doi:10.11835/j.issn.1000-582X.2021.209

自适配权重特征融合的持续身份认证

陶 鹏,邓绍江
(重庆大学 计算机学院,重庆 400044)

摘要:针对现有智能手机用户身份认证方法的不足,提出了一种自适配权重特征融合的持续身份认证方法。设计了一种卷积神经网络,对手机内置传感器(加速度计、陀螺仪、磁力计)获取的用户行为信息数据进行深度特征提取及融合。通过网络中 3 个子网络流分别提取 3 种传感器特征,在特征融合层加权融合,各特征的权值会在网络学习过程中根据不同特征的贡献度实现自适应分配。融合特征经过特征选择之后,使用单分类支持向量机进行用户分类认证。实验结果表明:该方法对不同用户身份认证获得的等错误率为 1.20%,与现有其他认证方法相比具有更好的认证准确性。

关键词:持续身份认证;自适配权重;深度特征融合;卷积神经网络;单分类支持向量机
中图分类号:UTP391.4 **文献标志码**:A **文章编号**:1000-582X(2023)01-103-010

Continuous authentication based on adaptive deep feature fusion

TAO Peng, *DENG Shaojiang*
(College of Computer Science, Chongqing University, Chongqing 400044, P. R. China)

Abstract: To address the shortcomings of the existing smartphone user authentication methods, this paper proposes a continuous identity authentication method based on adaptive weight feature fusion. A convolution neural network is designed to extract and fuse the deep features of user behavior information data obtained from the built-in sensors (accelerometer, gyroscope, magnetometer) of mobile phones. In the network, three kinds of sensor features are extracted from the three sub-network flows respectively, and weighted fusion is performed in the feature fusion layer. The weight of each feature is adaptively assigned according to the contribution of different features in the network learning process. After feature selection for fused features, one-class support vector machine is used for user classification and authentication. The experimental results show that this method achieves an equal error rate of 1.20% for different user authentication. Compared with other existing authentication methods, the proposed method demonstrates better authentication accuracy.

Keywords: continuous authentication; adaptive weight; deep feature fusion; convolutional neural network (CNN); one-class support vector machine (OC-SVM)

收稿日期:2021-03-01 **网络出版日期**:2021-04-29
基金项目:国家自然科学基金资助项目(61672119)。
Supported by National Natural Science Foundation of China (61672119).
作者简介:陶鹏(1994—),男,硕士研究生,主要从事移动计算安全研究,(E-mail) 930095496@qq.com。
通信作者:邓绍江,男,教授,博士生导师,主要从事信息安全、移动计算、无线传感网络等研究,(E-mail) sj_deng@cqu.edu.cn。

智能手机已逐渐成为日常生活的必备工具，其存储着大量与用户个人隐私相关的信息，所带来的隐私安全问题已受到日趋重视。身份认证技术则是保护手机用户隐私安全的重要方式之一。

基于行为特征的持续身份认证，是指在用户与手机交互过程中，通过手机内置传感器自动获取用户的行为信息数据，提取相关行为特征，并使用分类算法来完成对用户身份合法性的认证。该认证方式具有持续、隐式的特点，克服了传统的基于密码和基于生物生理特征等一次性身份认证的局限性，已成为身份认证研究的重点方向[1-2]。目前基于行为特征的认证，大多数基于单一行为信息，如步态[3-4]、触摸手势[5-6]等，来提取特征用于认证，所提取的特征大多是人为设计的特征。随着深度学习的发展，卷积神经网络已被部分研究者应用于用户认证，以自动提取更具鲁棒性的行为特征[7-9]。此外，信息融合技术也在基于行为特征的用户持续认证中得到了应用[10-17]，以克服单一行为特征认证的局限性。基于信息融合的认证根据认证的流程可以分为数据级、特征级、分数级和决策级的4个层级的融合。特征级融合属于中间层的融合，它突破了单一特征在噪声、数据质量差等方面的限制，能够实现多特征之间优势互补，相比其他层级的融合可以实现更高的认证准确率。文献[12]和文献[13]的特征融合均是对步态和击键行为数据分别提人工特征，并对2种模态特征进行串联融合。文献[14]同样采取串联的融合策略，所提取特征是击键和手持2种行为数据的特征。文献[15]对加速度计、陀螺仪、磁力计等传感器采集的行为数据提取人工特征，同时使用了串联和并联的特征融合策略。现有的基于特征融合的身份认证方法在认证性能上虽然表现出色，但在特征融合时都是融合人为设计的特征，人工特征往往只适用于研究者特定的实验环境，且产生的认证精度有限。此外，这些方法在融合策略方面仅采取简单的串联和并联方法，没有将不同特征对认证贡献度的大小考虑其中，所以基于特征融合的身份认证还有提升的空间。

