属性，基于鼠标交互行为所提出的方法得到了 83.152%的识别率，基于键盘交互行为得到了 85.143%的识别率。

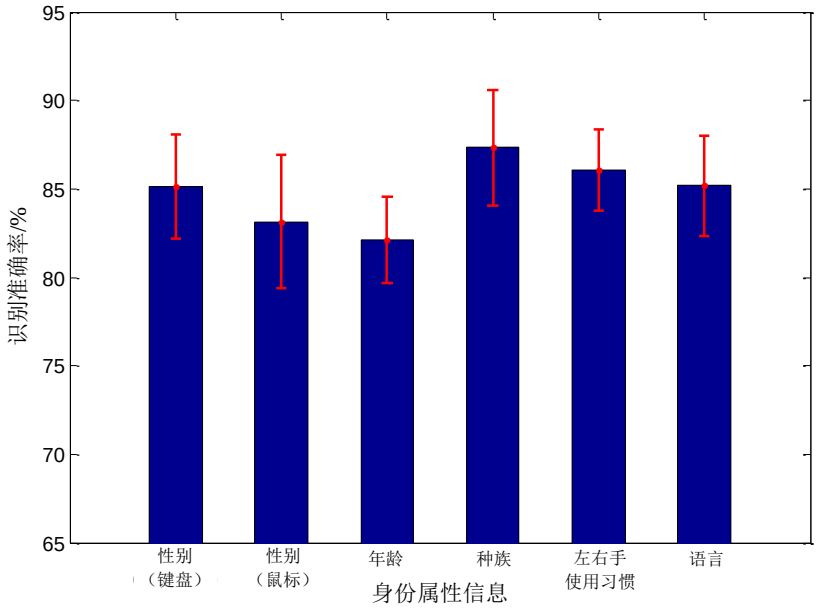


图 7-3 不同身份隐私属性的识别结果

表 7-1 不同身份隐私属性识别的统计分析结果

身份隐私属性	类别个数	识别率/%	识别率标准差/%	卡巴统计量	卡巴统计量标准差
性别[①]	2	85.143	2.965	0.703	0.059
		83.152	3.756	0.663	0.076
年龄	3	82.109	2.435	0.732	0.037
种族	2	87.323	3.242	0.746	0.065
左右手使用习惯	2	86.065	2.312	0.721	0.046
主要使用的语言	2	85.186	2.839	0.704	0.057

我们也观察到相比于识别率，身份隐私属性识别率的标准差较小（如图 7-3 中的错误条和表 7-1 中的第四列所示）。这说明我们的方法对行为的波动性和不同的参数选择方法呈现出了一定的稳定性和鲁棒性。这是由于所提出加权随机森林分类方法能够对样本较少的类别给予给多的权值，并在样本少的类别发生分类错误时给于更大的惩罚因子。此外，随机森林方法的随机性也在一定程度上确保了在小样本数据集上的高识别率。

我们也计算了卡巴统计量（如表 7-1 第五、六列所示）来进一步分析识别率和所建立方法的关联性。可以看出，所有属性对应的卡巴统计量都大于 0.6，这表明所获得识别结果真实的反映了所建立方法的识别性能。较小的标准差也从另一个方面表明了所建立方法的稳定性和鲁棒性。

7.8.2 训练数据大小的影响

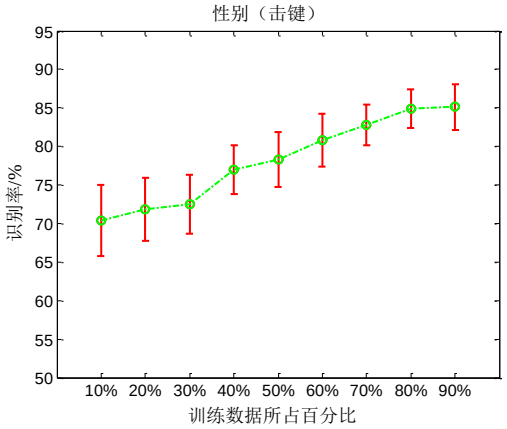
为了分析该技术的安全性（识别率）和可用性（用户数目）之间的关系，本实验检验了训练样本大小对隐私属性识别结果的影响。这里，训练数据的大小对应着训练数据中用户的数目。这个数目的大小在隐私属性识别中起到很重要的作用，因为它关系到能够建立一个可靠的、准确的识别模型所需要的用户数目的多少。在本实验中，我们使该数值从所有用户数目的 10%变化到所有用户数目的 90%，对于每次变化，我们进行了 20 次随机重复实验。

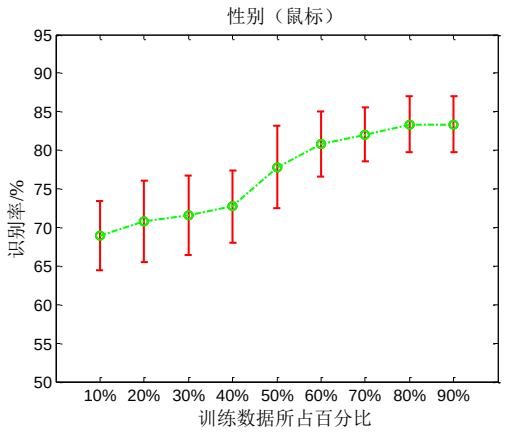
图 7-4 呈现了相关的实验结果。我们可以观察到所有的身份隐私属性识别结果都展现了相同的趋势，对应的识别率都随着训练样本的增加而变好。以基于键盘交互行为的种族识别为例（如（c）所示），当参与训练的用户的数目为总用户数目的 40%时，对应的识别率为 81.71%；随着这一比例增加到 60%，对应的识别率增长到 84.44%。

此外，针对所有隐私属性，我们可以观察到当训练用户的数目比例超过 50%时（大约为 25 名用户），对应的识别率都超过了 80%，并且在此之后继续增大相应的比例时，识别率并没有明显的提升。这从实用的角度说明了我们的方法可以在较小的数据集上

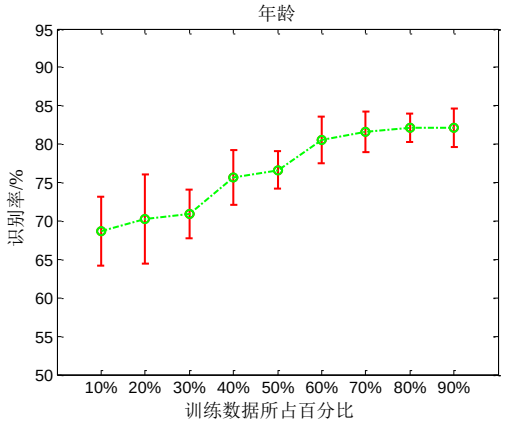
[①] 该行包含了 2 个识别结果，第一行是使用键盘交互行为的结果，第二行是使用鼠标交互行为的结果。

对用户的身份隐私属性进行识别和推测。

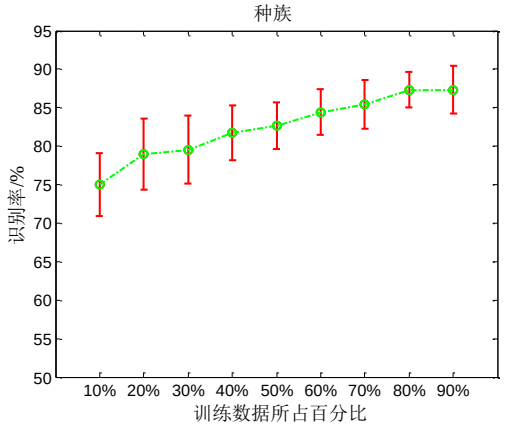




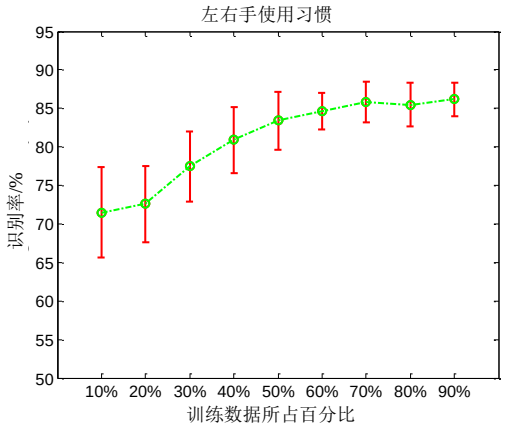
(a) 基于键盘行为和鼠标行为的性别识别



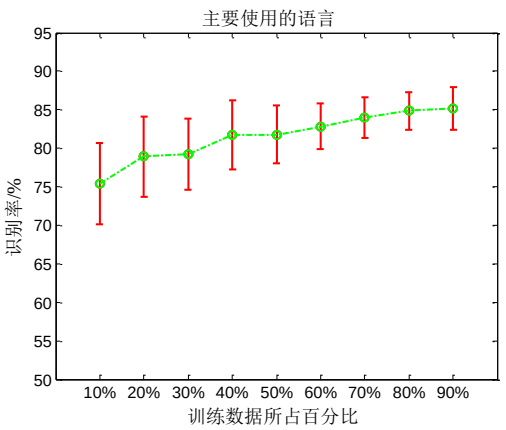
(b) 年龄识别



(c) 种族识别



(d) 左右手使用习惯识别



(e) 主要使用的语言识别

图 7-4 不同身份属性识别结果随训练样本大小变化

7.9 结论

本章提出了一种基于鼠标和键盘交互行为的身份隐私属性识别方法，该方法能够在用户与计算机交互过程中对用户进行持续的分析，且不会对用户的正常行为产生干

扰。通过分析用户操作人机交互设备（鼠标和键盘）所产生的人机交互行为，提取人机交互行为特征，并基于这些特征建立用户的身份隐私属性模型，对用户的身份隐私属性（性别、年龄、种族等）进行识别和推测。该方法填补了在智能计算系统中对操作者身份隐私属性进行分析的空白，为计算机用户信息感知分析提供了一种全新的思路。

