文章编号：2095-2163(2021)08-0154-04 中图分类号：TP309 文献标志码：A

基于触屏行为的智能移动设备身份认证

张彭明，张晓梅，胡建鹏
（上海工程技术大学,电子电气工程学院，上海 201620）

摘 要：在移动设备的身份认证方面,传统密码认证方式易受到窥肩攻击和屏幕解锁痕迹攻击,不足以保证移动设备隐私安全。本文提出一种基于触屏行为的身份认证方案,获取手指与屏幕交互数据,经预处理后提取触屏行为特征向量,用机器学习算法训练后生成认证模型,对用户进行身份认证。与传统密码身份认证不同,该方案以用户触屏行为信息作为认证密钥,持续检测移动设备用户真实性,即使攻击者看到用户操作行为也很难再现,提高了身份认证安全性。经实验验证,基于触屏行为的身份认证实现了 94.42%的认证准确率。

关键词：隐私安全；身份认证；行为特征；机器学习

Identity authentication of intelligent mobile devices based on touch-screen behavior

ZHANG Pengming, ZHANG Xiaomei, HU Jianpeng
(School of Electric and Electronic Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

【Abstract】 In the aspect of identity authentication of mobile devices, the traditional password authentication method is vulnerable to shoulder peeping attack and screen unlocking trace attack, which is not enough to ensure the privacy and security of mobile devices. This paper proposes an identity authentication scheme based on touch-screen behavior, which obtains the interactive data between finger and screen, extracts the feature vector of touch-screen behavior after preprocessing, and generates an authentication model after training with machine learning algorithm to authenticate the user. Different from the traditional password authentication, this scheme uses the user's touch-screen behavior information as the authentication key to continuously detect the authenticity of mobile device users. Even if the attacker sees the user's operation behavior, it is difficult to reproduce, which improves the security of identity authentication. The experimental results show that the authentication accuracy based on touch-screen behavior is 94.42%.

【Key words】 identity authentication; behavior characteristics; privacy and security; machine learning

0 引 言

智能移动设备的普及为人们获取信息提供了极大的便利,方便了生活。但在带来便利以外,同时引入了新的安全隐患[1]。传统的密码认证方式易被攻破,从而导致用户信息泄露。目前诸如手机等智能移动设备都是绑定了多个服务账户,比如银行、支付宝等支付软件在手机解锁后即可免密支付,不法分子可假冒用户身份行骗,手机作为存储用户重要信息的设备,一旦遗失不但用户自身会受其影响,其周围熟悉的人也会变成被攻击的目标。

目前大部分移动设备都基于传统知识型密码作为认证保护措施,比如 PIN 码或九宫格图案解锁等。这类密码认证安全性薄弱,容易被猜测或被黑客暴力破解[2]。虽然基于声纹、语音识别、指纹识别和虹膜识别等生物认证方案也取得了一定的成果,但都存在一些不足,这些特征容易被伪造从而欺骗认证系统(指纹伪造、3D 面部伪造,录音回放)。生物特征对识别环境要求较高,如:指纹识别需要保持手部干燥,人脸识别要求光亮环境,声纹认证扫描结果容易受到环境的影响,容易导致认证失败。采用虹膜认证准确率高且不易被复制破解,是一种安全性较高的生物特征认证方法。但虹膜认证需要专门的设备且设计比较复杂,一般用于军事领域或高级实验室使用,昂贵不适于普及。

针对以上认证方式缺陷,本文基于用户日常触屏行为特征,建立身份认证模型检测用户。该方案采集触屏传感器数据实时分析用户行为,若检测到

基金项目：国家自然科学基金(61802252)。

作者简介：张彭明(1993-),男,硕士研究生,主要研究方向:智能移动设备隐式认证；张晓梅(1981-),女,博士,副教授,硕士生导师,主要研究方向:信息安全;胡建鹏(1980-),男,博士,副教授,硕士生导师,主要研究方向:数据工程、软件工程。

通讯作者：张晓梅 Email：xmzhang@ sues.edu.cn

收稿日期：2021-01-12

异常立即强制重新认证系统，且在交互过程中可持续检测用户真实性。在使用中无需做特定的认证手势动作，体验度佳且易接受。该方案基于移动设备配备的屏幕传感器进行数据采集，不受环境限制、成本低、易于普及。