针对以上存在的问题，文中提出了一种自适配权重特征融合的身份认证方法，对传统的人工特征提取进行改进，设计了一种卷积神经网络提取多种传感器的深度特征，该特征具有更强的鲁棒性。在进行多特征融合时，对常用的串并联策略进行改进，设计了一种依据不同特征贡献度大小，实现自适配权重分配的融合策略，以使得融合后的特征具有更强的表现力，能够实现更有效和准确的身份认证。

1 持续身份认证框架

基于自适配权重特征融合的持续认证的系统框架如图1所示。

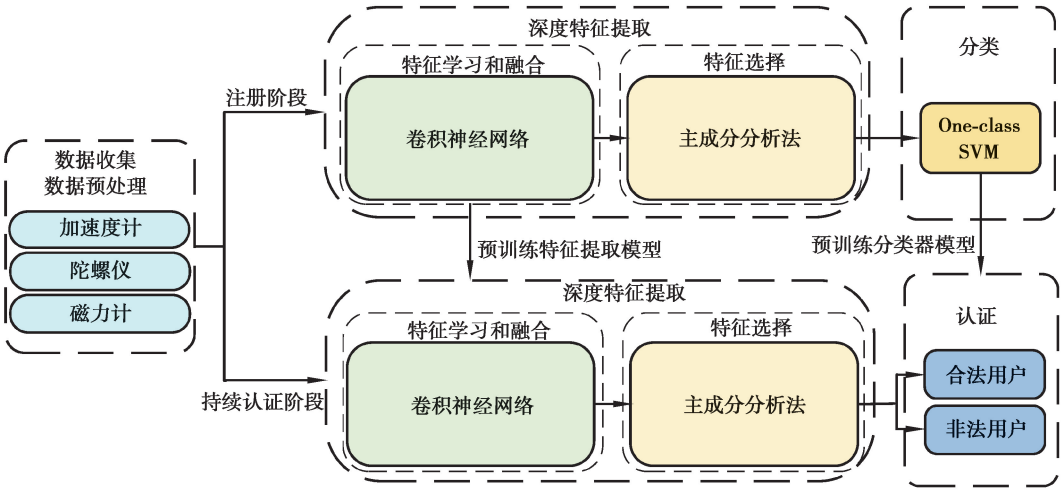


图1 基于自适配权重特征融合持续认证系统框架图

Fig. 1 Framework of continuous authentication system based on adaptive weight feature fusion

整个认证系统包括注册和持续认证2个阶段。注册阶段主要是完成对深度特征提取和分类认证2个模型的训练，在用户与手机交互的过程中，手机内置加速度、陀螺仪和磁力计传感器会自动获取到用户的行为信息数据，在经过预处理之后，输入到卷积神经网络中进行训练。该网络能够独立地提取3种传感器的特

征，并在网络的融合层中根据不同特征对认证贡献度大小进行自适配权重的融合，训练好的网络模型将作为特征提取模型。输出的融合特征经过特征选择之后，会输入到单分类支持向量机中进行训练得到分类认证模型。而在持续认证阶段，其他未知的用户以同样的方式获取传感器数据并预处理之后，使用预训练的特征提取和分类认证模型进行用户的身份认证。