8 基于鼠标交互行为的身份认证与监控原型系统

8.1 系统概述

相比于其它身份认证和监控手段（比如密码、指纹），基于鼠标交互行为的身份认证和监控使用标准的计算机输入设备，不需要特殊的硬件设备支持，且鼠标交互行为难以伪造和窃取，因此对系统的准确性和安全性有较高的保障。此外，基于鼠标交互行为的身份认证和监控可在用户正常使用计算机的过程中自动进行，实现无干扰的身份跟踪与监控。

本章在前述利用鼠标交互行为进行身份认证和监控方法研究的基础上，设计并实现了基于鼠标交互行为的身份认证与监控原型系统。该系统在用户登录及使用计算机过程中实时采集用户的鼠标交互行为数据，为合法用户建立身份检测模型，认证及监控当前用户身份，阻止和防御非法用户的侵入。

8.2 系统总体设计

基于鼠标交互行为的身份认证与监控原型系统（Mouse Behavior based Authentication and Monitoring System, MBAMS）主要由三个模块所组成：鼠标交互行为训练、鼠标交互行为认证和鼠标交互行为监控。其功能模块主要包括了数据采集、特征提取、身份认证和身份监控相关的模块。如图 8-1 所示。

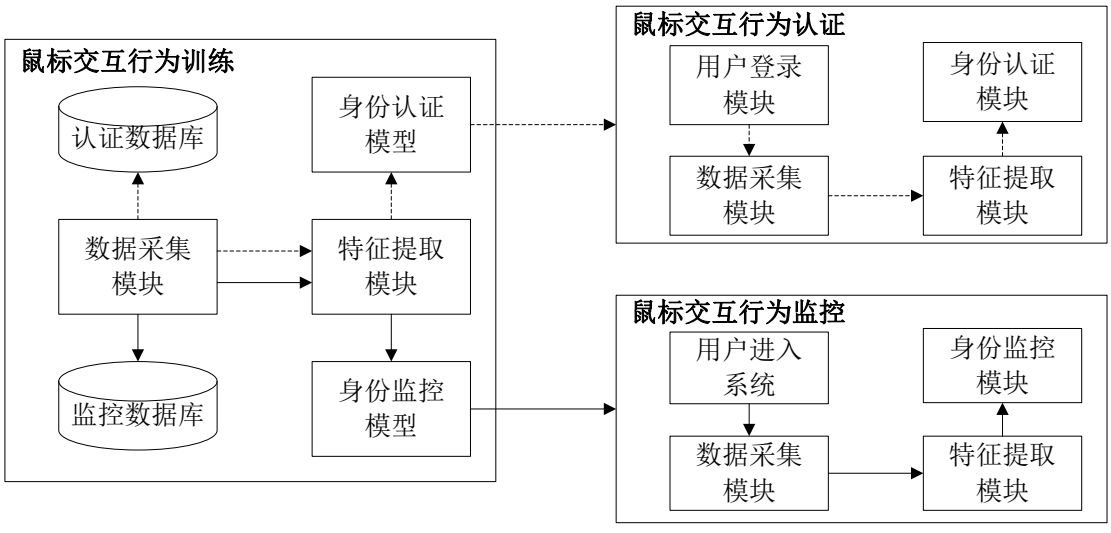


图 8-1 MBAMS 系统总体设计图

鼠标交互行为训练的目的是在某一固定模式下或在监控模式下获取正常用户的鼠标交互行为特征模板，生成对应的身份认证模型和身份监控模型。鼠标交互行为认证的目的是在用户登录计算机的过程中对用户身份进行检验。鼠标交互行为监控的目的

是在用户与计算机的交互过程中，实时监控用户的全局或局部鼠标交互行为，对用户身份的有效性进行检测。监控过程是十分重要的，因为现有的计算机登录并不能完全有效地保护计算机的安全，非法用户仍可以在合法用户登录成功后利用非法操作获取计算机资源。

8.3 系统模块设计

8.3.1 鼠标行为训练模块

用户首先登录 MBAMS 系统，选择鼠标认证模式，完成认证模式的操作并产生对应的鼠标交互行为原始数据，形成鼠标操作样本；从样本中提取出的特征向量加入用户认证特征向量库，当用户的训练特征向量数达到系统要求之后，系统可以通过第 4 章和第 5 章所述的方法，建立身份认证模型；用户也可以选择进行监控场景下的数据采集，形成鼠标操作块，从操作块中提取出特征向量加入用户监控特征向量库，当用户的训练特征向量数达到系统要求之后，系统可以通过第六章所述的方法，建立身份监控模型。

8.3.2 鼠标行为认证模块

用户开启计算机，输入用户名，进入用户选定的鼠标交互行为身份认证模式操作。系统首先使用鼠标消息钩子采集用户鼠标交互操作模式的原始数据，接着提取相关的特征作为认证输入，最后使用在训练阶段身份认证模型，计算输出值，判断用户身份是否合法。

8.3.3 鼠标行为监控模块

用户登录MBAMS系统，开启鼠标交互行为监控功能。在人机交互过程中，系统会自动采集用户的鼠标操作原始数据，并且在用户操作量达到系统要求的时候进行身份合法性的检验，按照设定方式阻断非法用户的操作。

8.4 原型系统实现

8.4.1 系统整体运行流程

计算机启动后可设置自动运行身份监控系统，新用户注册时启动训练模式，训练结束后系统对其训练数据进行分析并提取特征，生成特征模板，保存入特征模板库。

用户登录时，系统启动认证模式，要求用户完成固定的鼠标操作模式，捕获该模式下的鼠标交互行为数据，经过预处理和操作切分，提取相应的特征生成特征模板。随后与特征模板库中的模板进行匹配。若验证为合法用户，用户登入系统；若验证为非法用户，则对当前用户进行阻断，要求用户进行再认证；再认证的过程可以重复三次，三次过后若仍判定为非法用户，则强制锁定计算机。

用户登录后，系统启动监控模式，实时采集当前用户的鼠标交互行为数据，经过

预处理和操作切分后，提取特征并生成当前用户的特征模板。随后，系统将当前监控用户生成的特征模板与注册用户在特征模板库中的模板进行匹配。如果验证结果为非法用户，则对当前用户进行阻断，要求其重新输入密码，在对密码匹配的同时分析其击键行为特征，进行再认证。如果通过验证，则暂时停止监控，并将当前用户的特征模板对特征模板库中注册用户的模板进行更新。验证通过后经过一段设定的时间，或检测到当前用户切换应用环境时则重新激活系统，继续对当前用户身份进行监控，防止内部攻击。图 8-2 描述了系统的详细运行流程。

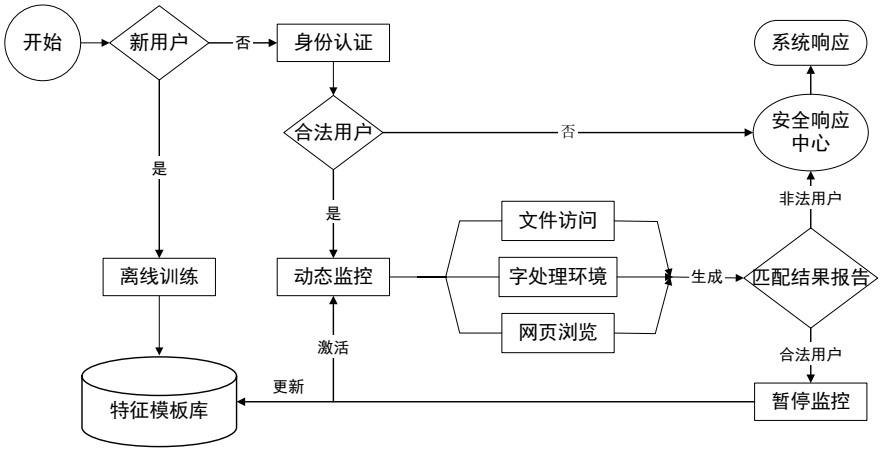


图 8-2 系统运行流程图

8.4.2 鼠标交互行为训练

本系统针对身份认证和身份监控场景设计了二种鼠标行为训练模式：固定模式（Fixed Mode）、自由模式（Free Mode）。用户可以选择不同的模式进行鼠标行为训练，生成不同模式下的鼠标交互行为特征模板和身份模型。