1　相关研究

因触屏行为特征认证的隐蔽性和难以模仿等特点，近年来基于触屏行为特征身份认证逐渐成为研究热点。

Mario Frank 等人采取用户触屏信息特征，利用 *XY* 坐标、手指触屏面积和手指划动轨迹建立行为模型来进行用户认证，当采用一次划屏模式时错误率（ERR）为 13%，采用 11～12 次划屏模式时 ERR 降低到 2% ～ 3% 之间，取得良好认证效果[3]。但在其实验中提取触摸行为特征，发现随着时间延长 EER 在不断上升，认证性能逐步下降，说明选取的特征不适合用于长期身份认证。这种认证方式要求用户多次划动才能获得触屏行为特征，操作繁琐不友好。Wang Xiao 等人采集手指点击的坐标等信息，通过 SVM 训练得到用户触摸行为模型，同时还尝试了跨设备认证，首次加入数据校正方法，提高了认证准确率[4]。但其特征值过多，在使用算法训练时容易产生过拟合，导致模型对同一个人不同的操作不能识别，造成认证失败。Gong Zhenqiang 等人基于触摸模式不同，把触摸行为看作是对于其他用户而言的随机“隐式秘密”模型，是真实用户在潜意识下使用设备形成的行为特征，可用于提升认证安全性[5]，不过其模型等错误率较高，为 18%，在高安全身份认证需求中并不适用。

本文通过分析用户的触屏行为信息提取行为特征，训练模型用于持续认证用户。由于不同用户的触屏操作习惯不同，使得个体行为很难模仿，训练的模型可提升认证安全性。选取的触屏行为特征容易采集、模型训练迅速，易于实现。

2　身份认证方案设计

2.1　认证方案流程设计

本文结合触屏信息提出一种新型智能移动设备身份认证方案，认证流程分为以下几个阶段：信息采集、数据预处理、特征提取与筛选、模型训练和匹配认证。在信息采集阶段，通过触屏传感器采集用户与设备交互行为信息；在预处理阶段，去除触屏噪声数据，数据归一化处理；在特征提取阶段，提取用户使用移动设备时手指触屏 *XY* 坐标、划动时长、点击压力、划动速度等原始行为特征，再根据原始行为特征提取触屏行为特征分量；在训练阶段，采用两种机器学习算法评估特征有效性，选取与特征相结合下性能最佳的分类器，并将认证模型保存；在匹配认证阶段，分类器载入认证模型，并与测试数据对比分析，返回认证结果。认证方案如图 1 所示。

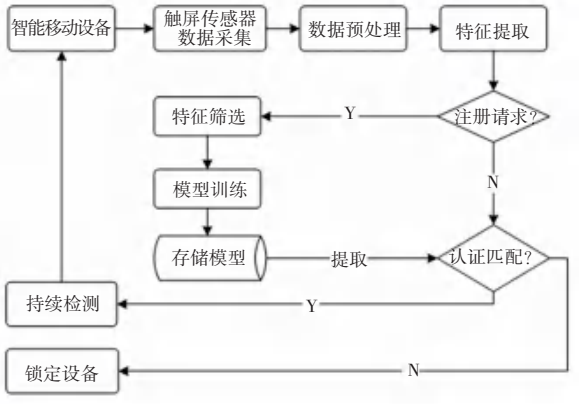

图 1　认证方案设计

Fig. 1　Authentication scheme design

2.2　分类器模型

为选取适合本文特征的分类算法，本文采用支持向量机（Support Vector Machine，SVM）和随机森林（Random Forests，RF）两种机器学习算法作对比分析。支持向量机是有监督二分类器，从训练集的两个类中寻找超平面，作为分类决策边界。对于复杂高维特征，可用核函数对数据进行映射，使得数据集易于分类。SVM 本身是通过间隔概念的结构化来分类优化目标，使得 SVM 具有优秀的泛化能力，因此对大多数类型数据具有较好的适用性。随机森林是通过组合多个弱分类器，经过多个弱分类器共同投票或取均值使得模型具有较高精确度和泛化性能。其能够处理高维度数据，对数据集的适应能力强。

3　实验设计

3.1　数据采集

为收集触屏行为数据，本文开发了安卓阅读程序并加入触屏数据收集功能，安装在 Huawei V10 手机上，用户阅读时，触屏行为收集功能自动在后台持续采集数据。本次实验共有 10 名在校学生参与，规定每人每次阅读 1 h 左右。全部人员共采集 100 次，共有12 000条数据。原始数据经预处理后按 7∶2∶1 分为训练集、测试集和验证集。训练集用于筛选和训练分类器模型，测试集用于评估认证模型性

