文章编号：2096-1472(2021)-03-20-04
DOI:10.19644/j.cnki.issn2096-1472.2021.03.005

移动端用户行为特征识别研究

杨 帆

(中国银联股份有限公司，上海 201201)
✉yangfan@unionpay.com

摘 要：随着移动互联网的高速发展，智能手机已经成为人们社交、支付、出行、娱乐等活动中不可或缺的工具。而一旦手机被盗用，用户的各类应用账户都可能被无限制地访问，继而导致身份冒用、隐私泄露、财产损失等严重后果。本文提出一种在移动端采集用户行为特征，并通过神经网络建模的识别方法，通过收集手机的倾斜角度、移动速度、加速度，以及用户点击、滑动屏幕的力度、速度、触点形状、面积等数据，验证设备是否被他人盗用。这种身份验证技术具有难以窃取和伪造、验证流程用户无感知、隐私性好等优点。

关键词：行为生物识别；身份验证；移动互联网；卷积神经网络
中图分类号：TP311.52 **文献标识码**：A

Research on Recognition of Mobile User Behavior Features

YANG Fan

(*China Unionpay Co*., *Ltd*., *Shanghai* 201201, *China*)
✉yangfan@unionpay.com

Abstract: With the rapid development of mobile Internet, smart phones have become an indispensable device in social activities, payments, travelling, entertainment and other activities. Once the mobile phone was stolen, the user's various application accounts might be accessed without restrictions, leading to serious consequences such as identity fraud, privacy leakage, and property loss. This paper proposes a recognition method that collects user behavior features on mobile terminals and uses neural network modeling. Data, such as tilt angle, movement speed, acceleration speed, as well as force, speed, shape and area of touchpoints, are collected to verify whether the device is stolen by others. This kind of identity verification technology has the advantages of being stealing and forgery resistant, undisturbed and privacy-friendly.

Keywords: behavioral biometrics; identity verification; mobile Internet; convolutional neural network

1 引言(Introduction)

目前，各类移动端应用为防止账户盗用，使用了多种身份认证技术，如数字密码、图形密码、短信验证码、指纹识别、人脸识别等，但这些身份验证方法均各自存在一些不足之处。首先，短信验证码在盗用者解锁手机之后就无法起到保护作用；数字和图形密码容易被猜测，其中图形密码还能够通过分析屏幕上残留的手指痕迹被攻破[1]；指纹和人脸识别一方面需要手机硬件支持，另一方面依赖用户的唯一生物信息，容易引起对个人隐私的担忧，如最近一份关于个人信息使用的调查中显示，六成受访者认为人脸识别技术有滥用趋势[2]。本文中，我们研究了在移动端采集用户行为特征进行身份验证的方案：通过用户使用手机时的握持方式、运动方式、屏幕点击习惯等信息，进行神经网络建模，验证设备使用者的身份。可内置于移动端的网页、小程序当中，以无感形式运行，具有较好的防盗和防伪性，且无须采集用户的唯一生物特征。

2 相关研究(Related research)

最近几年，国内对行为特征识别的研究从采集的行为类型上大致可以分为键盘鼠标行为、网络访问行为、手机携带行为、触摸行为四种。

基于键盘鼠标行为的身份验证：颜丽菁[3]和钟意[4]基于用户的击键动力学和鼠标动力学特征，分别提出了仅基于鼠标，以及结合鼠标和键盘行为的用户交互信息持续身份认证方法。因为在研究中只考虑用户使用鼠标和键盘的行为模式，所以只适用于电脑端认证，无法用于移动端。

基于网络访问行为的身份验证：谭飞越[5]提出了一套利用

用户Web浏览行为进行身份验证的方案，主要收集用户每天访问的网页数量、访问时间、网页URL，以及经过文本处理而提取出的网页主题等信息，体现不同个体之间在网络访问习惯和兴趣方面的差异。这个方案只使用和具体浏览内容相关的信息，而不采集从传感器取得的物理行为数据。

基于手机携带行为的身份验证：庞晓健[6]和胡海龙[7]各自提出了基于手机中加速度计、陀螺仪等传感器收集用户运动、步态等手机携带过程中产生的信息进行持续身份认证的方案，其中胡海龙的方案还采集了手机蓝牙、WIFI、GPS等信息。不过研究中没有采集用户和手机屏幕的交互数据。