1）固定模式训练：

界面设计与第 4 章的认证场景下的操作模式相同。在一个矩形窗体上设置了 8 个固定位置，在这些位置依次出现方块提示用户单击或者双击。用户认证一次需要完成 16 次移动和 16 次点击，包括 8 次左键单击和 8 次左键双击。在操作过程中，由鼠标原始数据采集子模块记录原始数据点，一旦用户操作出错（如在移动过程中出现点击事件），系统自动提示用户重新进行数据采集，同时删除此次操作的原始数据样本。一次完整操作之后，如果此次训练有新样本生成，系统提取这些新样本的特征模板入库。系统检测该用户该模式下的训练特征模板个数是否符合要求，是则提示用户建立身份认证模型。界面设计如图 8-3 所示：

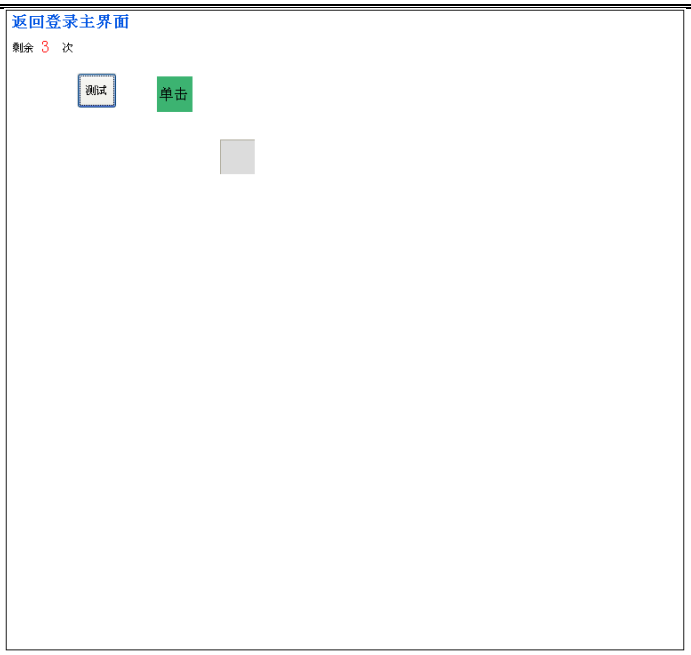


图 8-3 固定模式训练界面

2）自由模式训练：

在自由模式训练期间，用户没有界面模式的限制，可以进行全局人机交互。系统自动采集用户的所有鼠标行为原始数据并在数据达到系统要求之后，生成特征模板和认证网络模型。

8.4.3 鼠标交互行为认证

鼠标行为认证模块的主要功能是使用在鼠标行为模式训练阶段生成的身份模型，对登录计算机的用户身份进行验证。这里将鼠标行为认证功能集成到现有的 Windows 登录模块中，设计并实现了系统的自定义计算机登录界面。

自定义登录模块截图如下所示：

(1) 自定义登录界面如图 8-4 所示：

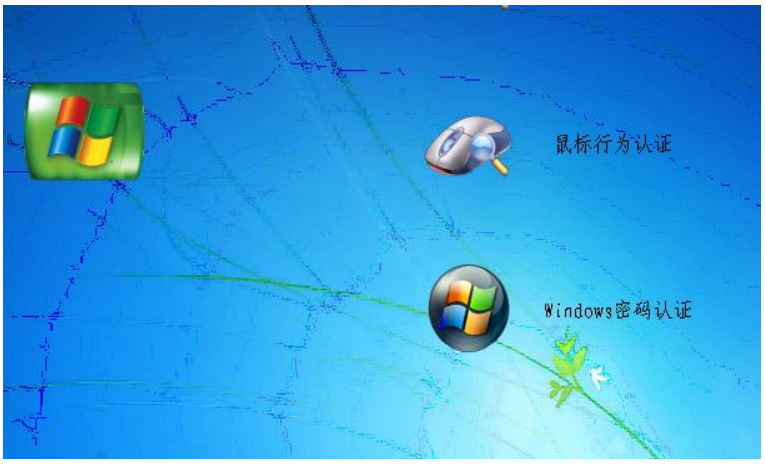


图 8-4 自定义登录界面

(2) 鼠标行为登录用户名输入界面如图 8-5所示：

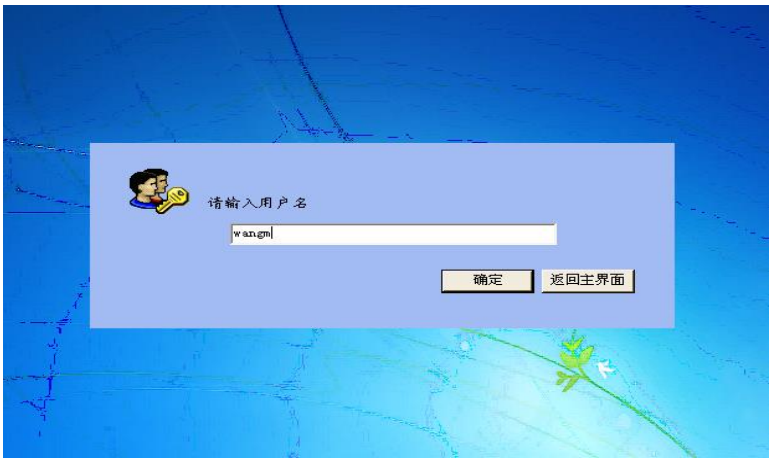


图 8-5 鼠标行为登录用户名输入界面

(3) 鼠标行为登录固定模式认证界面：同鼠标行为固定模式训练界面（见图 8-3）

每次进入Windows桌面前，总会出现一个用户登录的画面，要求输入用户名和密码。本文要在密码登录的基础上增加鼠标行为登录功能，可以通过修改注册表文件中的Winlogon项目来实现。

8.4.4 鼠标交互行为监控

鼠标交互行为监控模块包括三种监控状态，方便用户在不同人机交互环境下进行鼠标行为监控：全局监控（Global Mode）、office 监控（Office Mode）和聊天监控（Chat Mode）。

监控的过程为：系统采集用户鼠标交互行为原始数据，并且在原始数据量达到系统要求时，弹出用户预设的认证模式界面（训练的固定模式）进行身份再认证。如果认证通过，用户可以继续操作；认证未通过，系统按照用户设定的方式阻断用户操作。

全局监控是系统自动采集用户和计算机在任意应用程序下的鼠标交互行为原始数据，并且在数据量达标时，进行用户身份检测，阻断非法用户。

office 监控是系统使用用户在 office 应用程序下的鼠标交互原始数据作为判断，进行用户的身份检测。

聊天监控中，系统采集用户在聊天应用程序(如 QQ、MSN)下的鼠标交互操作原始数据，进行身份检测。

鼠标行为监控模块包括数据采集、身份检测和非法阻断子模块。

(1) 数据采集子模块

系统从用户开启监控功能开始，使用鼠标消息钩子技术自动采集用户的交互原始数据，当原始数据量达到用户预设的要求数量时，根据预设的监控认证模式强制用户进行身份验证。

(2) 身份检测子模块

用户在弹出的强制监控认证模式下进行鼠标操作，生成原始数据样本，提取特征

之后进行身份验证。

(3) 阻断子模块

对认证为非法的用户操作进行阻断，保护计算机资源安全。MBAMS系统共有5种阻断方式，用户可以根据实际需求进行设定。这5种阻断方式包括：

a) 锁定鼠标输入：采取不允许鼠标输入的方式进行阻断。

b) 锁定当前工作站：采取锁定当前工作状态的方式进行阻断。

c) 休眠：采取置计算机于休眠状态的方式进行阻断。

d) 重新启动：采取重新启动计算机的方式进行阻断。

e) 关机：采取关闭计算机的方式进行阻断。

监控设置界面如图 8-6 所示：

图 8-6 监控设置界面

阻断设置界面如图 8-7 所示：

图 8-8 阻断设置界面

8.5 结论

在本文前面部分对鼠标交互行为身份认证和监控方法研究的基础上，本章设计并实现了基于鼠标交互行为的身份认证和监控原型系统。首先对系统整体设计框架与运行流程进行分析，并详细介绍了系统各个子模块的设计与关键技术，包括数据采集与预处理，特征提取与身份模型模板生成。最后实现了系统设计要求的各项功能并介绍系统界面。

9 结论与展望

9.1 工作总结

缺少适合于现有计算环境的有效身份安全分析手段是造成目前信息系统中身份安全问题日益严重的重要原因。口令、身份卡、指纹等身份验证方式，通常需要额外的硬件设备或难以持续性的对用户身份进行分析，而人机交互行为无需记忆或携带，难以被窃取，不需要额外的硬件，且可无缝融入用户与计算机的交互过程，能够实现无干扰的全程身份安全分析。

基于人机交互行为的安全认证和监控是个新兴的研究领域，它利用计算机用户操作人机交互设备时所展现的人机交互行为特征进行身份安全的分析。它是一个复杂而又富有挑战性的研究课题，涉及到多个研究学科的知识，如生物力学、人机交互、模式识别、计算机安全等。目前，国内外的基于人机交互行为的身份安全分析仍处于起步阶段。然而，人机交互行为在身份认证和隐私分析领域的潜在应用激发了研究者们浓厚的兴趣。围绕这个主题，本文以最典型的人机交互设备“鼠标”为研究对象，开展了如下几方面的研究工作：