能,验证集用于调参优化分类器。实验者首先通过 APP 注册用户号,填写采集记录,之后开始采集。

3.2 数据预处理

3.2.1 去噪处理

由于用户在划动操作时,传感器会在开始与结束处记录大量冗余值,对此可采取截断法过滤冗余数据,去除开始与结束点处 1ms 内轨迹点。在实验中用户反常操作行为导致触屏传感器产生异常数据,这会对后续的特征提取产生影响。但对于每个用户产生的异常点的变化不同,需要针对不同用户计算出各个特征的门限值。本文采用行为数据均值的 ±10% 范围为上下界门限值用于过滤异常点,公式(1)和公式(2):

$$\begin{cases} th_{up} = \dfrac{\sum_{i=1}^{n} k_i}{n} \times 110\%, \\ th_{down} = \dfrac{\sum_{i=1}^{n} k_i}{n} \times 90\%, \end{cases} \tag{1}$$

$$\begin{cases} k_i = \min\{k_i, th_{up}\}, \\ k_i = \max\{k_i, th_{down}\}. \end{cases} \tag{2}$$

其中,k_i 为第 k 个特征集合内第 i 个为特征内的数据点;n 为特征内数据点个数;th_{up} 为门限值上界;th_{down} 为门限值下界。

3.2.2 归一化处理

如果数据直接用于训练会导致分类器仅仅依赖于某些特征,从而造成过拟合,模型泛化能力差。因此,需要对数据进行归一化处理。本文采用离散标准化方法把特征值映射在[0,1]区间内,式(3):

$$k_i^* = \frac{k_i - \min\limits_{1 \leqslant q \leqslant n}\{k_q\}}{\max\limits_{1 \leqslant q \leqslant n}\{k_q\} - \min\limits_{1 \leqslant q \leqslant n}\{k_q\}}. \tag{3}$$

其中,k_i 为第 k 维度下特征的第 i 个数据点;$\min\limits_{1 \leqslant q \leqslant n}\{k_q\}$ 为 k 维特征的最小值;$\max\limits_{1 \leqslant q \leqslant n}\{k_q\}$ 为第 k 维特征最大值;k_i^* 为第 k 维度下特征的第 i 个数据点的映射值。

3.3 特征提取与筛选

原始数据特征量较少,不能详细反映用户触屏行为特征。本文采集用户触屏时记录的 XY 坐标、手指压力、XY 速度和触屏时长共六维原始特征,在每个原始特征维度上,进一步提取了每个特征的最大最小值、均值、标准差和中位数共 5 种数据变化信息,因此本文共提取 5×6=30 维触屏行为信息作为特征集。

机器学习算法训练的分类模型性依赖于所选的特征集,特征集的优劣会影响分类器准确度,无用特征不仅会延缓训练速度,还有可能干扰分类器。由于初步提取的特征可能存在冗余,因此剔除不相关、不必要的特征可以提高模型的分类准确率,加快训练速度。因随机森林算法不受数据量纲影响,且可输出训练数据特征重要性,可用于特征贡献率分析,所以本文采用随机森林作为触屏行为特征子集筛选方法。

4 实验分析与结果对比

4.1 特征筛选分析

先采用小批量特征集数据,经 RF 算法输出每个特征分量对总体分类的重要性,每个分量在特征中的贡献率如图 2 所示。

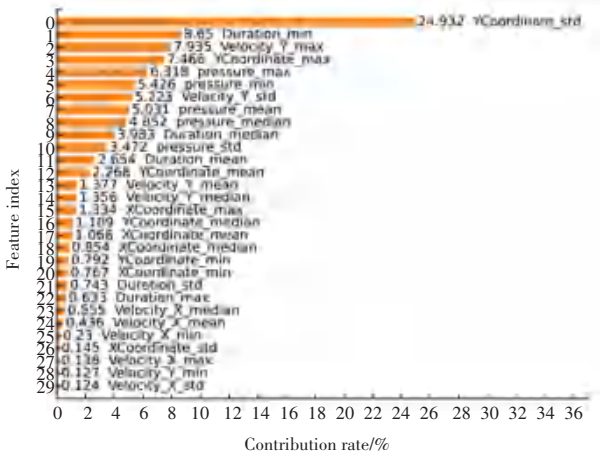

图 2 各个特征贡献率

Fig. 2 Contribution rate of each feature

从原始特征角度来看,关于坐标 XY、触屏压力的行为特征分量贡献率较大;其次是使用时长,关于 XY 速度特征分量贡献率最低,表明触屏操作时 XY 坐标和触屏压力与行为变化间关联密切,不同用户在这部分特征上有明显的差异性,区分度明显;划动时长也具有较高的贡献率,表明用户划动时长特征具有区分性。在默认采集频率下,数据相邻点的间隔时长变化不一,表明不同用户在使用移动设备时,手指在触屏轨迹上停留时间有明显差异;XY 速度特征分量整体贡献率较低,但其中一些特征分量的贡献率很高。从具体的特征分量上来看,Y 轴坐标的标准差特征贡献率最高,在 24% 以上,说明每个用户一段时间内的连续轨迹的 Y 轴坐标变化值的离散度不一,触屏行为表现出差异性。而划动时长最小值特征重要度排在第二,贡献率较高,说明触屏最短时间特征在每个用户上都保持稳定的触屏时长,在