2　数据的获取和预处理

2.1　3 种传感器数据的获取

笔者所用传感器数据来源于用户持续认证公开数据集[18]，该数据集的收集是通过在三星 Galaxy S4 手机上安装的数据采集工具进行的，采样频率为 100 Hz。采集了 100 名手机用户在 3 种使用场景下（文档阅读；文本编辑；地图导航）的行为信息数据。每个用户收集到 24 个会话（8 个阅读会话、8 个编辑会话以及 8 个地图导航会话），共 2～6 h 的数据。

在剔除包含缺失或异常数据的用户之后，最终选择了 100 个用户中的 95 个，将其加速度计、陀螺仪以及磁力计传感器的前 100 min 约 600 000 样本量的数据用于实验。加速度计传感器的原始数据可以表示为 $d\times n$ 的矩阵 $\boldsymbol{R}_{\mathrm{acc}}=(\boldsymbol{x}_{\mathrm{acc}},\boldsymbol{y}_{\mathrm{acc}},\boldsymbol{z}_{\mathrm{acc}})^{\mathrm{T}}$，其中 d 表示维度 3（即 x，y，z 轴），n 表示数据样本总量，$\boldsymbol{x}_{\mathrm{acc}}=(x_{\mathrm{acc},1},x_{\mathrm{acc},2},\cdots,x_{\mathrm{acc},n})$ 表示加速度计 x 轴上数据序列，$\boldsymbol{y}_{\mathrm{acc}}$ 和 $\boldsymbol{z}_{\mathrm{acc}}$ 分别为 y 轴和 z 轴的数据序列。类似地，陀螺仪和磁力计传感器的原始数据表示为，$\boldsymbol{R}_{\mathrm{gyr}}=(\boldsymbol{x}_{\mathrm{gyr}},\boldsymbol{y}_{\mathrm{gyr}},\boldsymbol{z}_{\mathrm{gyr}})^{\mathrm{T}}$ 和 $\boldsymbol{R}_{\mathrm{gyr}}=(\boldsymbol{x}_{\mathrm{gyr}},\boldsymbol{y}_{\mathrm{gyr}},\boldsymbol{z}_{\mathrm{gyr}})^{\mathrm{T}}$。

2.2　数据的预处理

2.2.1　数据归一化

为减少原始数据中噪声等异常对认证性能的影响，使用均值–标准差归一化对原始数进行处理。分别对各个传感器的每一轴数据序列（以加速度计传感器 x 轴数据序列 $\boldsymbol{x}_{\mathrm{acc}}=(x_{\mathrm{acc},1},x_{\mathrm{acc},2},\cdots,x_{\mathrm{acc},n})$ 为例）执行以下运算：

$$\boldsymbol{x}^{*}_{\mathrm{acc}}=\frac{x_{\mathrm{acc},i}-\overline{x}_{\mathrm{acc}}}{\sigma},\tag{1}$$

式中：下标 i 表示是序列 $\boldsymbol{x}_{\mathrm{acc}}$ 中第 i 个数据样本；$x_{\mathrm{acc},i}$ 和 x^{*}_{acc} 分别表示归一化之前和之后的样本；$\overline{x}_{\mathrm{acc}}$ 和 σ 表示加速度计 x 轴数据序列的均值和标准差，其计算方式分别为

$$\overline{x}_{\mathrm{acc}}=\frac{1}{n}\sum_{i=1}^{n}x_{\mathrm{acc},i},\tag{2}$$

$$\sigma=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_{\mathrm{acc},i}-\overline{x}_{\mathrm{acc}})^{2}}。\tag{3}$$

各传感器归一化之后的数据为 $\boldsymbol{R}^{*}_{\mathrm{acc}}=(\boldsymbol{x}^{*}_{\mathrm{acc}},\boldsymbol{y}^{*}_{\mathrm{acc}},\boldsymbol{z}^{*}_{\mathrm{acc}})^{\mathrm{T}}$、$\boldsymbol{R}^{*}_{\mathrm{gyr}}=(\boldsymbol{x}^{*}_{\mathrm{gyr}},\boldsymbol{y}^{*}_{\mathrm{gyr}},\boldsymbol{z}^{*}_{\mathrm{gyr}})^{\mathrm{T}}$ 和 $\boldsymbol{R}^{*}_{\mathrm{mag}}=(\boldsymbol{x}^{*}_{\mathrm{mag}},\boldsymbol{y}^{*}_{\mathrm{mag}},\boldsymbol{z}^{*}_{\mathrm{mag}})^{\mathrm{T}}$。

