



基于行为足迹的多模态融合身份认证

林梦琪, 张晓梅

(上海工程技术大学 电子电气工程学院, 上海 201620)

摘要: 针对单模态身份认证方法存在特征单一容易被伪造和攻破的问题, 提出基于用户行为足迹的多模态特征融合隐式身份认证方法。在移动设备中采集用户使用设备时的触摸压力、触摸轨迹、加速度等传感器数据, 利用特征选择技术提取触摸屏交互、移动模式、物理位置等特征并对其进行训练与融合, 最终通过多模态特征融合模型实现用户身份认证。实验结果表明, 该方法采用的特征级融合和决策级融合方式均获得了98%以上的认证准确率, 相比单模态身份认证方法更难以被伪造和攻破, 且认证准确率更高、稳定性更强。

关键词: 生物行为; 多模态特征; 隐式认证; 数据融合; 行为足迹

开放科学(资源服务)标志码(OSID):



中文引用格式: 林梦琪, 张晓梅. 基于行为足迹的多模态融合身份认证[J]. 计算机工程, 2021, 47(10): 116-124.

英文引用格式: LIN M Q, ZHANG X M. Identity authentication of multi-modal fusion based on behavioral footprint[J]. Computer Engineering, 2021, 47(10): 116-124.

Identity Authentication of Multi-Modal Fusion Based on Behavioral Footprint

LIN Mengqi, ZHANG Xiaomei

(School of Electronic and Electrical Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

[Abstract] Among identity verification methods, the single-mode verification methods rely on single features, and are vulnerable to forged authentication and attacks. To solve the problem, an implicit authentication method of multi-modal feature fusion based on user footprints is proposed. The data of user behavior when using the mobile devices, including the touch pressure, the track of finger movement, and the acceleration of user movement, is collected from sensors. Then the feature selection technique is used to extract the features of touch screen interactions, movement mode, and physical location. The extracted features are subsequently trained and fused. On this basis, the multi-modal feature fusion model is used to realize user identity authentication. Experimental results show that the proposed method achieves an authentication accuracy of over 98% in both the feature-level fusion mode and the strategy-level fusion mode. It is less vulnerable to forged authentication and attacks, and displays higher authentication accuracy and stability.

[Key words] biological behavior; multi-modal feature; implicit authentication; data fusion; behavioral footprint

DOI: 10.19678/j.issn.1000-3428.0061434

0 概述

随着移动互联网和移动设备的不断发展, 以智能手机和平板电脑为代表的便携式移动电子设备在很大程度上改变了人们的生活方式, 也成为现代人生活中不可或缺的工具。现有研究表明, 92.8%的用户习惯将隐私信息存储至智能手机中, 并且有62%的用户并没有为智能手机设置密码^[1-3]。移动设备通常存在着较大的安全隐患, 隐私信息的泄露会造成个人经济财产的损失, 因此需要给移动设备实施安全认证^[4-5]。传统的移动设备认证方式^[6-8]主要包

括图形密码认证、指纹认证、面部识别等, 但这些认证方式较为频繁, 每次唤醒设备都要进行验证, 给用户带来了极大的不便, 而且安全性较低, 容易被攻破^[9-10]。除了传统认证方式之外, 基于生物行为特征的持续隐式认证也是近年来研究的热点, 通过采集用户的行为特征等信息识别出当前使用者的身份, 并且对用户进行持续不间断的隐式认证, 能够兼顾用户体验度与设备安全性^[11-12]。文献[13]利用手机触摸屏采集用户的滑动行为, 调用手机自带的传感器, 通过用户与触摸屏之间的交互行为特征进行认证。文献[14]结合长文本和自由文本, 提出基于动

基金项目: 国家自然科学基金(61802252)。

作者简介: 林梦琪(1997—), 女, 硕士研究生, 主研方向为隐式认证、数据挖掘; 张晓梅(通信作者), 副教授、博士。

收稿日期: 2021-04-25 修回日期: 2021-05-25 E-mail: mengqi.lin0912@qq.com

态击键的用户认证方式。文献[15]使用可穿戴式的加速度传感器进行步态认证和识别,将加速度传感器附着在受试者裤袋上采集步态特征。文献[16]介绍声音行为,根据用户的说话方式和模式来识别和认证用户。

在实际应用场景中,由于环境的不可预测性,单模态的身份认证受到限制,同时单模态特征由于特征单一,容易被仿造或攻击^[17]。目前,研究人员逐步将单模态认证转换为多模态认证,与基于单一交互信息源的身份认证方式不同,基于多模态特征的隐式身份认证具有更高的准确率且难以被伪造。文献[18]通过用户使用设备时的时空、环境、步态、生物和行为特征,提出一种基于多特征融合的隐式身份认证方案。文献[19]通过在智能手机上挖掘能持续认证的行为习惯提出身份认证方案,使用Wi-Fi、蓝牙、活动、位置、应用程序、呼叫和短信数据来构建用户交互行为,得到了98.3%的认证准确率。虽然目前生物行为特征的连续身份验证应用越来越广,但基于单一交互信息源的单模态认证方法只适用于特定操作或场景。为解决这一问题,本文提出基于用户行为足迹的多模态特征融合的隐式认证方法,采用多模态生物特征来适应不同环境,并从移动设备中获得不同的传感器数据,通过多特征融合模型得到最终的身份认证结果。

1 多模态特征融合模型

在用户使用手机的过程中,手机自带的众多传感器会产生大量与用户身份有关的数据。利用这些原始数据提取出多种有效特征,并通过机器学习算法对特征进行训练和融合,得到多模态特征融合模型,实现对用户身份的持续认证。本文主要采集触摸屏、加速度传感器、GPS传感器、陀螺仪传感器、压力传感器和磁场传感器数据。