基于触摸行为的身份验证：邹斌[8]和刘永帅[9]各自提出了通过记录用户触屏行为，使用SVM、SMO等算法进行身份认证的方案。其中邹斌使用的是一个公开的数据集，并未设计数据采集方案；而刘永帅则是在安卓2.3系统下开发了一款数据采集应用，该应用始终保持在后台运行，静默记录用户和手机屏幕的交互。但是需要指出，随着安卓系统的不断更新，从2017年谷歌推出安卓8.0开始，对应用的后台运行做出了严格的限制：后台应用仅在特定的情况下才会获得约几分钟的时间窗口，随后安卓系统会停止其服务。因此，比起通过后台应用持续收集触摸行为等信息，将数据采集以模块化的方式内置于页面中，如从HTML5页面进行数据收集，具有更高的可行性。

3　数据采集和处理(Data collection and parsing)

3.1　数据采集

设计HTML5页面，向页面中的<html>元素添加eventListener，监听三类行为事件：触摸事件、设备角度变化事件、设备移动事件，具体包括：触摸开始(touchstart)、触点移动(touchmove)、触摸结束(touchend)、设备角度变化(deviceorientation)和设备移动(devicemotion)。

(1)触摸事件。在HTML5页面上捕获三类触摸event后，可以通过event.touches[n]获取由Touch对象构成的数组TouchList，其中n表示触点的编号：数组中一个Touch对象代表一个触点，当有多个手指触摸屏幕时，TouchList就会存储多个Touch对象。

需要注意的是，Touch对象可以细分为三种：touches、targetTouches和changedTouches。changedTouches对象中记录的是最近一次发生变化的触摸点信息，例如同时有两根手指触摸屏幕，只移动其中一根手指，那么对应的touchmove事件中changedTouches就只会存在发生了移动的触点信息。另一方面，targetTouches对象中会包括此时屏幕上所有触点的信息，无论其内容是否发生了变化，但有一个前提是触点必须保持在同一个dom元素内。例如，手指先按下按钮A，之后移动到按钮B上，那么从targetTouches中只能读到按钮A对应的触摸信息，移动到按钮B之后的则会被忽略。而touches则是表示范围最广的事件，它记录当前屏幕的所有触点，无论触点信息是否发生变化，也无论触点是否保持在同一个dom元素内。

通过以上分析，changedTouches适用于只需要关注触点状态更新的场景，而targetTouches适用于只需要关注单个dom元素的场景，而我们需要对整个HTML页面上所有触点的状态做持续的记录，因此最适用的是touches对象。从touches对象的属性中，我们可以获得按压力度、触点形状、触点位置等信息。

(2)设备角度变化事件。在HTML5页面上捕获设备角度变化事件后，可以从事件属性中获得设备当前在空间中的x、y、z坐标角度。

(3)设备移动事件。同样的，在HTML5页面上捕获设备移动事件后，可以从事件属性中获得设备当前移动加速度、重力加速度、旋转角速度的数据，均有x、y、z三个方向。

3.2　数据处理

(1)合并事件

以上三类行为事件是相互独立的，也就是说，在用户没有操作屏幕时也会持续产生设备角度变化和设备移动的数据。但我们最关注的是用户进行点击、滑动等操作时对应的设备状态，因此在数据处理的第一步，需要找到每个触摸事件所对应的设备角度和移动数据。具体方法是，对每个触摸事件，向前找到距离它最近的角度变化和移动事件各一条，将它们的属性转存到触摸事件对象的属性中。

(2)计算滑动速度

对于滑动事件，滑动时各个触点在屏幕上的绝对坐标往往并不是十分重要，因为根据页面布局的不同，用户滑动的位置也会存在差别。而滑动速度和位置无关，更能反映用户的操作习惯。因此我们使用前后两次触点移动事件的坐标差除以时间差，计算出对应的手指滑动速度。而对于点击操作，直接将速度赋值为0。

(3)数据分片

一个孤立的操作，例如一次点击，所包含的信息量是很少的，很难作为身份验证的依据。而一系列操作，例如一个完整的业务流程所对应的多个点击、滑动操作的组合，就能提供较多的信息。因此，我们不直接把单个事件作为模型的输入，而是将全量数据切分为数据片。

如前一节所述，在原始数据中，触摸事件有三个种类，即触摸开始(touchstart)、触点移动(touchmove)、触摸结束(touchend)。一次点击操作只会包含触摸开始和触摸结束两个事件，而一次滑动操作会包含触摸开始、触摸结束，以及在它们之间的数个触点移动事件。分片时从第一条touchend开始，向后找touchstart事件，并比较两个事件的时间差是否大于设定的阈值k，如果大于则分片：将touchstart之前的所有记录添加(extend)进当前片，并创建(append)一个新片；如果时间差在阈值k以内，则不进行分片，只把touchstart之前