1) 创建了 XJTUMOUSE 人机交互行为数据库。从操作数、用户数、应用场景而言，它是当前国际上唯一可获得的中等规模的算法评估数据库。该数据库已经向国内外同行共享。

2) 分析了人机交互行为的输入特性，并实现了三种不同的鼠标交互行为数据截获技术：消息钩子、原始输入和过滤驱动，从采样时钟分辨率、时间精度和位置信息等方面对不同方法所获取数据进行了差异分析。分析结果表明使用消息钩子获取的数据最为丰富和稳定。

3) 针对人机交互行为的特征建模问题，从鼠标交互行为的时空轨迹形态分析入手，提出了一种基于光标运动时空轨迹形态特征的身份认证方法。对于每个交互序列而言，提取描述鼠标交互行为时空轨迹形态的特征向量；利用距离度量和成分分析获取低维的鼠标特征量；引入单分类学习器构建身份认证和识别模型。该方法没有直接直接分析轨迹的运动特性，而是间接的捕捉了轨迹的形态结构。大量的实验结果表明该算法获得了令人鼓舞的认证性能。。

4) 针对人机交互行为的行为结构化描述问题，从鼠标交互行为的轨迹形态信息和运动过程信息入手，提出了一种判决级上融合光标轨迹形态特征和运动过程特征的身份认证方法。基于 Box-Cox 幂指数变化和近邻传播聚类分别对形态信息和过程信息进行表示和建模，在决策层对两种信息进行融合。该方法不仅分

析了鼠标运动轨迹的整体形态结构，而且利用轨迹的运动阶段性衍生出一个紧致且细粒度的轨迹描述，间接地捕获了交互行为的结构化特性。在不同融合规则下的实验结果表明：融合后的认证性能均优于使用任何单一模态下的认证性能，能够迅速并且准确对用户身份进行判定。这个结果也鼓励我们在未来的工作中进一步探索任何可能获得的鼠标交互行为线索，并充分融合这些可获得的信息来提高算法的性能。

5) 针对人机交互行为的行为波动性问题，从鼠标交互行为中存在的交互模式入手，提出了一种基于频繁交互行为模式挖掘的身份监控方法。结合计算机用户日常操作鼠标进行交互的特性，利用基于模式生长的序列模式挖掘方法获取频繁的交互行为模式。从这些模式中提取稳定的特征刻画量，对用户的身份进行监控和检测。实验结果表明从行为模式中提取的特征体现了较强的稳定性和可区分性，极大的提升了身份监控和检测的精度。

6) 针对计算机和移动网络环境中用户信息感知的需求，根据“人机交互行为包含身份信息”这一结论，提出了一种基于多种人机交互行为的身份隐私属性感知和分析方法。在随机森林学习框架下，对计算机用户的身份隐私属性进行建模和识别。信息取证分析场景下的实验结果验证了基于鼠标和键盘交互行为对计算机用户的身份隐私属性进行识别和推测的可行性。该方法填补了在智能计算系统中对操作者身份隐私属性进行分析的空白，为计算机用户信息感知分析提供一种新的技术手段。

7) 目前国际上没有一个通用的人机交互行为评估数据库，许多已有的工作都是在各自的小数据库上评估自己的算法性能，还没有人做过不同认证方法和行为分类器之间的性能比较工作。我们针对目前一些主要的身份认证方法、监控方法和行为分类器进行了定量的性能评价和比较，同时也对其它方法进行了一定程度上的定性分析。在实验结果的基础上，获得了一些有益的结论和启示。

8) 在上述研究的基础上，设计并实现了基于鼠标交互行为的身份认证和监控原型系统。该系统在用户登录及使用计算机过程中采集用户的鼠标交互行为数据，为正常用户建立行为特征模型，认证及监控当前用户身份，有效阻止和防御非法用户的侵入。

综上所述，本文在人机交互行为特征的提取和刻画、人机交互行为的认证和监控、人机交互行为的隐私分析等方面做了一些尝试和探索，并取得了一定的研究成果。

9.2 未来展望

尽管我们在文章中提出了几种基于人机交互行为的身份认证和监控方法，但就象现有的许多方法一样，它们都或多或少的存在一些局限，如受控的实验环境、模式的依赖性、小的评估数据库等。因此许多问题仍有待进一步的研究和完善。

1) 更加鲁棒的特征提取

运动轨迹分析对于人机交互过程性特征的提取是个关键。就鼠标交互行为而言，我们需要分割和识别运动轨迹分段，而且需要从轨迹分段中获取鼠标行为特征。它们性能的好坏直接影响了后续鼠行为特征的稳定性和可区分性。象大多数基于鼠标交互行为的身份认证方法一样，在我们的实验中，认证场景下的鼠标操作模式相对而言是比较简单的，而且限定了用户是按照预设的轨迹进行移动的，这对于未来实际的鼠标交互行为的身份认证是不够的。因此，相关于鼠标运动轨迹分析的分割和识别技术必须完善和改进。

就运动轨迹分割和识别而言，它是个相当困难的问题。这是由于交互过程中捕获的行为数据受到多方面的影响，比如鼠标类型、屏幕分辨率、用户身体状况、用户坐姿等。如何建立对于各种环境因素的动态变化均具有自适应性的轨迹分割模型仍是严峻的挑战。目前大部分运动轨迹的分析都不能很好地解决运动阶段的划分问题，尤其是在监控场景下，运动轨迹的多样性和复杂性问题更是难以处理。为了减少轨迹多样性所带来的问题，我们必须开发更好的模型来处理运动轨迹的归类问题。可喜的进步在于利用相似行为自聚类的方法可以获得运动轨迹的统计类别信息；不过，对于解决运动轨迹分割和识别问题最有实际意义的潜在方法也许是在概率图模型框架下采用条件随机场等推理模型得到轨迹分段的边界定位，从而实现运动轨迹的自适应分段与弹性匹配。这是我们未来工作的一个主要方向。

2) 创建更大规模的评估数据库

当前基于人机交互行为的身份安全的研究局限是缺乏一个标准的人机交互行为评估数据库。尽管早期的基于人机交互行为的身份认证和监控研究展现了令人鼓舞的结果，然而人的人机交互行为，不像虹膜和指纹，未必对于个体而言是唯一的。因此，进一步的评估人机交互行为作为一种生物特征的潜力是非常重要的。

在身份认证和监控领域，数据库的质量和规模是两个非常重要的因素。我们实验中的数据库的规模偏小，因此创建更大的数据库来测试算法的性能是完全必要的。创建用于开发目的、具有一定规模的通用数据库和标准测试协议必将有益于人机行为认证和监控方法的开发和评估。这些数据库必须包含影响人机交互行为感知的因素变化，如人机交互设备类型、屏幕分辨率等。只有更大规模，更加实际的数据库(更多的用户数、操作数、条件变化数等)才允许我们对获取的人机交互行为特征的局限性有所开发。

3) 多种人机交互行为特征的融合

选择不同的行为特征对于身份认证和监控而言有着不同的分辨能力，利用不同特征的组合作为扩展特征对于提高人机交互行为认证和监控的效果是必然趋势。形态与过程特性相结台的行为认证和监控是个有前景的方向，这已经在过去的工作中得到验证。人机交互行为不仅包括运动轨迹的形态变化，而且也包括其运动过程的动态特性。当然，不同的分类器和相似性度量函数也将直接影响着身份认证和监控性能。目前，

我们的分类方法比较简单，因此寻找更加成熟的分类方法至关重要。

4) 人机交互行为对多生物特征融合的贡献

多生物特征的身份监控技术是指融合多个生物特征，或者在多个不同的生物特征之间依据不同的操作条件进行切换，选择最为合适的特征进行身份监控的方法。考虑到鼠标交互行为和键盘交互行为都具有无干扰的优点，因此在身份监控系统中可以选择它们作为生物特征用于动态身份监控。当键盘不可用时可以利用鼠标交互行为进行身份监控；当鼠标不可用时可以利用键盘交互行为进行身份监控；当两者都可用的时候可以融合两种交互行为特征进行身份监控来提高身份监控的准确度。

5) 其它人机交互行为特征的研究

对鼠标/键盘交互行为以外的人机交互行为特征进行研究。当前的研究还没有涉及到鼠标/键盘以外的其它人机交互设备如触摸屏、指点杆的行为特征，这些设备作为图形交互界面下的重要输入方式，包含了更加丰富的信息源，如触摸或指点的力度等，所以有可能比鼠标交互行为更能展现出用户身份的行为特征。

总之，我们未来的工作可以集中于以下几个方面：

（1）创建更大、更实际的数据库来评估方法；（2）开发更加鲁棒的运动轨迹分割和识别方法；（3）融合鼠标交互行为自身的多特征用于身份安全分析；（4）评估影响系统性能的关键性因素；（5）设计性能更好的分类器；（6）尝试性地研究其它人机交互行为特征等。

参考文献

[1] 中国互联网络信息中心. 2012年中国网民信息安全状况研究报告. CNNIC: 北京, 2012年12月.

[2] 卡巴斯基. 2011卡巴斯基安全公告. 2012年3月.

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

[4] Daugman J. How iris recognition works[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2004, 14(1): 21-30.