1.1 用户与触摸屏的交互

文献[13]通过实验证明简单的触摸动作就能验证用户身份,所收集的数据包括屏幕上的压力、手指覆盖的屏幕面积、手指相对于屏幕的方向和位置。本文将触摸屏数据与压力传感器数据归类为用户与触摸屏的交互数据。

1.2 用户使用手机的移动模式

在用户使用手机的过程中,手机自带的加速度传感器主要用于捕捉手机的运动模式,记录3个轴上的加速度,如图1(a)所示。加速度传感器用于检测手机向某一个轴方向的线性变化,而陀螺仪传感器可以全方位得到手机在空间上位移的变化。陀螺仪传感器也有3个轴,每个轴都带有一个角度分量,如图1(b)所示。通过加速度传感器和陀螺仪传感器可以确定用户移动模式。

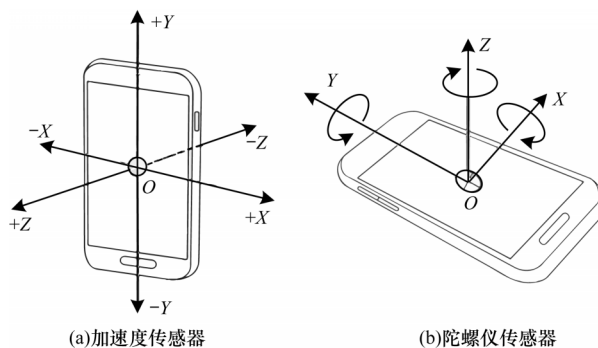


图1 手机移动模式

Fig.1 The movement mode of mobile phone

1.3 用户经常所处的物理位置

GPS传感器用于记录位置信息。文献[20]提出一种基于用户历史位置信息的主动认证方案,通过实验证明该方案可与其他模式的特征进行融合来提高认证性能。对于利用磁场传感器数据进行认证的情况较少,并且本文通过实验发现磁场传感器数据与用户身份的相关性较小,因此本文采用GPS传感器数据作为用户所处的物理位置。

2 数据采集

采用自建数据集,在不同型号的3部手机上对5名女性和7名男性进行实验,其中有2名用户为左利手。基于Android Studio平台开发一款电子书e-book软件,让用户选择自己感兴趣的文章导入电子书,采集真实有效的阅读数据。数据采集过程如图2所示,软件会在用户滑动手机时调用内置传感器,同时后台记录用户在手机屏幕上滑动时所产生的系列特征数据。为保证数据有效性并减少误差,要求每位用户至少进行8次数据采集,每次采集时长不小于30 min,至少获得3 000条轨迹信息。

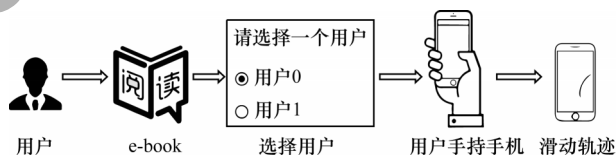


图2 数据采集过程

Fig.2 Process of data collection

在实验中采集的数据为原始数据,需要经过处理后才可进行数据分析。例如,在阅读过程中选择章节、退出等操作时会产生很多点动数据。这些点动数据往往是无序随机的,并且与用户的相关性较小,因此需要将点击屏幕的数据判断为异常值。

实验采用拉依达准则^[21]剔除异常值,主要操作步骤如下:

- 1) 假设数据是通过等精度的设备得到,将其定义为 x_1, x_2, \dots, x_n 。
- 2) 计算该组数据的均值 \bar{x} 和残差 v_i :

$$v_i = x_i - \bar{x} (i = 1, 2, \dots, n) \quad (1)$$

3)按贝塞尔公式计算标准差 σ :

$$\sigma = \sqrt{\sum_{i=1}^n (x_i - \bar{x})^2 / (n-1)} \quad (2)$$

4)判断该组数据 x_b 的残差 $v_b (1 \leq b \leq n)$,若满足

$|v_b| = |x_b - \bar{x}| > 3\sigma$,则认为 x_b 是含有较大误差的异常值,将其剔除。

在去除异常值后,得到部分用户的滑动轨迹如图3所示,可以看出不同用户的滑动轨迹明显不同,相同用户的滑动轨迹走向非常相似。

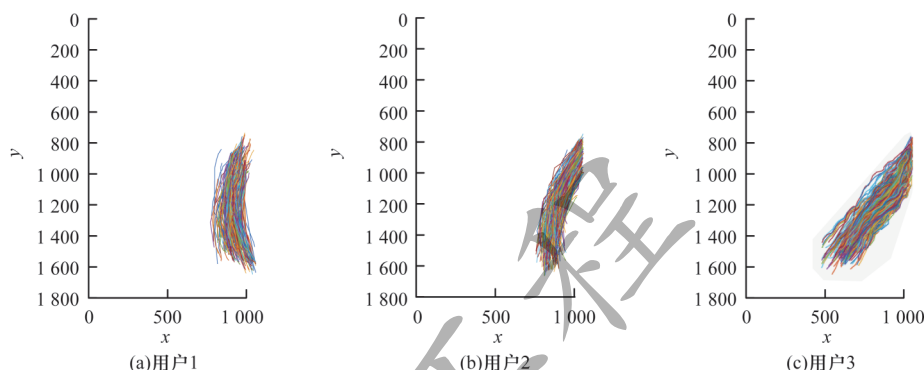


图3 部分用户的滑动轨迹

Fig.3 Sliding track of some users

3 特征选择

实验采集的原始数据包括在触摸时的所有传感器数据以及产生每条数据的用户ID信息。本文将传感器数据分为用户与触摸屏的交互、用户使用手机时的移动模式、用户经常所处的物理位置3类特征,经过特征分析处理后得到新特征,然后剔除无用的特征,得到最终选择的特征。

