文章编号:1007-5321(2019)06-0118-08 **DOI**:10.13190/j.jbupt.2019-043

基于上下文感知的智能手机隐式身份认证机制

王任重, 陶 丹
(北京交通大学 电子信息工程学院, 北京 100044)

摘要: 针对现有智能手机隐式认证方法难以被实际应用的情况,提出了一种基于上下文感知的隐式身份认证机制. 首先,由智能手机内置传感器(加速计、陀螺仪、磁力计)获取点击行为数据;然后从这些数据中提取上下文特征以识别上下文信息 (用户的身体姿势状态),同时提取点击特征为每个上下文训练相应的认证子模型用于认证;最后利用所收集的 7000 + 数据进行实验评估. 结果表明,该方案对不同用户进行认证所得的平均错误接受率和错误拒绝率分别为 1.29% 和 1.03%,与无上下文感知的认证方法相比,平均错误接受率和错误拒绝率分别降低了 1.72% 和 2.59%. 所提的机制可有效提高身份认证的准确性.

关 键 词: 上下文感知; 隐式认证; 身体姿势
中图分类号: TP391.4 **文献标志码**: A

Implicit Authentication Mechanism Based on Context Awareness for Smartphone

WANG Ren-zhong, TAO Dan
(School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: Considering that the existing implicit authentication method for smartphone is difficult to be applied in practice, an implicit authentication mechanism based on context awareness was proposed. Firstly, the tapping behavior data acquired by embedded sensors (i.e. accelerometer, gyroscope, and magnetometer) of the smartphone is used to identify the context information (that is, the user's body posture state). Then, the context feature and tapping feature is extracted from the data after noise elimination which is employed to train the corresponding authentication sub-model for each context. Experiment evaluation is performed using the collected 7000 + data. It is shown that the average false acceptance rate (FAR) and false rejection rate (FRR) of the proposed scheme for different users is 1.29% and 1.03% respectively. Compared with the authentication method without context awareness, FAR and FRR is reduced by 1.72% and 2.59% respectively. The proposed mechanism can effectively improve the accuracy of authentication.

Key words: context awareness; implicit authentication; body posture

智能手机已逐渐成为了人们生活当中的必需品,与此同时用户的隐私安全问题也日渐凸显. 目前,智能手机上虽然已普遍部署了密码保护机制来认证用户的身份以保护用户的隐私信息,但是这种

收稿日期: 2019-03-28
基金项目: 国家自然科学基金项目(61872027)
作者简介: 王任重(1995—), 女, 硕士生.
通信作者: 陶 丹(1978—), 女, 教授, E-mail: dtao@bjtu.edu.cn.

身份认证机制很容易受到肩窥攻击和污迹攻击的威胁. 为此,在密码保护机制中引入生物行为识别技术来进一步加强用户的身份认证已成为相关领域的研究新热点. 这种生物识别技术通过利用一些智能手机内置的传感器就可以“隐形地”捕获用户的行为数据并实现身份认证,因而也被称为“隐式身份认证”. 隐式身份认证机制可以通过与密码机制结合以提高智能手机的安全保护级别[1-4]. Zheng 和 Gurary 等[1-2]提出的是一种增强数字密码机制的隐式认证方法,利用智能手机内置的加速度传感器和压力传感器来表征用户输入数字密码过程中的点击行为习惯,再利用统计学方法或者分类算法提取用户的行为特征并实现了隐式认证. Inoue 和 Teh 等[3-4]提出的是基于智能手机内置加速计、陀螺仪以及磁力计传感器来表征用户触摸行为习惯的隐式认证方法. 然而,上述认证方法均没有考虑用户身体姿势对点击行为的影响. 例如,Zheng、Gurary、Inoue 等的工作都只对用户坐在椅子上或者站立时的点击行为数据进行了研究,但是日常生活中用户使用智能手机时的身体姿势是没有固定模式的. 虽然 Teh 等[4]对用户日常生活中各种姿势下的点击行为进行了认证研究,但是由于身体姿势会影响一个人的点击行为[5],因而这些方法在实际应用时取得的认证精度都比较低.