2.2.2　时间窗口划分

对归一化之后的加速度计数据 $\boldsymbol{R}^{*}_{\mathrm{acc}}$ 划分时间窗口，将其划分为 τ 秒时间窗口且数据宽度为 k（$k=\tau\times f_{\mathrm{s}}$，其中 f_{s} 为采样频率）的片段数据，每个时间片段的数据可表示成 $d\times k$ 的矩阵 $\boldsymbol{T}_{\tau}=(\boldsymbol{x}_{\mathrm{acc}},\boldsymbol{y}_{\mathrm{acc}},\boldsymbol{z}_{\mathrm{acc}})^{\mathrm{T}}$，其中 $\boldsymbol{x}_{\mathrm{acc}}=(x_{\mathrm{acc},1},x_{\mathrm{acc},2},\cdots,x_{\mathrm{acc},k})$ 表示加速度计传感器在时间 τ 内 x 轴上的样本，通过划分可以得到 (n/k) 数量的时间窗口的数据。陀螺仪传感器数据 $\boldsymbol{R}^{*}_{\mathrm{gyr}}$ 和磁力计传感器数据 $\boldsymbol{R}^{*}_{\mathrm{mag}}$ 也依此方式进行划分。

3　特征的提取及自适配特征融合

在设计的用于特征提取的卷积神经网络结构中，引入了 ShuffleNet V2[19] 轻量级网络框架中的基本模块（basic block）和下采样模块（down block）。这 2 种模块是在带有残差结构的深度可分离卷积（depthwise separable convolution）结构的基础上，加入通道分割（channel split）、拼接（concat）和通道混合（channel shuffle）等操作改进而来，相比普通的卷积，在不损失模型较大精确度的前提下，可以减少大量计算参数，适合在智能手机这种资源有限的移动设备上进行运算。基于这 2 种模块设计了如图 2 所示的一种卷积神经网络结构，该结构由卷积层 1，包含下采样模块 1 和基本模块 1 的阶段 2，包含下采样模块 2、基本模块 2 和基本

模块3的阶段3,卷积层2,全连接层1和全连接层2组成,使用该网络对不同传感器数据提取深度特征。

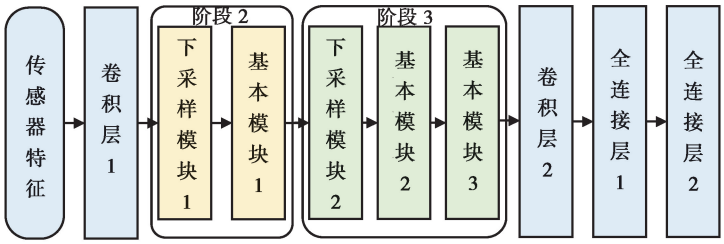
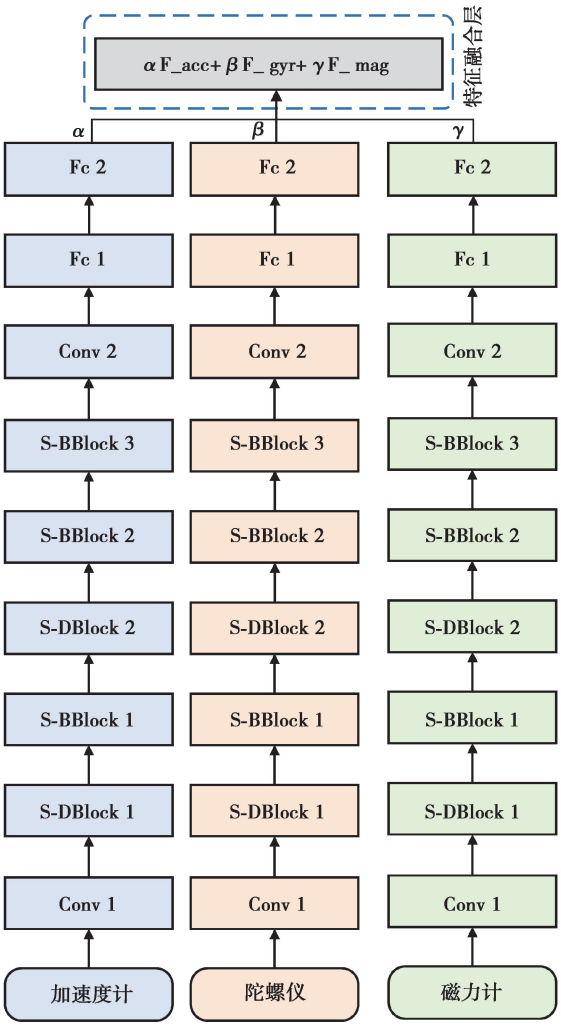