3.1 原始特征

实验通过调用手机的内置传感器进行数据采集,记录用户操作手机时所产生的一系列行为,选出一部分常用且便于理解的数据作为原始特征。用户与触摸屏的交互行为包括手指接触屏幕的压力、滑动过程中的 x 和 y 方向的速度、每条滑动轨迹经过的点坐标。在数据采集过程中,利用手机在空间移动产生的加速度表示用户使用手机时的移动模式,采用经度和纬度表示用户在使用手机时的物理位置。原始特征设置如下:

- 1)Time,表示采集时间。
- 2)TouchType,表示触摸类型,其中,0代表按下,1代表抬起,2代表滑动。
- 3)XCoordinate,表示 x 坐标。
- 4)YCoordinate,表示 y 坐标。
- 5)Pressure,表示压力。
- 6)XVelocity,表示 x 方向的速度。
- 7)YVelocity,表示 y 方向的速度。
- 8)X_ACC,表示 x 方向的加速度。

9)Y_ACC,表示 y 方向的加速度。

10)Z_ACC,表示 z 方向的加速度。

11)X_GYRO,表示 x 方向的陀螺仪数据。

12)Y_GYRO,表示 y 方向的陀螺仪数据。

13)Z_GYRO,表示 z 方向的陀螺仪数据。

14)X_MAG,表示 x 方向的磁场数据。

15)Y_MAG,表示 y 方向的磁场数据。

16)Z_MAG,表示 z 方向的磁场数据。

17)Latitude,表示纬度。

18)Longitude,表示经度。

3.2 经过处理的特征

将通过手机传感器得到的原始数据按照不同特征进行可视化处理,对于区分度明显的特征予以保留,区分度不明显的特征则需要进行处理,形成具有明显区分度的新特征再加以使用。

如图4所示,YCoordinate和Z_ACC特征对于用户原始数据进行可视化后区分度极低,不同用户对于该特征所表现出的结果相差不大,不能很好地表征不同的用户,因此需要对该特征进行处理得到新的特征。

由于相同用户的滑动轨迹偏转角度相似,不同用户的偏转角度相差较大,因此需要对偏转角特征进行处理得到新的特征。如图5所示,为获得一条轨迹起点到终点的偏转角 θ ,计算该条轨迹的起点和终点的坐标之间的向量 A_1A_n ,使用向量 A_1A_n 的余弦值来表示偏转角Angle。

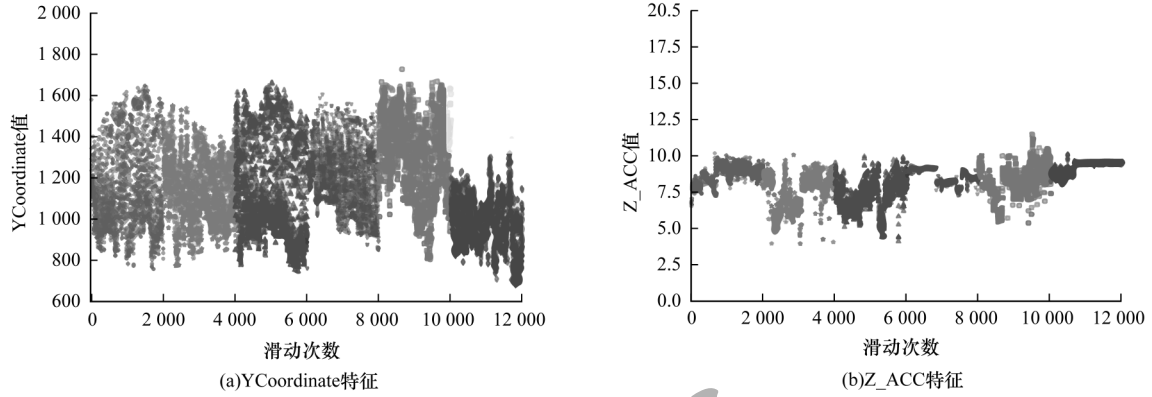


图4 部分用户的YCoordinate和Z_ACC特征

Fig.4 YCoordinate and Z_ACC feature of some users

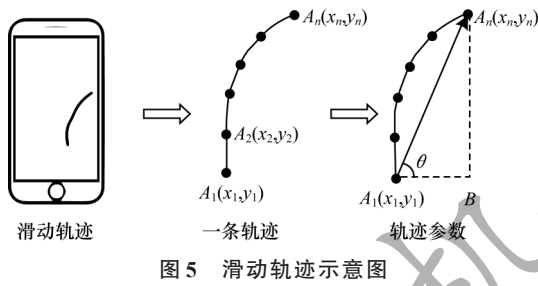


图5 滑动轨迹示意图

Fig.5 Schematic diagram of sliding track

假设起点和终点在手机屏幕上的坐标为 $A_1(x_1, y_1)$ 和 $A_n(x_n, y_n)$, 则有:

$$A_1B = x_n - x_1 \quad (3)$$

$$A_1A_n = \sqrt{(x_n - x_1)^2 + (y_n - y_1)^2} \quad (4)$$

$$\cos \theta = AB / A_1A_n = \frac{x_n - x_1}{\sqrt{(x_n - x_1)^2 + (y_n - y_1)^2}} \quad (5)$$

将部分用户的数据以滑动轨迹的偏转角可视化显示,如图6所示,可以看出相同用户的点基本分布在一个范围内,而不同用户的点所在范围差异较大,因此滑动轨迹的偏转角特征可以较好地地区分不同的用户。