现实世界的可变性和复杂性对生物识别方法的灵活性提出了更高的要求. Nappi 等[6]的研究表明,在生物识别技术中,利用用户的一些上下文信息(如用户的身体姿势或者所处环境)实现上下文感知的识别系统在提高系统灵活性方面具有很高的价值. 上下文感知的一个基本思想是根据不同的上下文来选择最适配的特征匹配或分类方法. 例如 Feng 等[7]提出了一种以应用程序为上下文的隐式认证方法,为智能手机每个运行的应用程序提供了不同的触摸行为认证模板,并执行自适应分类以提高认证性能. 受此启发,笔者提出了一种对用户的身体姿势和操作手势均具有自适应性的、以用户点击触摸屏的行为习惯为基础的隐式身份认证机制(见图 1),以克服 Zheng、Gurary 、Inoue 和 Teh 等工作[1-4]所存在的不足.

所提的认证机制通过将智能手机用户的身体姿势作为上下文信息,并将其划分为静态和动态 2 种上下文,为用户不同身体姿势下点击行为构建不同的认证子模型,并实现自适应认证. 其中,静态指的是用户身体姿势相对稳定的状态,例如静坐或站立;动态指的是用户身体处于行走或上下楼梯等运动状态;另一方面,考虑到不同人在操作智能手机时具有他们自己的手势习惯,在为用户的点击行为训练认证模型时还提取了一系列表征用户手势习惯的特征,以进一步增强认证性能. 所提出的认证方案可以集成到各种密码保护机制,例如 PIN 解锁或程序登录界面,以提高隐私安全的保护强度.

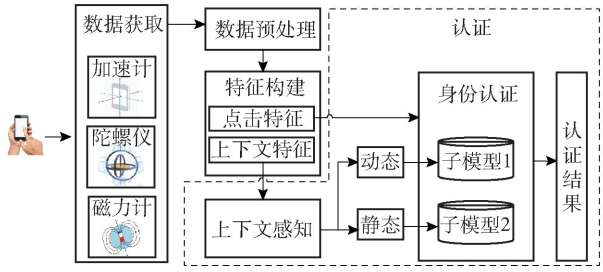


图 1　基于上下文感知的隐式身份认证框图

1　数据获取

为获取用户的点击行为数据,智能手机的 3 个内置传感器被用于表征用户的行为数据,分别是加速计、陀螺仪和磁力计传感器. 其中,加速计可以记录用户较大幅度的运动模式,比如用户使用智能手机时的触屏点击力度以及身体运动状态. 陀螺仪可以测量智能手机在人机交互过程中发生的方向偏转或移动轨迹,进而表征用户握持手机的手势习惯. 磁力计可以用于进一步表征用户与智能手机交互的方位习惯. 使用这 3 个传感器记录的用户行为数据表示为

$$(a,g,m)^s = \{(a_1^s,g_1^s,m_1^s),\cdots,(a_t^s,g_t^s,m_t^s),\cdots,(a_n^s,g_n^s,m_n^s)\} \tag{1}$$

其中(a_t^s,g_t^s,m_t^s)分别表示用户第 s 次操作对应的加速计、陀螺仪以及磁力计传感器的时间序列. $a_t^s=(a_{x_t}^s,a_{y_t}^s,a_{z_t}^s)$,表现为三轴($XYZ$)序列,$g_t^s,m_t^s$ 与之类似. n 为第 s 次行为对应的时间序列总点数.

此外,为进一步解决传感器灵敏度对读数的影响,采用了文献[8]提到的方法,对现有三轴传感器数据进行了模值计算,并将其作为传感器的第 4 维数据. 例如,加速度传感器的模值计算为

$$a_m = \sqrt{a_x^2 + a_y^2 + a_z^2} \tag{2}$$

同样,可得到陀螺仪和磁力的模值. 这些模值受灵敏度的影响要远小于原有的三轴值(XYZ),对于分析传感器数据具有很大的帮助.