[5] Frumkin D, Wasserstrom A, Davidson A, et al. Authentication of forensic DNA samples[J]. Forensic Science International: Genetics, 2010, 4(2): 95-103.

[6] Jain AK, Ross A, Pankanti S. Biometrics: a tool for information security[J]. IEEE Transactions on Information Forensics and Security, 2006, 1 (2): 125-143.

[7] Maio D, Jain AK. Handbook of fingerprint recognition[M]. Springer, 2009.

[8] Jain AK, Bolle RM, Pankanti S. Biometrics: Personal identification in networked society[M]. Springer, 1999.

[9] Delac K, Grgic M. A survey of biometric recognition methods[C]. Proceedings of 46th International Symposium on Electronics in Marine, 2004: 184-193.

[10] Wayman JL, Jain AK, Maltoni D, et al. Biometric systems: technology, design and performance evaluation[M]. Springer, 2005.

[11] Faundez-Zanuy M. On-line signature recognition based on VQ-DTW[J]. Pattern Recognition, 2007, 40(3): 981-992.

[12] Han J, Bhanu B. Individual recognition using gait energy image[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2006, 28(2): 316-322.

[13] Li M, Tieniu T, Yunhong W, et al. Efficient iris recognition by characterizing key local variations[J]. IEEE Transactions on Image Processing, 2004, 13(6): 739-750.

[14] Monrose F, Rubin AD. Keystroke dynamics as a biometric for authentication[J]. Future Generation Computer Systems, 2000, 16(4): 351-359.

[15] Phillips PJ, Hyeonjoon M, Rizvi SA, et al. The FERET evaluation methodology for face-recognition algorithms[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2000, 22(10): 1090-1104.

[16] Van Lancker D, Kreiman J. Voice discrimination and recognition are separate abilities[J]. Neuropsychologia, 1987, 25(5): 829-834.

[17] Raskin J. The humane interface: new directions for designing interactive systems[M]: Addison-Wesley Professional, 2000.

[18] Gaines RS, William Lisowski, Press SJ, et al. Authentication by Keystroke Timing: Some Preliminary Results[R]. RAND Corporation: Santa Monica, Calif., 1980.

[19] Joyce R, Gupta G. Identity authentication based on keystroke latencies[J]. ACM Communication, 1990, 33 (2): 168-176.

[20] Bergadano F, Gunetti D, Picardi C. User authentication through keystroke dynamics[J]. ACM Transactions on Information and System Security, 2002, 5(4): 367-397.

[21] Cho S, Han C, Han DH, et al. Web-based keystroke dynamics identity verification using neural network[J]. Journal of Organizational Computing and Electronic Commerce, 2000, 10(4): 295-307.

[22] Cho SZ, Hwang S. Artificial rhythms and cues for keystroke dynamics based authentication[J].

Proceedings of Advances in Biometrics, 2006, 3832: 626-632.
[23] Choe YG, Kim SJ. Secure password authentication for keystroke dynamics[J]. Knowledge-Based Intelligent Information and Engineering Systems, 2005, 3683: 317-324.
[24] e Silva SRD, Roisenberg M. Continuous authentication by keystroke dynamics using committee machines[J]. Intelligence and Security Informatics, 2006, 3975: 686-687.
[25] Hwang SS, Lee HJ, Cho S. Improving authentication accuracy of unfamiliar passwords with pauses and cues for keystroke dynamics-based authentication[J]. Intelligence and Security Informatics, 2006, 3917: 73-78.
[26] Kotani K, Horii K. Evaluation on a keystroke authentication system by keying force incorporated with temporal characteristics of keystroke dynamics[J]. Behaviour & Information Technology, 2005, 24(4): 289-302.
[27] Sang YP, Shen H, Fan PZ. Novel impostors detection in keystroke dynamics by support vector machine[J]. Parallel and Distributed Computing: Applications and Technologies, 2004, 3320: 666-669.
[28] Yu E, Cho S. Novelty detection approach for keystroke dynamics identity verification[J]. Intelligent Data Engineering and Automated Learning, 2003, 2690: 1016-1023.
[29] Yu EZ, Cho S. Keystroke dynamics identity verification - its problems and practical solutions[J]. Computers & Security, 2004, 23(5): 428-440.
[30] Ahmed AAE, Traore I. Anomaly intrusion detection based on biometrics[C]. Proceedings of the Sixth Annual IEEE SMC Information Assurance Workshop, 2005: 452-453.
[31] Ahmed AAE, Traore I. Detecting computer intrusions using behavioral biometrics. Proceedings of Third Annual Conference on Privacy Security and Trust, 2005.
[32] Ahmed AAE, Traore I. A new biometric technology based on mouse dynamics[J]. IEEE Transactions on Dependable and Secure Computing, 2007, 4(3): 165-179.
[33] Ahmed AAE, Traore I. Dynamic sample size detection in continuous authentication using sequential sampling. Proceedings of the 27th Annual Computer Security Applications Conference. ACM: Orlando, Florida, 2011: 169-176.
[34] Shen C, Cai ZM, Guan XH, et al. Feature Analysis of Mouse Dynamics in Identity Authentication and Monitoring[C]. Proceedings of the IEEE International Conference on Communications: Dresden, Germany, 2009: 1-5.
[35] Shen C, Cai ZM, Guan XH, et al. A hypo-optimum feature selection strategy for mouse dynamics in continuous identity authentication and monitoring[C]. Proceedings of IEEE International Conference on Information Theory and Information Security, 2010: 349-353.
[36] Shen C, Cai ZM, Guan XH, et al. User Authentication Through Mouse Dynamics[J]. IEEE Transactions on Information Forensics and Security, 2013, 8 (1): 16-30.
[37] Zwiesele A, Munde A, Busch C, et al. BioIS study. Comparative study of biometric identification systems[C], 2000: 60-63.
[38] Kang PS, Park S, Cho SZ, et al. The effectiveness of artificial rhythms and cues in keystroke dynamics based user authentication[J]. Intelligence and Security Informatics, 2006, 3917: 161-162.
[39] Lee H, Cho SZ. Retraining a novelty detector with impostor patterns for keystroke dynamics-based authentication[J]. Advances in Biometrics, 2006, 3832: 633-639.
[40] Revett K, de Magalhaes ST, Santos HMD. Enhancing login security through the use of keystroke input dynamics[J]. Advances in Biometrics, 2006, 3832: 661-667.
[41] Rodrigues RN, Yared GFG, Costa CRD, et al. Biometric access control through numerical keyboards based on keystroke dynamics[J]. Advances in Biometrics, 2006, 3832: 640-646.
[42] Sung K, Cho SZ. GA SVM wrapper ensemble for keystroke dynamics authentication[J]. Advances in Biometrics, 2006, 3832: 654-660.

[43] Lee HJ, Cho S. Retraining a keystroke dynamics-based authenticator with impostor patterns[J]. Computers & Security, 2007, 26(4): 300-310.

[44] Minetti AE, Ardigo LP, Mckee T. Keystroke dynamics and timing: Accuracy, precision and difference between hands in pianist's performance[J]. Journal of Biomechanics, 2007, 40(16): 3738-3743.

[45] Campisi P, Maiorana E, Lo Bosco M, et al. User authentication using keystroke dynamics for cellular phones[J]. IET Signal Processing, 2009, 3(4): 333-341.

[46] Hwang SS, Cho S, Park S. Keystroke dynamics-based authentication for mobile devices[J]. Computers & Security, 2009, 28(1-2): 85-93.

[47] Killourhy KS, Maxion RA. Free vs. transcribed text for keystroke-dynamics evaluations[C]. Proceedings of the 2012 Workshop on Learning from Authoritative Security Experiment Results, Arlington, Virginia, 2012: 1-8.

[48] Checco JC. Keystroke Dynamics & Corporate Security. Ticker, WallStreet Technology Association, 2006.

[49] DARPA. Active Authentication Defense Advanced Research Projects Agent, 2012.

[50] Yampolskiy RV, Govindaraju V. Behavioural biometrics: a survey and classification[J]. International Journal of Biometrics, 2008, 1(1): 81-113.

[51] Forrest S, Hofmeyr S, Somayaji A. The Evolution of System-Call Monitoring. Proceedings of the 2008 Annual Computer Security Applications Conference, 2008: 418-430.

[52] Fitts PM. The information capacity of the human motor system in controlling the amplitude of movement.[J]. Journal of Experimental Psycholog, 1954, 47(6): 381-391.

[53] Abernethy B, Kippers V, Hanrahan SJ, et al. Biophysical foundations of human movement[M]: Human Kinetics, 2013.

[54] Everitt RAJ, McOwan PW. Java-based Internet biometric authentication system[J]. Ieee Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(9): 1166-1172.

[55] Gamboa H, Fred ALN, Jain AK. Webbiometrics: user verification via web interaction[C]. Biometrics Symposium, 2007, 2007: 1-6.

[56] Nazar A. Synthesis & Simulation of Mouse Dynamics[D]. University of Victoria, 2007.

[57] Asha S, Chellappan C. Authentication of e-learners using multimodal biometric technology[C]. Proceedings of the International Symposium on Biometrics and Security Technologies, 2008: 1-6.

[58] Fullu CJ. Login session using mouse biometrics[D]. 2008.