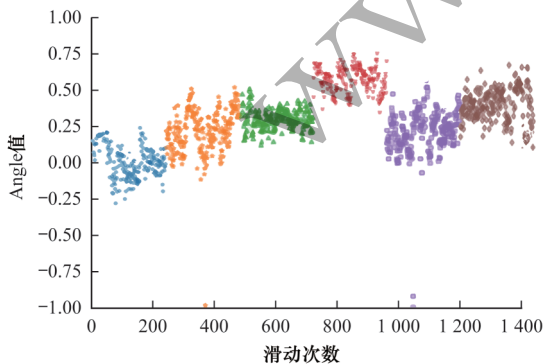


图6 部分用户的偏转角特征

Fig.6 Deflection angle feature of some users

在计算向量 A_1A_n 余弦值的过程中发现,不同用户滑动轨迹的向量 A_1A_n 长度也有所差异,因此可作为一个新的特征来区分用户。

由图5可知,一条轨迹由很多个离散的点构成,为求得一条轨迹的长度,可以按照式(6)计算每两个连续的点之间的欧氏距离,然后进行累加得到轨迹长度 Track_Length。

$$D_{\text{Track_Length}} = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (6)$$

将部分用户的数据以滑动轨迹的长度可视化显示,如图7所示,可以看出相同用户的点基本分布在一个范围内,而不同用户的点所在的范围差异较大。在实际生活中,不同用户的手指长度也有所差异,且手持手机的方式不同,会造成滑动轨迹的长度不同,因此滑动轨迹的偏转角特征可以较好地地区分不同用户。

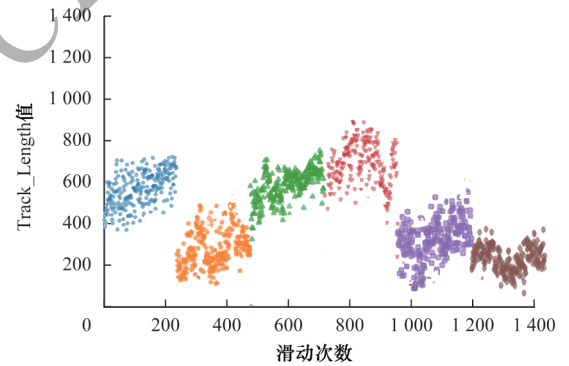


图7 部分用户的轨迹长度特征

Fig.7 Track length feature of some users

3.3 其他特征

在实验中发现,通过对编号为3~13的原始特征(以 XCoordinate 为例)计算每次滑动过程的均值(XCoordinate_Average)、方差(XCoordinate_Std)、最大值(XCoordinate_Max)、最小值(XCoordinate_Min)、起始点(XCoordinate_Start)、终止点(XCoordinate_End)、波动范围(XCoordinate_Range)共获得77个新特征,更能体现

用户的差异性,其中XVelocity和YVelocity在滑动结束时为0,整段滑动过程中的最小值也为0,属于无效特征,需要剔除,因此共得到73个新特征。加上每次滑动的持续时间(Time)和用户所处位置的经度(Longitude)、纬度(Latitude)以及偏转角(Angle)、向量长度(Vector_Length)、轨迹长度(Track_Length),共得到79个特征。其中,属于用户与触摸屏的交互的特征有35个,属于用户使用手机时的移动模式的特征有42个,属于用户经常所处的物理位置的特征有2个。

4 基于用户行为足迹的多模态融合身份认证

本文选择3个维度的特征共同对用户进行识别和认证,分别是用户与触摸屏的交互、用户使用手机时的移动模式、用户经常所处的物理位置。由于这3个维度包含不同类型的特征,为起到共同认证用户的作用,因此需要对这3个维度的特征进行融合。

4.1 身份认证框架

为实现用户身份识别,本文构建基于行为足迹的多模态融合身份认证框架,如图8所示。

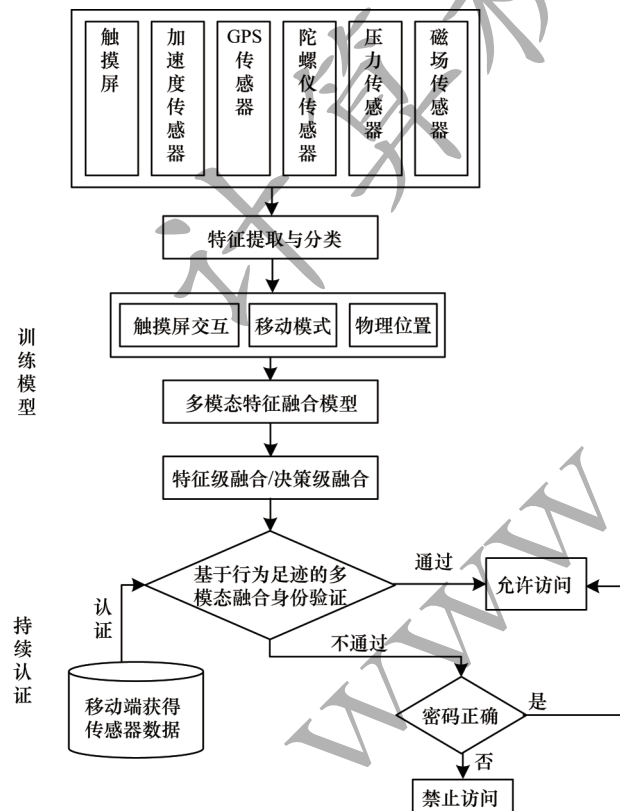


图8 多模态特征融合的身份认证框架

Fig.8 Identity authentication framework of multi-modal feature fusion

身份认证过程具体如下:

1)数据采集。在用户滑动手机时调用内置传感器,包括触摸屏、加速度传感器、GPS传感器、陀螺

仪传感器、压力传感器和磁场传感器,同时后台记录用户在手机屏幕上滑动时所产生的一系列特征数据。

2)特征选择。对小样本数据进行调研,选择与用户身份相关度较高的特征,并从选出的特征中提取出新的特征,通过互信息法计算特征与用户ID之间的互信息量,去除低互信息量的特征。