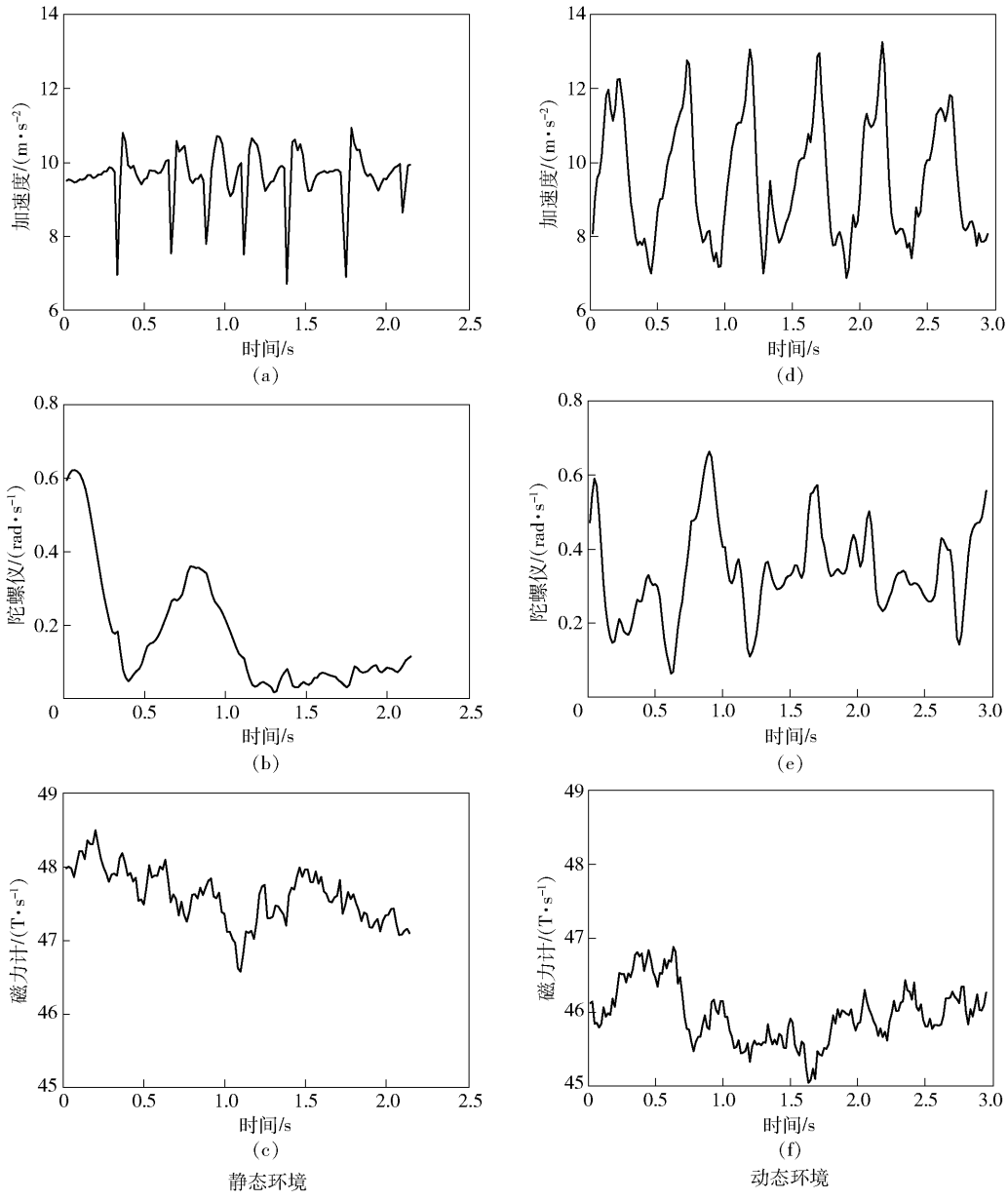


图2 传感器对用户点击行为的反应

2 数据分析与特征构建

图2描述了用户在使用智能手机密码过程中,3种传感器对用户静态和动态认证环境下点击行为的反应.

通过对比图2中动、静态下的传感器数值可发现:1) 用户在不同认证环境下的点击行为之间也存在显着差异. 直观的表现是动态环境下的点击事件会导致加速计产生更大的跳变值,并且会导致陀螺仪和磁力计产生更剧烈的数值波动[9]. 2) 不论是在静态还是动态认证环境下,用户的点击行为都会导致加速度传感器的值发生跳变. 用户输入6位长度的密码对应于加速度传感器的值将受到6次点击事件的影响而产生6个跳变. 因而,为有效区分动静态认证环境,基于统计学方法对每个传感器的数据提取8个时域特征来描述用户的运动模式,包括平均值、中位数、标准差、范围、峰度、偏度和四分位数(25%、75%),这些统计值都是表征数据的波动程度时最常用到的统计量. 其中,范围表示传感器读数的最大值和最小值之间的差值,对于区分用户动静态十分有效. 峰度(K)表征传感器读数的峰值宽度,是数据的标准四阶中心矩. 偏度(S)由数据的三阶标准化矩得到,用以表征传感器读数的峰值方向. 以加速计为例,其计算公式分别为

$$K(a)=\frac{\frac{1}{n}\sum_{i=1}^{n}(a_i-\bar{a})^4}{\left(\frac{1}{n}\sum_{i=1}^{n}(a_i-\bar{a})^2\right)^2}-3 \tag{3}$$

$$S(a)=\frac{\frac{1}{n}\sum_{i=1}^{n}(a_i-\bar{a})^3}{\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(a_i-\bar{a})^2}^3} \tag{4}$$