图2 卷积神经网络结构

Fig. 2 Structure of convolution neural network

为了充分利用各个传感器采集的数据,使各个传感器所提取的特征达到优势互补,需要对这些传感器的特征进行融合。笔者将特征融合功能结合到了卷积神经网络中,设计了如图3所示的多传感器特征融合的网络结构,该网络将图2网络作为子网络流提取3个传感器的特征,在全连接层2之后加入特征融合层,特征融合层将输出各传感器的融合特征向量。迭代更新融合的特征向量,以最小化网络的损失函数为目标训练模型,直到模型收敛为止。



注:Conv表示卷积层,S-BBneck和S-DBneck分别表示ShuffleNet V2的基本模块和下采样模块,Fc表示全连接层,F_acc、F_gyr、F_mag表示全连接层2输出的特征向量

图3 多传感器特征融合的网络结构

Fig.3 Network structure of multi-sensor feature fusion

传统特征融合策略是串联和并联，即对原始多模特征进行横向和纵向连接。以双模特征向量融合为例，对于 2 个同质向量 $\boldsymbol{v}_1$ 和 $\boldsymbol{v}_2$，特征维度分别为 a 和 b，使用串联方式融合，融合后特征向量为 $\boldsymbol{v}=[\boldsymbol{v}_1,\boldsymbol{v}_2]$ 的形式，其维度为 $a+b$。使用并联方式融合，融合后特征向量为复向量 $\boldsymbol{v}=\boldsymbol{v}_1+i\,\boldsymbol{v}_2$（$i$ 为虚数单位），融合特征的维度为 a 和 b 中的较大者，对于维度较低的向量融合后相应位用 0 补位。

并联和串联的融合策略将原始特征重要性同等看待，没有考虑不同特征对认证结果的贡献度大小。文中对每个子网络流输出的传感器特征乘以一个自动分配的权重系数，通过这种方式，在网络迭代的过程中，自动地根据贡献度大小为传感器特征分配自适应的权重系数。每个子网络流中的传感器特征都在特征融合层以公式(4)的前向和公式(5)的反向传播的方式进行迭代：

$$\text{前向传播：}X_{\text{out}}=\alpha X_{\text{in}}, \tag{4}$$

$$\text{反向传播：}\frac{\partial L}{\partial X_{\text{in}}}=\alpha\frac{\partial L}{\partial X_{\text{out}}}, \tag{5}$$

式中：X_{in} 和 X_{out} 表示特征融合层每个子网络流的输入和输出；α 表示权重；$\partial x/\partial X_{\text{in}}$ 和 $\partial L/\partial X_{\text{out}}$ 分别表示损失函数对 X_{in} 和 X_{out} 的偏导数。

在网络训练阶段，将各模态传感器的权重初始化为 1/3，经过自动学习，具有不同权重的传感器特征会形成融合特征：

$$\boldsymbol{F}=\alpha\,\boldsymbol{F}_{\text{acc}}+\beta\,\boldsymbol{F}_{\text{gyr}}+\gamma\,\boldsymbol{F}_{\text{mag}}, \tag{6}$$

式中：α、β 和 γ 是每个传感器的自适配权重；$\boldsymbol{F}_{\text{acc}}$、$\boldsymbol{F}_{\text{gyr}}$、$\boldsymbol{F}_{\text{mag}}$ 和 $\boldsymbol{F}$ 分别为 3 个传感器提取的初始深度特征向量和融合深度特征向量，维度均是 95。