3)模型训练与特征级融合。特征级融合是先将所有特征放在一起,再选择分类器对特征进行训练。决策级融合是先将不同维度的特征进行训练得到一个可信分数,再将不同维度返回的分数融合在一起,最终得到基于行为足迹的多特征融合模型。

4)持续隐式身份认证。用户在使用手机的过程中,若要访问更高权限的内容,需在移动端获得传感器数据,将数据存入生成模型中得到认证结果,若认证通过则可以继续访问手机,若不通过则需要使用显示的认证方式,如输入密码。

4.2 特征级融合

特征级融合发生在特征分类之前,主要利用特征选择技术,从融合的所有特征中找到能最大限度提高分类器性能的特征,最终采用分类器获得分类结果。

互信息^[22]是度量两个事件集合之间的相关性。假设有两个离散的随机变量 X 和 Y ,它们之间的互信息量可以定义如下:

$$I(X; Y) = \sum_{y \in Y} \sum_{x \in X} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} \quad (7)$$

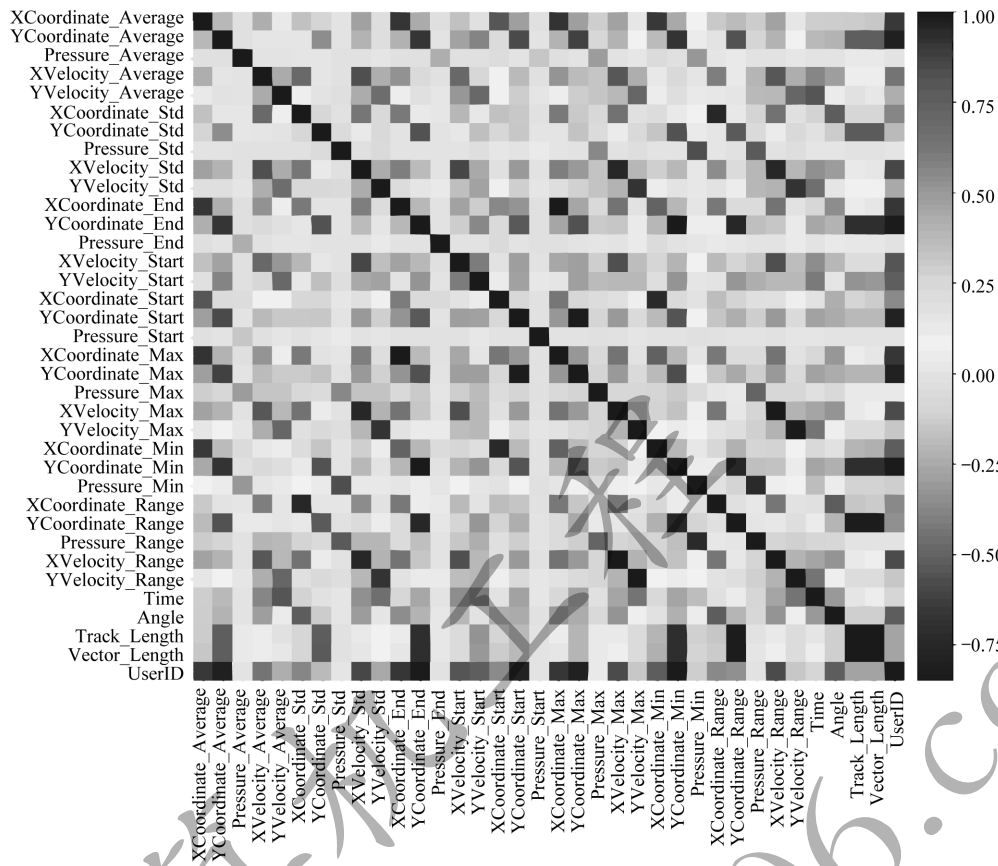
其中: $p(x, y)$ 是 X 和 Y 的联合概率分布函数; $p(x)$ 和 $p(y)$ 是 X 和 Y 的边缘概率分布函数。

若 X 和 Y 是两个连续的随机变量,则互信息量可以表示为二重积分的形式:

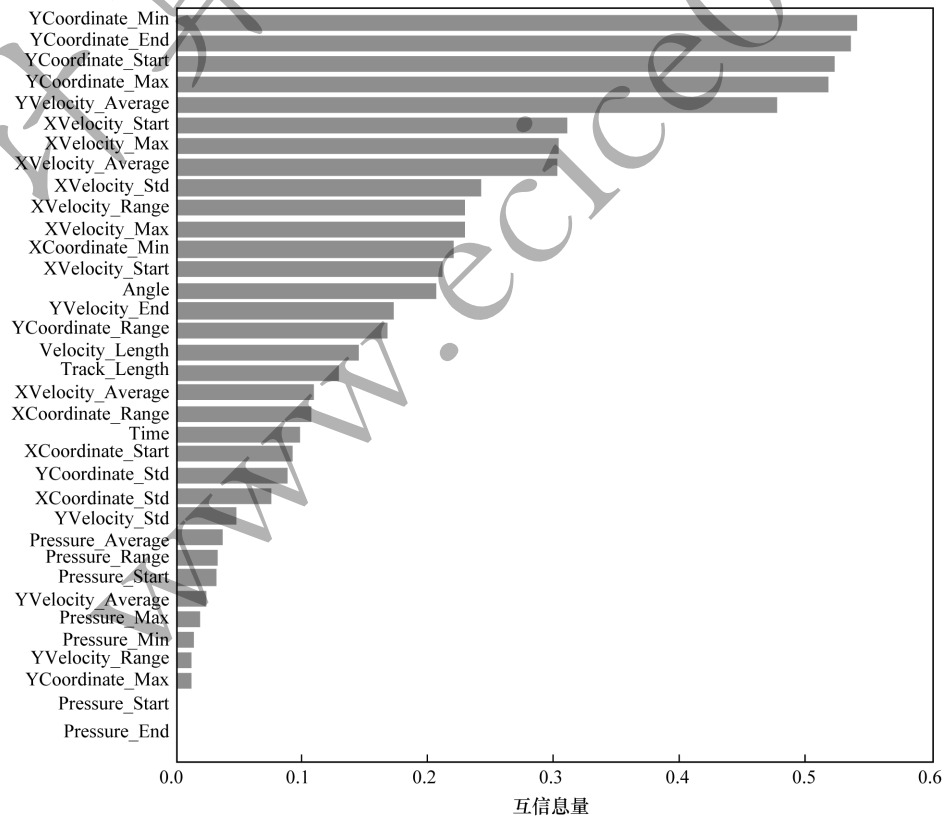
$$I(X; Y) = \iint_{Y \times X} p(x, y) \log \frac{p(x, y)}{p(x)p(y)} dx dy \quad (8)$$