其中 $\bar{a}$ 是 a 的 n 个数据对应的均值. 此外还提取了传感器数据的样本熵(SampEn)以及傅里叶变换的频谱能量(E_f)作为反映用户行为数据复杂度的特征. 样本熵的计算算法如下.

步骤 1　将 $a_1,\cdots,a_t,\cdots,a_n$ 按顺序组成 m 维矢量,如

$$A_m(i)=[a_i,a_{i+1},\cdots,a_{i+m-1}],1\leqslant i\leqslant n-m+1 \tag{5}$$

步骤 2　定义矢量 $A_m(i)$ 与 $A_m(j)$ 之间的距离为

$$\mathrm{d}[A_m(i),A_m(j)]=\max|a_{i+k}-a_{j+k}|,\\ 1\leqslant k\leqslant m-1;1\leqslant i;j\leqslant n-m+1,i\neq j \tag{6}$$

步骤 3　给定相似容限 $r(r>0)$,计算 $B_i^m(r)$,并计算平均值.

$$B_i^m(r)=\frac{1}{n-m+1}\mathrm{num}\{\mathrm{d}[A_m(i),A_m(j)]<r\} \tag{7}$$

$$B^m(r)=\frac{1}{n-m}\sum_{i=1}^{n-m}B_i^m(r) \tag{8}$$

步骤 4　样本熵为

$$\mathrm{SampEn}=-\ln[B_i^{m+1}(r)/B_i^m(r)] \tag{9}$$

对于加速度数据 a 的傅里叶变换 A_f而言,E_f 计算式为

$$E_f(a)=\sum|A_f|^2 \tag{10}$$

通过计算,共提取了 120 个特征作为上下文特征,这些特征在区分用户身体姿势方面具有很好地表现[9].

此外,从全局和局部 2 个方面来为用户提取点击特征. 全局特征用于表征手机产生的旋转和微动,由时域和频域中特征组成. 时域特征均为上述提及的 8 个统计学时域特征. 4 个频域特征通过计算传感器数据的傅里叶变换得到,分别是频域幅度峰值及其频率、幅度第二大峰值及其频率. 局部特征由用户使用智能手机输入 6 位长度的密码时引起传感器读数产生的跳变值构成,这些值通过极值计算求得,包括 6 个最大峰值和 6 个最小峰值. 全局特征和局部特征组成的 156 个特征构成了点击特征.

3　上下文感知与身份认证

3.1　上下文感知算法

在整个认证过程中,上下文感知首先被执行用于检测用户在使用智能手机输入密码的过程中其身体姿势所对应的认证环境是静态还是动态,因而可将其视为一个二分类问题.

为了从上下文特征中筛选出冗余性小且有益于分类的特征,首先采用最小冗余最大相关(mRMR, minimum-redundancy maximum-relevance)算法进行特征选择. 作为一种滤波式特征选择方法,mRMR 算法可以最大化特征和分类变量之间的相关性,同时最小化不同特征之间的相关性[10],这里的相关性由变量之间的互信息进行度量. 对于 2 个变量 x 和 y 的互信息计算公式为

$$I(x,y)=\iint p(x,y)\log\frac{p(x,y)}{p(x)p(y)}\mathrm{d}x\mathrm{d}y \tag{11}$$

其中:$p(x,y)$为 x 和 y 的联合概率分布函数,$p(x)$和 $p(y)$分别为 x 和 y 的边缘概率分布函数.

利用 mRMR 算法实现特征选择的过程如下.

步骤 1　第 i 个特征和分类变量之间的相关性可通过计算 $I(x_i;c)$得到,不同特征之间的相关性可通过 $I(x_i;x_j)$求得.

步骤 2　为了进一步挑选出来与分类结果相关性大的特征,使用最大相关式进行如下计算:

$$\max D(S,c),D=\frac{1}{|S|}\sum_{x_i\in S}I(x_i;c) \tag{12}$$

其中 S 表示的是特征集.