[59] Kaklauskas A, Zavadskas EK, Seniut M, et al. Web-based biometric mouse decision support system for user's emotional and labour productivity analysis[C]. Proceedings of The 25th International Symposium on Automation and Robotics in Construction, Lithuania, 2008: 69-75.

[60] Kaminsky R, Enev M, Andersen E. Identifying game players with mouse biometrics[R]. Technical Report, University of Washington, 2008.

[61] Nazar A, Traore I, Ahmed AAE. Inverse biometrics for mouse dynamics[J]. International Journal of Pattern Recognition and Artificial Intelligence, 2008, 22(3): 461-495.

[62] Revett K, Jahankhani H, Magalh ães ST, et al. A Survey of User Authentication Based on Mouse Dynamics[C]. Proceedings of 4th International Conference on Global E-Security. Springer Berlin Heidelberg: London, UK, 2008: 210-219.

[63] Aksari Y, Artuner H. Active authentication by mouse movements[C]. Proceedings of the 24th International Symposium on Computer and Information Sciences, 2009: 571-574.

[64] Bours P, Fullu CJ. A Login System Using Mouse Dynamics[C]]. Proceedings of the Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2009: 1072-1077.

[65] Hamdy O, Traore I. Cognitive-Based Biometrics System for Static User Authentication[C].

Proceedings of the Fourth International Conference on Internet Monitoring and Protection, 2009: 90-97.

[66] Kaklauskas A, Krutinis M, Seniut M. Biometric Mouse Intelligent System for Student's Emotional and Examination Process Analysis[C]. Proceedings of the Ninth IEEE International Conference on Advanced Learning Technologies, 2009: 189-193.

[67] Moskovitch R, Feher C, Messerman A, et al. Identity theft, computers and behavioral biometrics[C]. Proceedings of IEEE International Conference on Intelligence and Security Informatics, 2009: 155-160.

[68] Sayed B. A Static Authentication Framework Based On Mouse Gesture Dynamics[D]. University of Victoria, 2009.

[69] Wobbrock JO, Fogarty J, Liu S-Y, et al. The angle mouse: target-agnostic dynamic gain adjustment based on angular deviation[C]. Proceedings of the 27th international conference on Human factors in computing systems. Boston, MA, USA, 2009: 1401-1410.

[70] Nakkabi Y, Traore I, Ahmed AAE. 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.

[71] Rustighi E, Dohnal F, Mace BR. Influence of disturbances on the control of PC-mouse, goal-directed arm movements[J]. Medical Engineering &amp Physics, 2010, 32(9): 974-984.

[72] al-Khateeb H. Security and usability in click-based authentication systems[D]. 2011.

[73] Boopathi M, Vani M. Enhanced Authentication Using Keystroke and Mouse Dynamics[J]. Advanced Materials Research, 2011, 214: 230-234.

[74] Dehnavi MK, Fard NP. Presenting a multimodal biometric model for tracking the students in virtual classes[J]. Procedia-Social and Behavioral Sciences, 2011, 15(0): 3456-3462.

[75] Hamdy O, Traore I. Homogeneous Physio-Behavioral Visual and Mouse-Based Biometric[J]. ACM Transactions on Computer-Human Interaction, 2011, 18(3): 1202-1230.

[76] Jorgensen Z, Yu T. On mouse dynamics as a behavioral biometric for authentication[C]. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, Hong Kong, China, 2011: 476-482.

[77] Shen C, Cai Z, Guan X. Can it be more practical?: improving mouse dynamics biometric performance. Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011: 853-856.

[78] Zheng N, Paloski A, Wang H. An efficient user verification system via mouse movements[C]. Proceedings of the 18th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2011: 139-150.

[79] Chien-Cheng L, Chin-Chun C, Deron L. A New Non-intrusive Authentication Approach for Data Protection Based on Mouse Dynamics[C], 2012: 9-14.

[80] Feher C, Elovici Y, Moskovitch R, et al. User identity verification via mouse dynamics[J]. Information Sciences, 2012, 201(0): 19-36.

[81] Lin CC, Chang CC, Liang D, et al. A New Non-Intrusive Authentication Approach for Data Protection Based on Mouse Dynamics[C]. Proceedings of International Symposium on Biometrics and Security Technologies, Taibei, 2012: 9-14.

[82] Mondal S, Bours P. Continuous authentication using mouse dynamics[C], 2013: 1-12.

[83] Sayed B, Traore I, Woungang I, et al. Biometric Authentication Using Mouse Gesture Dynamics[J]. IEEE Systems Journal, 2013, 7(2): 262-274.

[84] Gianvecchio S, Wu Z, Xie M, et al. Battle of Botcraft: fighting bots in online games with human observational proofs[C]. Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA, 2009: 256-268.

[85] Guo Q, Agichtein E, Clarke C, et al. Understanding "Abandoned" Ads: Towards Personalized Commercial Intent Inference via Mouse Movement Analysis[C]. SIGIR 2008 Workshop on Information Retrieval in Advertising, Singapore, 2008.

[86] Chao S, Zhongmin C, Xiaohong G. Continuous authentication for mouse dynamics: A pattern-growth approach[C], 2012: 1-12.

[87] Schwartz B, Wasserman EA, Robbins SJ. Psychology of learning and behavior[M]. New York, 2002.

[88] Pfleeger CP, Pfleeger SL. Security in computing[M]: Prentice Hall PTR, 2006.

[89] Crossman ERFW, Goodeve PJ. Feedback control of hand-movement and Fitts' law[J]. The Quarterly Journal of Experimental Psychology Section A, 1983, 35(2): 251-278.

[90] MacKenzie IS, Buxton W. Extending Fitts' law to two-dimensional tasks[C]. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Monterey, California, USA, 1992: 219-226.

[91] MacKenzie IS. Fitts' law as a research and design tool in human-computer interaction[J]. Hum-Comput Interact, 1992, 7(1): 91-139.

[92] Standardization IOf. ISO 9241-11: Ergonomic Requirements for Office Work with Visual Display Terminals (VDTs): Part 11: Guidance on Usability[M]. 1998.

[93] Soukoreff RW, MacKenzie IS. Towards a standard for pointing device evaluation, perspectives on 27 years of Fitts' law research in HCI[J]. International Journal of Human-Computer Studies, 2004, 61(6): 751-789.

[94] Card SK, English WK, Burr BJ. Evaluation of Mouse, Rate-Controlled Isometric Joystick, Step Keys, and Text Keys for Text Selection on a CRT[J]. Ergonomics, 1978, 21(8): 601-613.

[95] Kotani K, Horii K. A fundamental study on pointing force applied to the mouse in relation to approaching angles and the index of difficulty[J]. International Journal of Industrial Ergonomics, 2001, 28(3–4): 189-195.

[96] Boritz J, Booth KS, Cowan WB. Fitts's Law studies of directional mouse movement[C], 1991: 216-223.

[97] Whisenand TG, Emurian HH. Analysis of cursor movements with a mouse[J]. Computers in Human Behavior, 1999, 15(1): 85-103.

[98] Thompson SG, McConnell DS, Slocum JS, et al. Kinematic analysis of multiple constraints on a pointing task[J]. Human Movement Science, 2007, 26(1): 11-26.

[99] Gamboa H, Fred A. An Identity authentication system based on human computer interaction behaviour. In: Ogier J, Trupin E, editors. Proceedings of the 3rd International Workshop on Pattern Recognition in Information Systems. ICEIS Press, 2003.

[100] Pusara M, Brodley CE. User re-authentication via mouse movements[C]. Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security, Washington DC, USA, 2004: 1-8.

[101] :Hashia S, Pollettb C, Stampc M, et al. On using mouse movements as a biometric[C]. Proceedings of the International Conference on Computer Science and its Applications, 2005.

[102] Schulz DA. Mouse curve biometrics. Biometric Consortium Conference, Biometrics Symposium: Special Session on Research at the, 2006: 1-6.

[103] Garg A, Vidyaraman S, Upadhyaya S, et al. USim: a user behavior simulation framework for training and testing IDSes in GUI based systems[C]. Proceedings of the 39th Annual Simulation Symposium, 2006.

[104] Hocquet S, Ramel J, Cardot H. Users authentication by a study of human computer interactions[C]. Proceedings of the 8th Annual (Doctoral) Meeting on Health, Science and Technology, 2004.

[105] Shen C, Cai ZM, Guan XH, et al. On the effectiveness and applicability of mouse dynamics

biometric for static authentication: A benchmark study[C]. Proceedings of 5th IAPR International Conference on Biometrics, 2012: 378-383.

[106] Syukri A, Okamoto E, Mambo M. A user identification system using signature written with mouse[J]. Information Security and Privacy. Springer Berlin Heidelberg, 1998: 403-414.

[107] Shen C, Cai ZM, Maxion RA, et al. On User Interaction Behavior as Evidence for Computer Forensic Analysis[C]. Proceedings of 12th International Workshop on Digital-Forensics and Watermarking: CBD Auckland, New Zealand, 2013.

[108] Ting-Yi Chang Y-JY, Chun-Cheng Peng. A personalized rhythm click-based authentication system[J]. Information Management & Computer Security, 2010, 18(2): 72 - 85.

[109] Mark E, Solomon RDA. 深入解析 Windows 操作系统. 北京: 电子工业出版社, 2007.