其中: $p(x, y)$ 是 X 和 Y 的联合概率密度函数; $p(x)$ 和 $p(y)$ 是 X 和 Y 的边缘概率密度函数。

为得到能最大限度提高分类器性能的特征,先计算各维度中特征之间的互信息量,若两个特征之间具有强相关性,只选择其中一个特征作为表征用户的特征。在筛选完特征后,计算特征与用户ID之间的互信息量,去除低信息量的特征。通过热度图的方式表现特征之间的互信息量,并将特征与用户ID之间的互信息量从大到小排序,部分结果如图9所示。



(a)特征之间的互信息量



(b)特征与用户ID之间的互信息量

图 9 各维度中特征及特征与用户 ID 之间的互信息量

Fig.9 The mutual information between features and between features and user ID in each dimension

通过计算各维度中特征与用户 ID 之间的互信息量可以得出, Pressure_Start 和 Pressure_End 与用户 ID 的互信息量为 0, 说明它们不能提供任何信息量, 在本文中删除该特征, 而 YCoordinate 提取出的所有新特征与用户 ID 之间的信息量都比较高。采用互信息法进行优质特征选择后, 直接将这些特征进行融合, 再选择一个分类器对用户进行识别和认证。

4.3 决策级融合

决策级融合指的是对于不同维度的特征, 选择使用不同的分类器进行分类, 得到基于每个维度选择的分类器结果后将所有结果进行融合, 最终得到唯一的分类结果, 如图 10 所示。

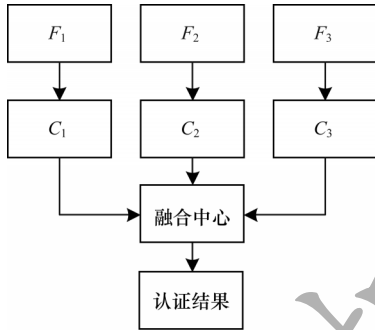


图 10 决策级融合过程

Fig.10 Process of decision-level fusion

在图 10 中, F_1 、 F_2 和 F_3 表示本文提出的 3 个维度的特征, C_1 、 C_2 和 C_3 表示选择的分类器, 分别得到一个二元分类结果 $[-1, 1]$, 通过融合中心进行计算, 最终得到唯一的认证结果。文献[23]提出一种决策级融合规则, 具体表示如下:

$$u_i = \begin{cases} 1, & \text{合法用户} \\ -1, & \text{非法用户} \end{cases} \quad (9)$$

其中: u_i 表示通过分类器 C_i 得到的分类结果。融合中心通过最小化全局贝叶斯风险来结合这些局部分类结果。决策级融合规则进行如下似然比检验:

$$\frac{P(u_1, u_2, \dots, u_n | H_1)}{P(u_1, u_2, \dots, u_n | H_0)} \geq P_0 / P_1 = \tau \quad (10)$$

其中: H_1 和 H_0 分别表示合法用户和非法用户; P_1 和 P_0 表示判断用户为合法的概率和判断用户为非法的概率。在该情况下, 得到最终的决策级融合结果为:

$$f(u_1, u_2, \dots, u_n) = \begin{cases} 1, & a_0 + \sum_{i=0}^n a_i u_i > 0 \\ -1, & \text{其他} \end{cases} \quad (11)$$

$$a_0 = \ln P_1 / P_0 \quad (12)$$

$$a_i = \begin{cases} \ln(1 - P_{M_i}) / P_{F_i}, & u_i = 1 \\ \ln(1 - P_{F_i}) / P_{M_i}, & u_i = -1 \end{cases} \quad (13)$$

其中: P_{M_i} 表示错误拒绝率(False Rejection Rate, FRR), 即不该拒绝的样本中拒绝的比例; P_{F_i} 表示错误接受率(False Acceptance Rate, FAR), 即不该接受的样本中接受的比例。根据式(13), 最终得到 $[-1, 1]$ 的二元分类结果。决策级融合方式适用于不同维度的数据, 尤其是数据不统一的情况。

5 实验与结果分析

利用两种融合方式对 12 名用户进行身份认证实验。采用朴素贝叶斯分类器对用户进行分类识别, 图 11 给出了两种不同融合方式下的 ROC 曲线, 可以看出在只有物理位置特征的情况下, 认证准确率很低, 说明仅依据物理位置特征无法对用户进行认证, 而在特征级融合和决策级融合两种方式下, 准确率分别为 98.2% 和 98.7%, AUC 值几乎达到 1。与单一模态下的识别结果不同, 融合 3 个维度的特征后能够得到更优的分类结果。通过计算认证结果的等错误率(Equal Error Rate, EER)证明, 在单一模态的验证下 EER 均在 15% 以上, 而融合后的多模态认证模型的 EER 下降至 1.7% 左右。