步骤 3　由于这些特征之间还存在着冗余性,所以需要进一步使用最小冗余式来进一步移除冗余特征,计算式为

$$\min R(S),R=\frac{1}{|S|^2}\sum_{x_i,x_j\in S}I(x_i;x_j) \tag{13}$$

步骤 4　利用加法规则整合最大相关性和最小冗余度:

$$\max\phi(D,R),\phi=D-R \tag{14}$$

进而采用增量搜索方法将其转化为下述优化问题:

$$\max_{x_j\in X-S_{m-1}}\left[I(x_j;c)-\frac{1}{m-1}\sum_{x_i\in S_{m-1}}I(x_j;x_i)\right] \tag{15}$$

通过在已选择的 $m-1$ 个特征组成的特征集

S_{m-1}的基础上,在剩下的$\{X - S_{m-1}\}$的样本自己中找到使式(15)为最大的特征,即可对剩下的特征进行计算和排序.

通过上述方法进行特征选择后,随机森林(RF, random forest)分类算法被选择用于对上述 mRMR 算法选择出来的特征进行分类. RF 算法采用 Bootstrap 方法对样本进行重采样并利用随机属性选择的方法训练多棵决策树,输出结果由所有决策树输出结果的众数而定. 在参数选择时,RF 中的树木的数量根据袋外误差率来确定. RF 的具体实现过程如下.

输入:

① 样本集 $D = \{(x_1, y_1), (x_2, y_2), \cdots, (x_m, y_m)\}$,其中 x_m 为 mRMR 算法选择后的特征,y_m 为上下文标签

② 决策树数目 T

③ 待检测样本 x'

输出:待分类样本的上下文标签 label′

1 For $t = 1:T$ //创建 T 棵决策树

2 通过对 D 进行 t 次 Boostrap 采样,共采集 m 次,得到采样集 D_t

3 利用采样集 D_t 训练第 t 个 CATR 决策树模型 G_t. ① 在训练决策树模型节点时,在节点上所有样本特征中随机选择一部分特征. ② 对这些随机选择的特征计算基尼系数,基尼系数最小的特征作为分裂特征

4 得出随机森林$\{G_1, G_2, \cdots, G_t\}$

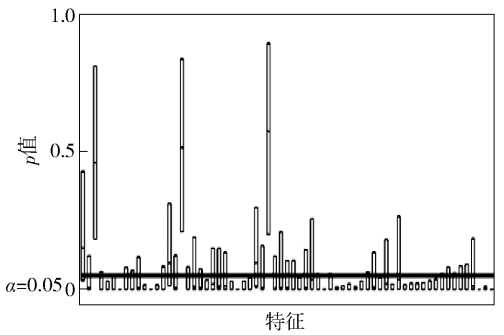
5 End For

6 label′ = 多数投票机制$\{G_1(x'), G_2(x'), \cdots, G_t(x')\}$

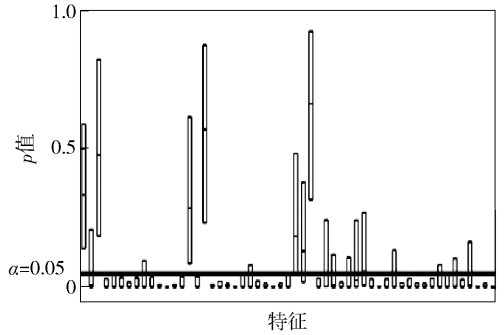
3.2 身份认证算法

所提出的机制在训练阶段会为不同的上下文训练相应的认证子模型,使得不同身体姿势操作下的认证可以自适应地利用相应的认证模型,为了建立鉴别能力较好的认证模型,利用了 K-S (Kolmogorov-Smirnov)检验来从点击特征中挑选出一些有益于区分不同用户的"好"特征.