[110] Richter J. Windows 核心编程[M]: 机械工业出版社, 2000.

[111] 谭文, 杨潇, 邵坚磊. 寒江独钓: Windows 内核安全编程[M]: 电子工业出版社, 2009.

[112] Killourhy KS, Maxion RA. Comparing anomaly-detection algorithms for keystroke dynamics[C]. Proceedings of IEEE/IFIP International Conference on Dependable Systems & Networks, 2009: 125-134.

[113] Schölkopf B, Smola AJ, Müller K-R. Kernel principal component analysis[C]. Proceedings of Advances in kernel methods, MIT Press, 1999: 327-352.

[114] Schölkopf B, Smola A, Müller K-R. Nonlinear Component Analysis as a Kernel Eigenvalue Problem[J]. Neural Computation, 1998, 10(5): 1299-1319.

[115] Tax D. J. One-class classification: concept-learning in the absence of counter-examples[D]. Delft University of Technology, 2001.

[116] Markou M, Singh S. Novelty detection: a review—part 2:: neural network based approaches[J]. Signal Processing, 2003, 83(12): 2499-2521.

[117] Markou M, Singh S. Novelty detection: a review—part 1: statistical approaches[J]. Signal Processing, 2003, 83(12): 2481-2497.

[118] Schölkopf B, Platt JC, Shawe-Taylor J, et al. Estimating the Support of a High-Dimensional Distribution[J]. Neural Computation, 2001, 13(7): 1443-1471.

[119] Schölkopf B, Williamson RC, Smola AJ, et al. Support Vector Method for Novelty Detection[C]. Proceedings of Neural Information Processing Systems, 1999.

[120] Chang C-C, Lin C-J. LIBSVM: A library for support vector machines[J]. ACM Transactions on Intelligent Systems and Technology, 2011, 2(3): 1-27.

[121] Duda RO, Hart PE, Stork DG. Pattern classification[M]. New York: John Wiley, Section, 2001, 10: l.

[122] Kohavi R. A study of cross-validation and bootstrap for accuracy estimation and model selection[C]. Proceedings of International Conference on Artificial Intelligence, 1995: 1137-1145.

[123] Swets J. Evaluation of diagnostic systems[M]. Access Online via Elsevier, 1982.

[124] Bengio S, Mariéthoz J. A statistical significance test for person authentication[C]. Proceedings of Speaker and Language Recognition Workshop, 2004.

[125] CENELEC. European Standard EN 50133-1: Alarm systems. Access control systems for use in security applications, Part 1: System requirements, Standard Number EN 50133-1:1996/A1[R]. European Committee for Electrotechnical Standardization, 2005.

[126] Mika S, Schölkopf B, Smola AJ, et al. Kernel PCA and De-Noising in Feature Spaces[C]. Proceedings of Neural Information Processing Systems, 1998: 536-542.

[127] Efron B, Tibshirani R. An introduction to the bootstrap[M]. CRC press, 1993.

[128] Bowman AW, Azzalini A. Applied smoothing techniques for data analysis[M]. Oxford Statistical Science Series,1997.

[129] Frey BJ, Dueck D. Clustering by Passing Messages Between Data Points[J]. Science, 2007,

315(5814): 972-976.

[130] Kaufman L, Rousseeuw PJ. Finding groups in data: an introduction to cluster analysis[M]. Wiley. com, 2009.

[131] Van Der Heiden R, Groen FCA. The box-cox metric for nearest neighbour classification improvement[J]. Pattern Recognition, 1997, 30(2): 273-279.

[132] Srisuk S, Petrou M, Fooprateep R, et al. A Combination of Shape and Texture Classifiers for a Face Verification System[C]. Proceedings of Biometric Authentication. Springer Berlin Heidelberg, 2004: 44-51.

[133] Rodríguez-Liñares L, García-Mateo C, Luis Alba-Castro J. On combining classifiers for speaker authentication[J]. Pattern Recognition, 2003, 36(2): 347-359.

[134] Czyz J, Kittler J, Vandendorpe L. Multiple classifier combination for face-based identity verification[J]. Pattern Recognition, 2004, 37(7): 1459-1469.

[135] Kittler J, Hatef M, Duin RPW, et al. On combining classifiers[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, 20(3): 226-239.

[136] Yitzhaki S. Gini's Mean difference: a superior measure of variability for non-normal distributions[J]. Metron-International Journal of Statistics, 2003, 61(2): 285-316.

[137] Wu K, Childers DG. Gender recognition from speech. Part I: Coarse analysis[J]. The Journal of the Acoustical Society of America, 1991, 90(4): 1828-1840.

[138] Bocklet T, Maier A, Bauer JG, et al. Age and gender recognition for telephone applications based on GMM supervectors and support vector machines[C]. IEEE International Conference on Acoustics, Speech and Signal Processing, 2008: 1605-1608.

[139] Makinen E, Raisamo R. Evaluation of Gender Classification Methods with Automatically Detected and Aligned Faces[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2008, 30(3): 541-547.

[140] Moghaddam B, Ming-Hsuan Y. Learning gender with support faces[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2002, 24(5): 707-711.

[141] Badawi A, Mahfouz M, Tadross R, et al. Fingerprint-Based Gender Classification[C]. Proceedings of IPCV, 2006.

[142] Wang J-F, Lin C-L, Chang Y-H, et al. Gender determination using fingertip features[J]. Internet Journal of Medical Update-EJOURNAL, 2008, 3(2).

[143] Xuelong L, Maybank SJ, Shuicheng Y, et al. Gait Components and Their Application to Gender Recognition[J]. IEEE Transactions onSystems, Man, and Cybernetics, Part C: Applications and Reviews, 2008, 38(2): 145-155.

[144] Jiwen L, Yap-Peng T. Gait-Based Human Age Estimation[J]. IEEE Transactions on Information Forensics and Security, 2010, 5(4): 761-770.

[145] Giot R, Rosenberger C. A new soft biometric approach for keystroke dynamics based on gender recognition[J]. International Journal of Information Technology and Management, 2012, 11(1): 35-49.

[146] Chawla NV, Japkowicz N, Kotcz A. Editorial: special issue on learning from imbalanced data sets[J]. SIGKDD Explor Newsl, 2004, 6 (1): 1-6.

[147] Breiman L. Random Forests[J]. Machine Learning, 2001, 45(1): 5-32.

附 录

个人简历

1985.09.29　　出生于陕西西安，籍贯四川省万县市，成长于陕西省西安市。

2003.09～2007.7　　西安交通大学电子与信息工程学院本硕连读专业。

2007.09～2009.02　　西安交通大学电子与信息工程学院硕博连读专业硕士阶段。

2009.03 至今　　西安交通大学电子与信息工程学院硕博连读专业博士阶段。

2011.02～2013.08　　美国卡内基梅隆大学计算机学院联合培养，指导老师为 Roy Maxion 教授

博士期间的荣誉和奖励

[1] 2013　　全国生物特征识别会议最佳论文

[2] 2012-2013　　博士新人奖助学金 / 国家奖学金

[3] 2011-2013　　中国留学生奖学金

[4] 2012　　新兴一等奖学金

[5] 2011　　西门子奖学金

[6] 2010　　中国航天科技奖学金

[7] 2009-2010　　国家自然创新基金一等奖学金

[8] 2009　　微软精英大挑战校内赛一等奖

[9] 2007-2012　　西安交通大学优秀研究生

[10] 2007-2008　　国家自然创新基金奖学金

[11] 2007　　国际大学生北美数学建模竞赛二等奖

博士期间参加的科研项目

[1] 基于行为模型的桌面安全阻断系统的研究与实现（863计划项目，编号：2007AA01Z464）

[2] 大规模网络化系统的优化、安全与信息服务（国家自然科学基金创新群体基金，编号：60921003）

[3] 下一代 e-Learning 系统的关键理论与技术（国家杰出青年科学基金，60825202）

[4] 基于指点触控行为的身份认证与监控方法研究（国家自然科学基金，编号：61175039）

[5] 图形交互环境中的生物行为特征建模与分析（教育部博士点基金，编号：20070698107）

[6] 基于人机交互行为的身份认证与监控方法研究（陕西省国际合作项目，编号：2013KW11）

博士期间的主要学术活动

[1] 2011.02-2013.08　　美国卡内基梅隆大学联合培养.

[2] 2013.10　　在第12届信息取证和数字水印大会上作学术报告.新西兰奥克兰

[3] 2012.09　　在第5届生物测定学理论/方法/应用大会上作学术报告.美国华盛顿.

[4] 2012.06　　在第42届可靠性系统和网络大会上作学术报告.美国波士顿.

[5] 2012.05 在美国卡内基梅隆大学计算机系作学术报告.美国匹兹堡.

[6] 2011.10 在第12届计算机网络与通信安全大会上作学术报告.美国芝加哥.

[7] 2010.10 在第3届信息系统与安全大会上作学术报告.中国北京.

[8] 2009.06 在第22届世界通信大会上作学术报告.德国德雷斯顿.