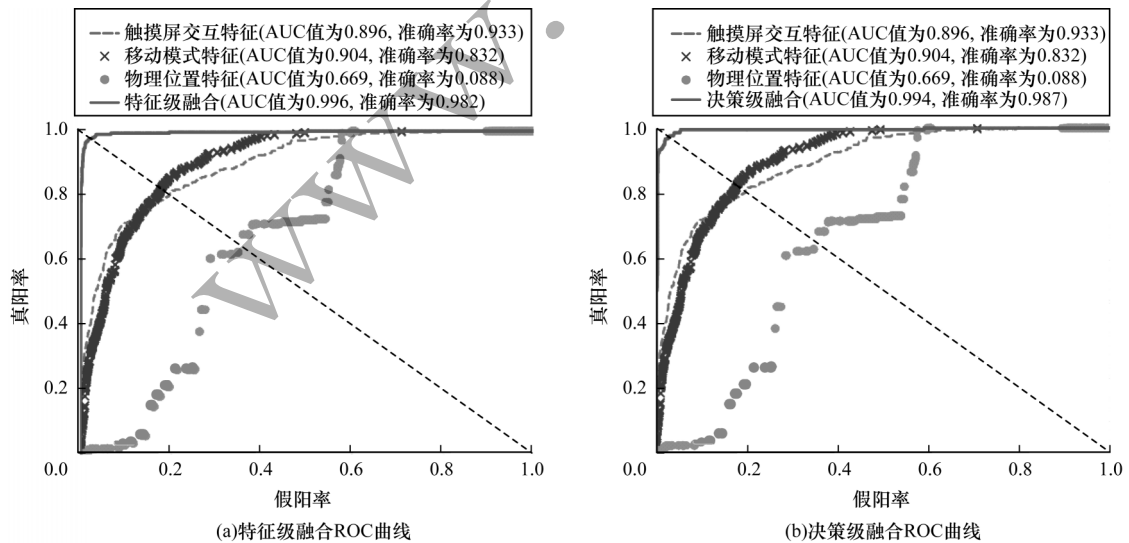


图 11 两种融合方式下的 ROC 曲线

Fig.11 ROC curve under two fusion modes

两种融合方式下的F1分数如图12所示,特征级融合和决策级融合的认可效果相差不大,但均比单一模式的认证效果好。

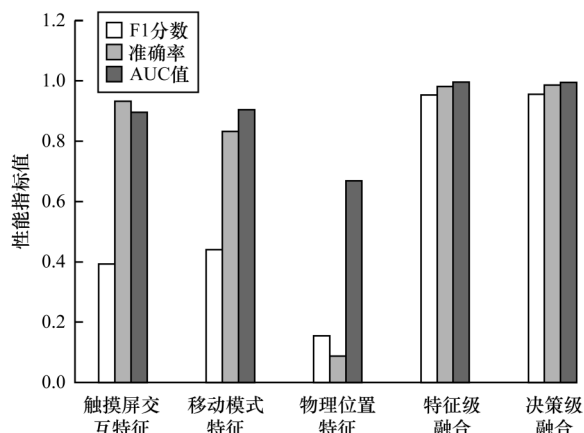


图12 两种融合方式下的F1分数

Fig.12 F1 score under different fusion modes

图11与图12均是在三星 Galaxy C5 手机上所得的

表1 单一模态与多模态融合身份认证性能对比

Table 1 Performance comparison of identity authentication of single-modal and multi-modal fusion

性能指标	手机设备	触摸屏交互特征	移动模式特征	物理位置特征	特征级融合	决策级融合
准确率	三星 Galaxy C5	0.933	0.832	0.088	0.982	0.987
	VIVO Y83	0.838	0.873	0.385	0.836	0.963
	华为 mate7	0.877	0.918	0.268	0.773	0.917
AUC 值	三星 Galaxy C5	0.896	0.904	0.669	0.996	0.994
	VIVO Y83	0.923	0.945	0.755	0.952	0.992
	华为 mate7	0.826	0.918	0.883	0.949	0.966
F1 分数	三星 Galaxy C5	0.393	0.439	0.154	0.953	0.956
	VIVO Y83	0.799	0.848	0.553	0.820	0.953
	华为 mate7	0.527	0.752	0.305	0.758	0.815

6 结束语

本文提出基于用户行为足迹的多模态特征融合身份认证方法,采集移动设备的触摸屏、加速度传感器、GPS传感器、陀螺仪传感器、压力传感器和磁场传感器数据,利用这些原始数据提取多种有效隐式特征,并通过机器学习算法对特征进行训练和融合得到多模态特征融合模型,实现对用户身份的持续隐式认证。实验结果表明,与单一模态特征身份认证方法相比,该方法具有更高的认证准确率和稳定性,且难以被伪造和攻破。下一步将优化本文多模态特征融合模型并对其进行跨设备应用,以实现同一用户在不同设备上的身份认证。

参考文献

[1] KARANIKIOTIS T, PAPAMICHAIL M D. Continuous implicit authentication through touch traces modelling[C]//Proceedings

实验结果,本文还分别在 VIVO Y83 和 华为 mate7 手机上对相同用户采集数据进行实验,结果数据如表1所示,可以看出不同设备在单一模态下的各指标认证结果波动较大,鲁棒性较差,而多模态特征融合下的认证结果明显优于单一模态,各手机设备的特征融合认证结果较稳定,并且决策级融合方式略微优于特征级融合方式。

然而,在不同数据集和不同用户上进行实验,不同特征的表现会有所不同,例如文献[24]介绍了对于应用程序使用、Web浏览和GPS定位的认证性能,通过实验得出性能最好的是基于物理位置的认证模型,而本文在基于物理位置的模式下对用户进行认证并没有得到最好的结果,计算得到的 EER 为 35.5%,说明这一特征不具有很好的稳定性,因此若只选用单一模态下的特征进行认证,结果可能存在偶然性,在不同数据集中会有不同的表现。为使认证模型具有更强的适应能力,采用多模态融合的身份认证是更好的选择。

of the 20th International Conference on Software Quality, Reliability and Security. Washington D. C., USA: IEEE Press, 2020: 111-120.