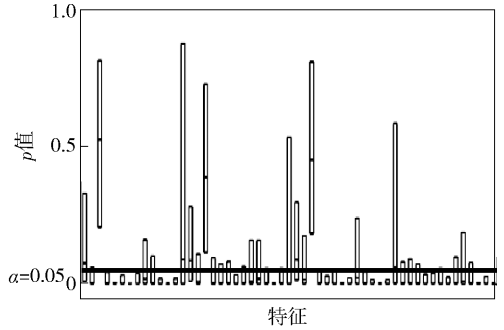
K-S 检验是一种非参数统计假设检验方法,在分析 2 个样本分布是否相同时非常有用. 其原假设表示为 H_0:2 个样本来自相同分布. 在利用该方法提取特征时,需对不同用户的每一维点击特征均进行假设检验,若某一维点击特征对应的原假设 H_0 成立,则认为该特征对于不同用户而言分布相同,即难以有效区分不同用户,将其视为一个"差"特征. 假设用户 1 的 m 个样本对应的某特征集合表示为 $O = O_1, O_2, \cdots, O_m$,用户 2 的 n 个样本对应的某特征集合为 $P = P_1, P_2, \cdots P_n$. 该算法具体的实现过程如下.



(a) 加速计特征的K-S检验结果



(b) 陀螺仪特征的K-S检验结果



(c) 磁力计特征的K-S检验结果

图3 K-S 检验结果

步骤 1 建立假设 H_0:2 个特征集合来自相同分布,即该特征的区分不同用户的能力很差.

步骤 2 计算统计量 $S = \max |F_1(O) - F_2(P)|$,其中 $F_1(O)$和 $F_2(P)$分别为 O 和 P 对应的经验分布函数.

步骤 3 计算统计量 S 对应的显著性水平 p 值,该值由可靠性分布函数 Q_{ks} 表示: $\text{prob}(S) = Q_{ks}(\lambda)$. 其中 $\lambda = \left(\sqrt{N_e} + 0.12 + \frac{0.11}{\sqrt{N_e}}\right)S, N_e = \frac{mn}{m+n}$.

步骤 4 比较 p 值与拒绝域 α(通常取值为

0.05[11]），若 $p>\alpha$，则接受假设 H_0，丢弃该特征.

通过上述过程，对点击特征进行 K-S 检验结果如图 3 所示. 图中详细描述了从每个传感器所提取特征的 K-S 检验结果，横坐标表示特征维数，矩形表示每个特征的 p 值的箱线图分布，加粗横线表示 $\alpha=0.05$的基准线. 通过这种方式，从所有点击特征中剔除了基准线以上的“差”特征.

后续的认证可通过用户的点击行为特征来区分用户是否合法，仍然可视为一个分类问题，相应的认证子模型的训练过程如下.

步骤 1　由上下文特征以及上下文感知算法得到上下文标签，将相同上下文标签对应的 K-S 检验筛选后的点击特征分到一组.

步骤 2　将不同上下文下的点击特征输入 RF 分类器中，分别训练得到相应的认证子模型. 在实际应用中，如果用户当前的认证环境被上下文感知模块划分为静态，那么将会触发其中训练好的静态认证子模型给出认证结果. 反之，如果是动态，则会触发动态认证子模型.

4　实验结果与分析

4.1　数据集

在数据收集过程中，共包括 30 名参与者. 由于所提出的认证方案是用于增强用户密码保护机制的隐式认证，针对用户在密码泄露的情况下仍然可以进一步认证用户，所以在实验仿真中，笔者主要基于用户输入特定密码的行为进行研究. 为此，分别采集了 2 组密码的行为数据进行实验分析，分别是简单密码“111111”和复杂密码“182537”. 前者由重复数字组成，代表极易被破解的简单密码；后者则是数字键盘上不同位置数字的自由组合，代表在日常生活中随机设置的密码.

为数据收集部署了 3 个用户操作环境.

1）静态环境. 使用智能手机在站立或静坐时完成输入密码的行为.

2）动态环境. 在行走时使用智能手机完成输入密码的行为.

3）自由环境. 使用智能手机以使自己喜欢的方式完成输入密码的行为.

在上述 3 种操作环境中，参与者的手势均不受限制，他们可以按自己喜欢的方式握持和点击智能手机，最终共收集了这 30 名参与者的 7000 + 次输入密码行为的数据，具体情况如表 1 所示.

表 1　数据集

密码	操作环境	数据集大小	平均操作次数
111111	静态	1 194	34
111111	动态	1 120	50
111111	自由	1 350	45
182537	静态	1 500	50
182537	动态	1 170	39
182537	自由	1 470	49

4.2　评价标准

1）训练与测试

在实验中，假定一个参与者为智能手机的所有者，表明他/她是合法用户，其余参与者均为攻击者或非法用户. 为了避免合法用户的独特性，从所有参与者中挑选出其中 5 名分别轮流作为合法用户，他们分别是初中生（用户 1：男性，14 岁）、大学生（用户 2：男性，20 岁）、研究生（用户 3：女性，25 岁）以及两名工作人员职业（用户 4：男性，35 岁，用户 5：女性，46 岁）. 在性能评估中，使用了十折交叉验证法来划分训练集和测试集，并重复这种测试方法 10 次，将这 10 个结果的平均值作为最终结果.