致　谢

衷心感谢我的导师管晓宏教授和蔡忠闽副教授在我攻读博士期间从学习、生活和科研力面给予的无微不至的关怀和孜孜不倦的教诲。论文从开始的选题到最后的修改都是在管老师和蔡老师的悉心指导下完成的。管老师渊博的学识和敏锐的学术眼光拓宽了我的视野；他对事业的执著追求和严谨的治学态度使我深受鼓舞。蔡老师在工作中对我严格要求，在生活中为我排忧解难，从论文选题、课题研究、论文撰写的整个过程中，都浸透着蔡老师的帮助和关心。蔡老师忘我的科研精神和严谨的治学态度更是我学习的楷模。

感谢美国卡内基梅隆大学 Roy Maxion 教授！在美国为期二年半的学习工作期间给予我很大的指导和空间，让我有各种机会与世界最成功的计算机科学家们一起学习和工作！

我还特别感谢我硕士阶段的导师孙国基教授。孙老师严谨的治学精神和崇高的人生风范使我受益良多，是我人生中宝贵的精神财富，值此论文完稿之际，谨向孙老师表示衷心的感谢和深深的敬意。

感谢系统工程研究所和智能网络与网络安全教育部重点实验室的的各位老师和同学。彭勤科老师、高峰老师、杜友田老师、陶敬老师、秦涛老师、刘烃老师在工作和生活上给予我无私的关心和帮助，与他们在工作和生活方面的讨论使我受益匪浅。感谢行为安全分析小组的房超、牛非、杜静子、沙惠兰、王嘉霖、刘晓梅，以及曾经同在科学馆 139 实验室的马小博，他们在科研一直配合我，并且在生活上给予我很多帮助和鼓励。

感谢我的室友王海军，他在生活上对我的关心和帮助，在学习上对我的鼓励和支持让我一生难忘。

我要深深地感谢我的父母和我的女友杨玥，感谢你们在我多年的求学道路上无微不至的关怀和支持，你们永远是我奋斗的源动力，是我陷入困境时最大的精神支柱，是你们无私的付出让我顺利完成学业，我永远爱着和感谢你们。这里，我祝福他们永远健康快乐!

最后非常感谢在百忙之中抽出宝贵时间来为本文审稿的各位老师，感谢你们的付出和支持。

攻读学位期间取得的研究成果

论文：

期刊：

[1] Chao Shen, Zhongmin Cai, Xiaohong Guan, Youtian Du, Roy Maxion. User Authentication through Mouse Dynamics[J]. IEEE Transaction on Information Forensics and Security, 2013, 8(1): 16~30. (计算机安全领域顶级期刊)

[2] Zhongmin Cai, Chao Shen, Xiaohong Guan. Mitigating Behavioral Variability for Mouse Dynamics: A Dimensionality-Reduction-based Approach [J]. to appear in IEEE Transaction on Human-Machine System, 2014.

[3] Chao Shen, Zhongmin Cai, Shinghon Lau, Roy A. Maxion, Xiaohong Guan. Performance Evaluation of Anomaly-Detection Algorithms for Mouse Dynamics[J]. Pattern Recognition. (Under Review)

[4] 沈超, 蔡忠闽, 管晓宏, 房超, 杜友田. 基于鼠标行为特征的用户身份认证与监控[J]. 通信学报, 2010, 31(7): 68~75.

[5] Dai Wang, Xiaohong Guan, Ting Liu, Yun Gu, Chao Shen, Zhanbo Xu. EDSE: A Detection Method Against Tolerable False Data Injection Attack [J]. to appear in Energies, 2014.

[6] 王淼, 蔡忠闽, 沈超, 华涛. 行为截获技术对鼠标动力学身份认证的影响[J]. 微电子学与计算机, 2013, 30(4): 13~21.

[7] 房超, 蔡忠闽, 沈超, 牛非, 管晓宏. 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.

会议：

[8] Chao Shen, Zhongmin Cai, Roy A. Maxion, Xiaohong Guan. On User Interaction Behavior as an Evidence for Computer Forensic Analysis[C]. Proceedings of the 12th International Workshop on Digital-Forensics and Watermarking (IWDW), CBD Auckland, New Zealand, 2013.

[9] Zhongmin Cai, Chao Shen, Miao Wang, Yunpeng Song, and Jialin Wang. Mobile Authentication through Touch-Behavior Features[C]. Proceedings of the 8th Chinese Conference on Biometric Recognition, Jinan, China, 2013. (会议最佳论文)

[10] Chao Shen, Roy A. Maxion. A Study of the Consistency in Keystroke Dynamics[C]. Proceedings of the 8th Chinese Conference on Biometric Recognition, Jinan, China, 2013.

[11] Chao Shen, Zhongmin Cai, Roy Maxion, Guang Xiang, Xiaohong Guan. Comparing Classification Algorithm for Mouse Dynamics based User Identification[C]. Proceedings of IEEE Fifth International Conference on Biometrics: Theory, Applications and Systems (BTAS), Washington. DC, 2012.

[12] Chao Shen, Zhongmin Cai, Xiaohong Guan. Continuous Authentication for Mouse Dynamics: A Pattern-Growth Approach[C]. Proceedings of IEEE/IFIP 42nd International Conference on Dependable Systems and Networks (DSN), Boston, MA, 2012. (计算机可靠性领域顶级会议)

[13] Chao Shen, Zhongmin Cai, Xiaohong Guan, Jialin Wang. On the Effectiveness and Applicability of Mouse Dynamics Biometric for Static Authentication: A Benchmark Study[C]. Proceedings of

IAPR/IEEE Fifth International Conference on Biometrics (ICB), New Delhi, India, 2012.

[14] Chao Shen, Zhongmin Cai, Xiaohong Guan. Can It Be More Practical? Improving Mouse Dynamics Biometric Performance[C]. Proceedings of the ACM Conference on Computer and Communications Security (CCS), October, Chicago, IL, USA, 2011. (计算机安全领域顶级会议)

[15] Chao Shen, Zhongmin Cai, Xiaohong Guan, Jinpei Cai. A Hypo-optimum Feature Selection Strategy for Mouse Dynamics in Continuous Identity Authentication and Monitoring[C]. Proceedings of IEEE International Conference on Information Theory and Information Security (ICITIS), December, Beijing, China, 2010.

[16] Chao Shen, Zhongmin Cai, Xiaohong Guan, Huilan Sha, Jingzi Du. Feature Analysis of Mouse Dynamics in Identity Authentication and Monitoring[C]. Proceedings of 2009 IEEE International Conference on Communication (ICC), June, Dresden, Germany, 2009.

[17] Haijun Wang, Xiaohong Guan, Qinghua Zheng, Ting Liu, Chao Shen and Zijang Yang. Directed Test Suite Augmentation via Exploiting Program Dependency [C]. to appear in 36th ICSE workshop on Constraints in Software Testing, Verification, and Analysis, 2014.

[18] Miao Wang, Chao Shen, Zhongmin Cai, Tao Hua. The Effect of Input Messages Acquisition Methods on Mouse Dynamics[C]. Sciencepaper Online, February, 2011.

[19] Jingzi Du, Tao Hua, Weixuan Mao, Chao Shen, Zhongmin Cai. Keystroke Semantic Information based Identity Authentication and Monitoring[C]. Sciencepaper Online, February, 2011.

专利授权及申请：

[20] 基于击键乱序特征的计算机用户身份验证方法. 中国发明专利, 授权号: ZL201010176069.1, 2010年.

[21] 基于键鼠交叉认证的身份判定方法. 中国发明专利, 专利号: 201010158930.1, 2010年.

[22] 基于人机交互行为的用户身份属性检测方法. 中国发明专利, 专利号: 201310454565.2, 2013年.

软件著作权：

[23] 计算机桌面行为认证软件 V1.0. 登记号: 2009SR08149.

学位论文独创性声明（1）

本人声明：所呈交的学位论文系在导师指导下本人独立完成的研究成果。文中依法引用他人的成果，均已做出明确标注或得到许可。论文内容未包含法律意义上已属于他人的任何形式的研究成果，也不包含本人已用于其他学位申请的论文或成果。

本人如违反上述声明，愿意承担以下责任和后果：

1．交回学校授予的学位证书；

2．学校可在相关媒体上对作者本人的行为进行通报；

3．本人按照学校规定的方式，对因不当取得学位给学校造成的名誉损害，进行公开道歉。

4．本人负责因论文成果不实产生的法律纠纷。

论文作者（签名）：　　日期：　　年　　月　　日

学位论文独创性声明（2）

本人声明：研究生_____所提交的本篇学位论文已经本人审阅，确系在本人指导下由该生独立完成的研究成果。

本人如违反上述声明，愿意承担以下责任和后果：

1．学校可在相关媒体上对本人的失察行为进行通报；

2．本人按照学校规定的方式，对因失察给学校造成的名誉损害，进行公开道歉。

3．本人接受学校按照有关规定做出的任何处理。

指导教师（签名）：　　日期：　　年　　月　　日

学位论文知识产权权属声明

我们声明，我们提交的学位论文及相关的职务作品，知识产权归属学校。学校享有以任何方式发表、复制、公开阅览、借阅以及申请专利等权利。学位论文作者离校后，或学位论文导师因故离校后，发表或使用学位论文或与该论文直接相关的学术论文或成果时，署名单位仍然为西安交通大学。

论文作者（签名）：　　日期：　　年　　月　　日

指导教师（签名）：　　日期：　　年　　月　　日