的所有记录添加到当前片的尾部。递归地进行以上流程，直到无法找到下一个touchstart为止。此流程可用伪代码表示如下：

```
function slice(events, time_gap = 1000):
    function do_slice(events):
        i = 0
        # 找下一个touchend事件
            while i < len(events) and is_not_touchend(events[i]):
                i += 1
        # 如果后面没有touchend了，结束递归
        if i >= len(events):
            return
        end = events[i]
        # 继续找下一个touchstart事件
            while i < len(events) and is_not_touch_start(events[i]):
                i += 1
        # 如果后面没有touchstart，补全最后一个分片，并且结束递归
        if i >= len(events):
            extend_slice(slices, events)
            return
        start = events[i]
        # 找到touchend和touchstart，比较两者时间差
        if time_diff(end, start) < time_gap:
            extend_slice(slices, events[: i])
        else:
            new_slice(slices, events[: i])
        # 将还没处理的事件列表输入下一步递归
        do_slice(events[i: ])
    slices = []
    do_slice(events)
    return slices
```

(4)筛选和填充

分片后的数据，每一片可以表示为一个二维矩阵，矩阵的每一列表示一个特征维度，例如按压力度，设备x、y、z轴加速度等，每一行表示一个触摸事件。很显然，用户每次操作不会完全相同，所以每个矩阵中的事件个数也不同。而许多机器学习和深度学习模型要求输入的样本均具有相同的维度，因此需要对矩阵进行0填充(Zero Padding)。在填充之前，我们可以首先将行数小于3的矩阵筛去，这些矩阵只记录了一次孤立的点击，不确定性过强，不利于我们得到稳定的模型。之后找到所有矩阵中行数最多的矩阵，将其他矩阵用0填充到和它相同的行数。

在经过处理后，输入矩阵的列(特征)内容如表1所示。

表1 使用的特征列表

Tab.1 Input features

特征	数据示例
手机空间角度(x, y, z)	(18.1, 1.6, 38.3)
手机重力加速度(x, y, z)	(−0.2, 2.8, 9.4)
手机移动加速度(x, y, z)	(−0.2, 0.3, 0.2)
手机旋转角速度(x, y, z)	(−3.6, −0.1, 2.5)
触点压力	4.36
接触面外接椭圆轴长(x, y)	(31.16, 26)
接触面外接椭圆长轴角度	32
滑动速度(x, y)	(0.00793, −0.37301)
触点坐标(x, y)	(221.5, 369)
和上一事件的时间差(毫秒)	42
是否为touchstart	0
是否为touchmove	1
是否为touchend	0
切片序号	1
标签号	2

4 模型设计(Model design)

我们将身份验证视为多分类问题，训练一个二分类器基于一对多(1 vs N)策略建模。具体地，选择训练一维卷积神经网络作为分类器。

一维卷积和常用于图像建模的二维卷积类似，区别在于其对输入仅在一个维度上计算卷积，配合填充(padding)可保持各卷积层的输出总有一个维度的长度不变，即能保持时间序列信号的局部依赖关系不变，故而更加适用于序列化数据的建模[10]。其计算公式可表示为：

$$(f\times g)(i)=\sum_{j=1}^{m} g\ (j)\cdot f\left(i-j+\frac{m}{2}\right)$$

式中，f表示单个通道长度为n的输入，g表示尺寸为m的一维卷积核，i的取值为0到$(n-m+1)$。

我们设计的神经网络共有三个卷积层、一个全连接层，以及一个使用sigmoid激活函数的输出层。卷积层和全连接层均使用ReLU作为激活函数，卷积核尺寸分别为3、5、7，卷积核个数分别为32、64、128。因为卷积核是一个滑动窗口，输出的矩阵行数会少于输入。例如，输入矩阵有n行，通过一个尺寸为3的一维卷积核后，输出的行数会变为$(n-2)$行。因此我们在输入卷积层前使用0填充，以保持每层输出的feature map矩阵具有相同的行数。神经网络结构如图1所示，图中的数值94为训练数据中一个分片包含的最多事件数。

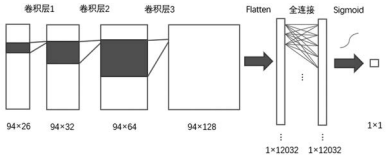


图1 卷积神经网络结构

Fig.1 Structure of CNN

神经网络经过Sigmoid激活的全连接层，对于每一个输入的数据片，输出为一个取值从0到1的伪概率，越接近1表示网络预测输入样本与对应的正类样本越接近。将样本输入各个

模型，取输出中最大值所对应的类别，预测为样本的类别。

5　实验(Experiment)