2）性能评估

错误接受率（FAR，false acceptance rate）和错误拒绝率（FRR，false rejection rate）是生物认证系统广泛使用的评估指标. FAR 是允许非法用户成功入侵智能手机的次数与他尝试的次数之比. FRR 是合法用户被拒绝访问智能手机的次数与他尝试的次数之比.

4.3　认证结果分析

1）操作环境的影响

为了避免用户操作环境变化的影响，现有的相关研究集中于某个特定操作环境中的隐式认证. 例如，只对用户坐下时输入密码的行为数据进行研究. 然而，用户的身体姿势在现实生活中是多变的，这种不可避免的多变性将使得其身份验证方法在实际应用时往往表现出比实验结果中更差的性能. 为了对上述内容做进一步的阐述，笔者对以下 2 种情况进行了认证实验：① 训练集和测试集为相同的操作环境（均为用户静坐时输入密码的行为数据），用以模拟大多数现有研究的实验方案；② 训练集和测试集都处于不受控的自由操作环境，用以模拟用户在实际生活中的真实操作环境. 对 2 种情况分别进行认

证实验,所得的认证结果如表2所示.

表2 不同操作环境的认证结果(密码:182537)

情况	操作环境		认证结果	
	训练集	测试集	FRR/%	FAR/%
①	行为数据(静坐操作)	行为数据(静坐操作)	0	1.66
②	行为数据(自由操作)	行为数据(自由操作)	4.46	3.76

从表2可见,情况①下的认证性能优于情况②,阐述了目前现有研究在实际应用时性能会变差的现象. 这一现象的发生主要是因为实际生活中用户的操作环境并不受控,特别是用户身体姿势的变化会使得用户的点击行为变得复杂、稳定性降低,因而导致相应的认证性能变差.

对于情况①,一个人的点击行为在某一特定操作环境下是相对稳定的,因此FRR可以达到0%. 不同于情况①,情况②中的操作环境更为复杂,这种环境的复杂多变性对FRR和FAR均产生了不良影响. 比情况①得到了更大的FRR,表明自由操作环境下一个人的点击行为数据是不稳定的,这也进一步证实了人体姿势的变化会对点击行为产生显著影响. 同时,情况②中更大的FAR意味着在自由操作环境中不同用户的点击行为之间存在着更大的相似性. 表现为某用户在行走时的点击行为可能与另一个用户在坐下操作时的点击行为之间高度相似,从而使FAR变大.

2)上下文感知的有效性

为了探索上下文感知的认证方案的有效性,分别对有和无上下文感知的身份认证进行了实验. 表3中括号中的数据代表是无上下文感知的认证结果,与不加括号的数据所代表的有上下文感知的结果相比,具有上下文感知的认证性能要优于无上下文感知的认证.

表3 不同密码下对应有(无)上下文感知的认证结果

用户	密码:111111		密码:182537	
	FAR/%	FRR/%	FAR/%	FRR/%
1	3.19(5.30)	3.65(5.16)	2.06(4.25)	2.78(5.76)
2	1.45(2.07)	0.83(2.44)	0.80(2.59)	0.28(3.56)
3	0.00(3.72)	0.51(3.90)	0.52(3.24)	0.00(3.16)
4	1.12(3.06)	1.40(3.44)	1.03(2.24)	0.94(2.67)
5	1.93(4.16)	1.37(3.78)	1.10(3.16)	1.15(2.98)
平均值	1.54(3.57)	1.56(3.74)	1.29(3.10)	1.03(3.62)

如果在无上下文感知的情况下使用所提出的认证方法,FAR和FRR的平均值约为3.5%. 然而,在引入上下文感知后,FAR和FRR的平均值可降低至1.5%左右. 而且,无论是简单密码还是复杂密码下的隐式认证,对于每位用户而言,在有上下文感知时的认证性能均优于没有上下文感知的认证,进一步表明了上下文感知对整个认证性能起着积极作用.