不同用户间区别明显；而 X 坐标标准差分量贡献率低，说明触屏行为在 X 坐标轴上变化差别较小，反映出用户在移动设备屏幕的纵向上与横向上的划动趋势，不难发现关于 X 轴划动速度特征变化较小，贡献率较低，因此可去除与 X 轴划动速度相关的特征分量，保留其他特征用于训练模型。

4.2　分类算法对比

选择最佳特征集后，本文采用准确率评估算法与特征相结合的整体性能，同时也探讨了参数对模型准确率的影响，结果见表 1。

表 1　分类器参数对模型准确率影响

Tab. 1　Influence of classifier parameters on model accuracy

分类器(Classifier)	参数 (*Parameters*)	准确率(*Accuracy*)
SVM	RBF-kernel	91.50%
	Linear-kernel	94.07%
RF	estimators = 20	93.51%
	estimators = 50	93.85%
	estimators = 100	94.42%
	estimators = 150	94.40%

由表 1 可以看出，分类器参数对模型准确率有重要影响。横向来看，SVM 的 Linear 核训练的模型准确率最高，高出 RBF 核 2.57 个百分点。而 RF 算法与初始化树的棵数有关，随着树的棵数增加，其训练的模型准确率逐步上升，说明增加树的棵数能有效提升准确率，但在 *estimators* = 150 时模型准确率没有提升，说明在 *estimators* = 100 时 RF 算法已经达到最优，不会再随树的增加而增加。纵向来看，SVM 算法在采用 Linear 核下也有较高的准确率，超过了 RF 算法在树的棵数为 20、50 时的情况，低于树棵数为 100 时的 RF 算法。因此将触屏行为特征与优化参数的 RF 算法结合，可使训练身份认证模型准确度最高。

5　结束语

本文基于触屏行为信息，经提取筛选后用机器学习方法建立身份认证模型，不需要显式输入密码验证身份，还能持续检测当前用户身份真实性。与传统密码认证相比，不仅增强了身份认证安全性，也提升了移动设备使用体验。采用的触屏行为特征易于采集，特征提取方便，模型易于实现。且通过特征选择进一步降低了模型整体的复杂度，有利于减少模型训练时间，提升认证速度。

虽然基于触屏行为特征的能实现身份认证，但本文只在阅读应用程序使用场景中做了相关研究，未深入分析用户在不同应用程序场景下的触屏行为，其触屏行为在不同应用上的变化是否一致，这一问题值得在下阶段工作中探讨分析。

参考文献

[1] FTC. Mobile privacy disclosures: Building trust through transparency [R]. 2013.

[2] LIU X, LI Y, DENG R H, et al. When Human cognitive modeling meets PINs: User-independent inter-keystroke timing attacks," Computers & Security, 2019, 80: 90-107.

[3] 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, 2012, 8(1):136-148.

[4] WANG X, YU T, MENGSHOEL O, et al. Towards continuous and passive authentication across mobile devices: an empirical study[C]// the 10th ACM Conference. ACM, New York, USA, 2017:35-45.

[5] GONG N Z, PAYER M, MOAZZEZI R, et al. Forgery-Resistant Touch-based Authentication on Mobile Devices[J]. Hydrological Processes, 2015, 26(23):499-510.

(上接第 153 页)

[4] ZOU H, YUE Y, LI Q, et al. An improved distance metric for the interpolation of link-based traffic data using kriging: a case study of a large-scale urban road network[J]. International Journal of Geographical Information Science, 2012, 26(4): 667-689.

[5] SUN S, ZHANG C, ZHANG Y. Traffic flow forecasting using a spatio-temporal bayesian network predictor[C]//International conference on artificial neural networks, 2005: 273-278.

[6] JIANG B. Street hierarchies: a minority of streets account for a majority of traffic flow[J]. International Journal of Geographical Information Science, 2009, 23(8): 1033-1048.

[7] 杜甜添.基于大数据挖掘技术的短时交通流预测方法研究[D]. 石家庄：石家庄铁道大学,2019.

[8] ERMAGUN A, CHATTERJEE S, LEVINSON D. Using temporal detrending to observe the spatial correlation of traffic[J]. PloS one, 2017, 12(5): e0176853.