- [2] EKIZ D, CAN Y S, DARDAGAN Y C, et al. Can a smartband be used for continuous implicit authentication in real life[J]. IEEE Access, 2020, 8: 59402-59411.
- [3] KIM Y, OH T, KIM J. Analyzing user awareness of privacy data leak in mobile applications[EB/OL]. [2021-03-14]. <https://www.hindawi.com/journals/misy/2015/369489/>.
- [4] YANG Y Y, HUANG X L, GUO Y H, et al. Dynamic multi-level privilege control in behavior-based implicit authentication systems leveraging mobile devices[C]//Proceedings of the 17th International Conference on Mobile Ad Hoc and Sensor Systems. Washington D. C., USA: IEEE Press, 2020: 229-237.
- [5] GOWRAJ N, AVIREDDY S, RAVI P V, et al. SAFE: shoulder-surfing attack filibustered with ease[C]//Proceedings of the 43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop. Washington D. C., USA: IEEE Press, 2013: 1-7.

- [6] BALDINI G, STERI G. A survey of techniques for the identification of mobile phones using the physical fingerprints of the built-in components [J]. IEEE Communications Surveys & Tutorials, 2017, 19(3): 1761-1789.
- [7] SIMANJUNTAK G D, NUR RAMADHANI K, ARIFianto A. Face spoofing detection using color distortion features and principal component analysis [C]//Proceedings of the 7th International Conference on Information and Communication Technology. Washington D. C., USA; IEEE Press, 2019: 1-5.
- [8] PATEL K, HAN H, JAIN A K. Secure face unlock; spoof detection on smartphones [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(10): 2268-2283.
- [9] HOSSEINI S. Fingerprint vulnerability: a survey [C]//Proceedings of the 4th International Conference on Web Research. Washington D. C., USA; IEEE Press, 2018: 70-77.
- [10] GALBALLY J, SATTI R. Three-dimensional and two-and-a-half-dimensional face recognition spoofing using three-dimensional printed models [J]. IET Biometrics, 2016, 5(2): 83-91.
- [11] 沈超. 移动终端交互行为分析的身份主动认证与安全感知[J]. 中国教育网络, 2016(11): 37.
- [12] ABUHAMAD M, ABUSNAINA A, NYANG D, et al. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: a contemporary survey [J]. IEEE Internet of Things Journal, 2021, 8(1): 65-84.
- [13] FRANK M, BIEDERT R, MA E, et al. Touchalytics: on the applicability of touchscreen input as a behavioral biometric for continuous authentication [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 136-148.
- [14] KANG P, CHO S. Keystroke dynamics-based user authentication using long and free text strings from various input devices [J]. Information Sciences, 2015, 308: 72-93.
- [15] GAFUROV D, SNEKKENES E, BOURS P. Gait authentication and identification using wearable accelerometer sensor [C]//Proceedings of 2007 IEEE Workshop on Automatic Identification Advanced Technologies. Washington D. C., USA; IEEE Press, 2007: 220-225.
- [16] WANG Q, LIN X, ZHOU M, et al. VoicePop: a pop noise based anti-spoofing system for voice authentication on smartphones [C]//Proceedings of IEEE Conference on Computer Communications. Washington D. C., USA; IEEE Press, 2019: 2062-2070.
- [17] KHAN H, HENGARTNER U, VOGEL D. Targeted mimicry attacks on touch input based implicit authentication schemes [C]//Proceedings of the 14th Annual International Conference on Mobile Systems, Applications, and Services. New York, USA; ACM Press, 2016: 387-398.
- [18] 刘礼才, 李锐光, 殷丽华, 等. 面向移动智能设备的多特征融合隐式鉴别机制研究 [J]. 电子学报, 2016, 44(11): 2713-2719.
- [19] LIU L C, LI R G, YIN L H, et al. Research on multi-feature fusion impact authentication for intelligent mobile device [J]. Acta Electronica Sinica, 2016, 44(11): 2713-2719. (in Chinese)
- [20] 庞晓健. 基于行为感知的移动终端持续认证研究 [D]. 西安: 西安电子科技大学, 2019.
- [21] PANG X J. Research on continuous authentication of mobile terminals based on behavior-awareness [D]. Xi'an: Xidian University, 2019. (in Chinese)
- [22] MAHBUB U, CHELLAPPA R. PATH: person authentication using trace histories [C]//Proceedings of the 7th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference. Washington D. C., USA; IEEE Press, 2016: 1-8.
- [23] 刘彬, 戴桂平. 基于白化检验和 3σ 准则的小波阈值去噪算法 [J]. 传感技术学报, 2005, 18(3): 473-476.
- [24] LIU B, DAI G P. Adaptive wavelet thresholding denoising algorithm based on white noise detection and 3σ rule [J]. Journal of Transduction Technology, 2005, 18(3): 473-476. (in Chinese)
- [25] 范雪莉, 冯海泓, 原猛. 基于互信息的主成分分析特征选择算法 [J]. 控制与决策, 2013, 28(6): 915-919.
- [26] FAN X L, FENG H H, YUAN M. PCA based on mutual information for feature selection [J]. Control and Decision, 2013, 28(6): 915-919. (in Chinese)
- [27] CHAIR Z, VARSHNEY P K. Optimal data fusion in multiple sensor detection systems [J]. IEEE Transactions on Aerospace and Electronic Systems, 1986, 22(1): 98-101.
- [28] FRIDMAN L, WEBER S, GREENSTADT R, et al. Active authentication on mobile devices via stylometry, application usage, Web browsing, and GPS location [J]. IEEE Systems Journal, 2017, 11(2): 513-521.

编辑 陆燕菲