我们仿造移动端支付应用设计了一个支付小程序的HTML5页面，内置了数据采集模块。征集50位志愿者，让每位志愿者在支付小程序中完成一系列操作流程，过程中让志愿者自由选择最习惯的操作方式。设计的页面如图2所示。

(a)小程序首页　　(b)转账页面

图2 数据采集页面

Fig.2 Data collection page

在对数据处理后输入神经网络进行建模，采用二元交叉熵(Binary Cross Entropy)损失函数，对每一个分类作独立建模。建模时基于1 vs N策略，将当前类作为正样本，其余所有类作为负样本，并取样以控制正负样本比例为1:1。预测时对一个样本通过每个模型进行评分，取Sigmoid函数输出最大的分类。模型迭代过程中的准确率曲线如图3所示，对应的AUC曲线如图4所示。

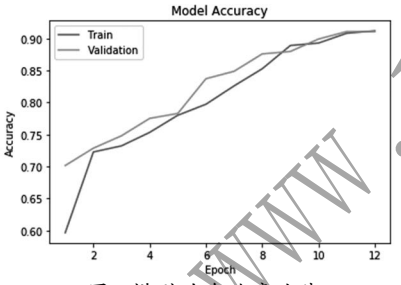


图3 模型的准确率曲线

Fig.3 Accuracy curve

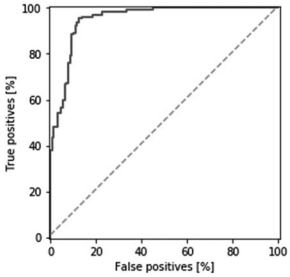
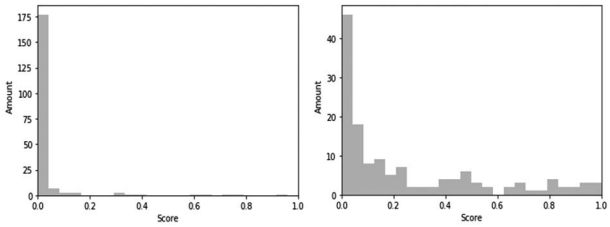


图4 模型的AUC曲线

Fig.4 AUC curve

使用模型进行预测，图5是其中一个模型在输入来自不同的两个人的负样本时，输出的频率分布直方图。可以看到，对于图中左侧的输入样本，模型的分类效果很好，输出p几乎都在0附近；对于图中右侧的输入样本，模型的分类效果稍差一些，但综合所有输入分片的结果，依然能明显看出模型偏向于拒绝($p<0.5$)。图6是同一个模型在输入正样本(本人操作)时的输出，大多数预测p值均接近1，表示成功地接受了大多数正样本。



(a)对模拟盗用者A的预测结果　　(b)对模拟盗用者B的预测结果

图5 对负样本的预测结果

Fig.5 Prediction on negative samples

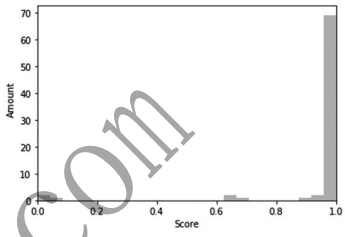


图6 对正样本的预测结果

Fig.6 Prediction on positive samples

6　结论(Conclusion)

本文分析了现有移动端身份识别技术存在的一些不足之处，之后提出一种移动端用户行为特征识别方案。采集设备传感器和屏幕产生的数据，如倾斜角、移动速度、加速度、触点压力、触点形状、滑动速度等，从中对用户使用手机时的行为习惯通过卷积神经网络进行建模和识别。方案中的数据采集模块可内置于网页、小程序中，无须安装额外应用。这种验证方法主要具有特征难以窃取和伪造、验证流程用户无感知、不涉及指纹和人脸等唯一身份标识等优点，可以作为传统身份认证技术的辅助技术。

参考文献(References)

[1] Aviv, A. J., Gibson, et al. Smudge attacks on smartphone touch screens[C]. Usenix Conference on Offensive Technologies, 2010:1-7.

[2] 南都个人信息保护研究中心.人脸识别应用公众调研报告[EB/OL].[2020-10-13].http://epaper.oeeee.com/epaper/A/html/2020-10/14/content_29847.htm.

[3] 颜丽菁.基于用户鼠标行为的身份认证方法研究[D].西安:西安理工大学,2018.

[4] 钟意.基于用户交互行为特征的持续身份认证研究[D].重庆:重庆邮电大学,2019.

[5] 谭飞越.基于用户行为特征的持续身份认证研究[D].重庆:重庆邮电大学,2019.

[6] 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.

[7] 胡海龙.基于行为生物特征的移动用户身份持续认证方法研究[D].重庆:西南大学,2019.

(下转第11页)