3)密码强度的影响

在以往的一些相关研究中,基于复杂密码的隐式认证性能普遍要比简单密码好很多. 因为在这些相关研究中都普遍使用了用户点击行为的一些按压时间间隔作为认证特征,例如停留时间、间隔时间等[1-2]. 停留时间是指按下和释放相同按钮的时间,间隔时间表示按下2个连续按键之间的时间间隔. 显然,对于这种时长特征而言,密码越简单,不同用户的时长特征会越相似,因而得到的认证性能也会相对较差. 不同于这些以往的研究方法,所提出的解决方案是利用具有更高鲁棒性的一些运动特征来认证用户.

从表3中可以看出,对于不同强度密码的隐式认证性能而言,平均FAR和FRR之间的差值在0.5%之内,表明所提出的认证方案对简单密码也很友好. 简单密码下的隐式认证取得的最佳FAR和FRR分别为0和0.51%,复杂密码下的隐式认证取得的最佳FAR和FRR分别为0.52%和0,说明了所提出的身份认证算法的有效性.

4)与相关工作的对比

对相关工作[3-4]的认证方法进行了相应的认证测试,所得到的认证结果如表4所示. 对比可见,所提出的上下文认证机制所得的FAR和FRR要远小于相关工作[4],在所有认证中取得了最小的FAR和FRR,可以实现最佳的认证性能.

表4 与相关工作的认证性能对比

方法	FRR/%	FAR/%
文献[3]	3.8	3.8
文献[4]	8.00	8.99
本文方法	1.29	1.03

5 结束语

基于上下文感知对生物识别系统的性能具有改善作用,提出了一种基于上下文感知的智能手机隐式身份认证机制. 实验结果表明,通过将用户的身

体姿势作为上下文信息，并实现上下文感知的身份认证，不同用户认证所得的平均 FAR 和 FRR 可由原来的 3.5% 左右降至 1.5% 左右. 所提方案不仅对复杂密码有效，而且对于简单密码的认证仍然可以取得较好的效果，充分表明了所提出的认证机制有效可行.

参考文献：

[1] Zheng Nan, Bai Kun, Huang Hai, et al. You are how you touch: user verification on smartphones via tapping behaviors[C]//2014 IEEE 22nd International Conference on Network Protocols. New York: IEEE Press, 2014: 221-232.

[2] Gurary J, Zhu Ye, Alnahash N, et al. Implicit authentication for mobile devices using typing behavior[M]// Lecture Notes in Computer Science. Cham: Springer International Publishing, 2016: 25-36.

[3] Inoue M, Ogawa T. TapOnce: a novel authentication method on smartphones[J]. International Journal of Pervasive Computing and Communications, 2018, 14(1): 33-48.

[4] Teh P S, Zhang Ning, Teoh A B J, et al. Recognizing your touch[C]// Proceedings of the 13th International Conference on Advances in Mobile Computing and Multimedia-MoMM 2015. New York: ACM Press, 2015: 108-116.

[5] Sitova Z, Sedenka J, Yang Qing, et al. HMOG: new behavioral biometric features for continuous authentication of smartphone users[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(5): 877-892.

[6] Feng Tao, Yang Jun, Yan Zhixian, et al. TIPS: context-aware implicit user identification using touch screen in uncontrolled environments[C]// Proceedings of the 15th Workshop on Mobile Computing Systems and Applications. New York : ACM, 2014: 1-6.

[7] Nappi M, Ricciardi S, Tistarelli M. Context awareness in biometric systems and methods: state of the art and future scenarios[J]. Image and Vision Computing, 2018, 76: 27-37.

[8] Ehatisham-Ul-haq M, Azam M A, Loo J, et al. Authentication of smartphone users based on activity recognition and mobile sensing[J]. Sensors, 2017, 17(9): 2043-2074.

[9] 肖玲，潘浩. 基于 WiFi 信号的人体动作识别系统[J]. 北京邮电大学学报，2018，41(3)：119-124.
Xiao Ling, Pan Hao. Human activity recognition system based on WiFi signal[J]. Journal of Beijing University of Posts and Telecommunications, 2018, 41(3): 119-124.

[10] Peng H, Long F, Ding C. Feature selection based on mutual information criteria of max-dependency, max-relevance, and min-redundancy[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2005, 27(8): 1226-1238.

[11] Massey F J Jr. The Kolmogorov-Smirnov test for goodness of fit[J]. Journal of the American Statistical Association, 1951, 46(253): 68-78.