网络中选用的损失函数是交叉熵损失函数，具有如下的形式：

$$L(l,v)=-\omega\log\left(\frac{e^{v}}{\sum_{j=1}^{N}e^{v_j}}\right), \tag{7}$$

式中：l 是传感器数据对应的用户标签；N 是用户的数量，为 95；v 是第二个全连接层的输出，可以表示为

$$\begin{aligned}v&=\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{F}+b=\\&\boldsymbol{\omega}^{\mathrm{T}}(\alpha\boldsymbol{F}_{acc}+\beta\boldsymbol{F}_{gyr}+\gamma\boldsymbol{F}_{mag})+b,\end{aligned} \tag{8}$$

式中：ω 和 b 是第二个全连接层的权重和偏差。

4　分类与认证

4.1　分类器训练

在提取深度融合特征之后，对所有用户进行分类训练。采集的行为数据中均为合法用户数据，缺少非法用户数据。对于这种正负样本失衡的分类问题，笔者使用单分类支持向量机（one-class support vector machine，OC-SVM）作为分类器。单分类支持向量机算法，类似于将零点当做负样本点，其他数据点作为正样本点进行训练的二分类支持向量机。具体策略是将数据映射到与内核对应的特征空间上，在数据和零点之间构建超平面，并最大化零点到超平面的距离。训练过程中选用径向基函数（radial basic function，RBF）作为核函数，并使用网格搜索法的方式进行超参数的选定。

4.2　用户认证

在深度特征提取融合的网络模型训练之后会生成深度特征提取融合模型，单分类支持向量机训练之后会生成用户认证模型。在认证阶段，用户使用手机期间 3 种传感器实时采集的行为数据经过预处理之后，输入深度特征提取融合模型，然后将输出的融合特征输入用户分类认证模型中，完成对用户身份合法性的判断，当检测到非法用户时，将进行重新认证或异常处理。

5　实验分析

5.1　认证性能评估指标

文中后续实验使用以下常用的持续认证系统的评估指标。

错误接受率（false acceptance rate，FAR）表示认证系统将非法手机用户错认为是合法手机用户的概率，

计算公式如式(9)所示，其值越小，表示认证系统越不会接受非法用户，安全性越好。

$$S_{\mathrm{FAR}}=\frac{F_{\mathrm{A}}}{F_{\mathrm{A}}+T_{\mathrm{R}}}, \tag{9}$$

式中：F_{A}表示系统错误地将非法用户当成合法用户；T_{R}表示系统正确地拒绝了非法用户。

错误拒绝率(false rejection rate，FRR)表示认证系统将合法手机用户错认为是非法手机用户的概率，计算公式如(10)所示，其值越小，认证系统越不会拒绝合法用户，易用性越好。

$$S_{\mathrm{FRR}}=\frac{F_{\mathrm{R}}}{T_{\mathrm{A}}+F_{\mathrm{R}}}, \tag{10}$$

式中：F_{R}表示系统错误地将合法用户当成非法用户；T_{A}表示系统正确地识别了合法用户。

等错误率(equal error rate，EER)是错误接受率和错误拒绝率相等(即$S_{\mathrm{FAR}}=S_{\mathrm{FRR}}$)时候的值，是认证系统的综合评价指标，其值越小表示认证系统整体性能越好。

5.2 深度融合特征的选择

3种传感器的特征经过自适配权重的特征融合之后形成了95维的高维深度融合特征，高维特征不仅影响分类效率，而且其包含的噪声对分类认证性能有较大影响。文中选用主成分分析法(principal component analysis，PCA)对深度融合特征进行选择，以5为步长，探究选择的不同特征数目下的认证的等错误率，其结果的箱型图如图4所示。从图4可以看出，整体上随着选择的特征数目的增加，等错误率的均值逐渐降低并在30时达到一个最低值，之后等错误率的均值随着选择特征数目的增加而缓慢地增加。因此，选择30作为最终用于认证的深度融合特征的数目。

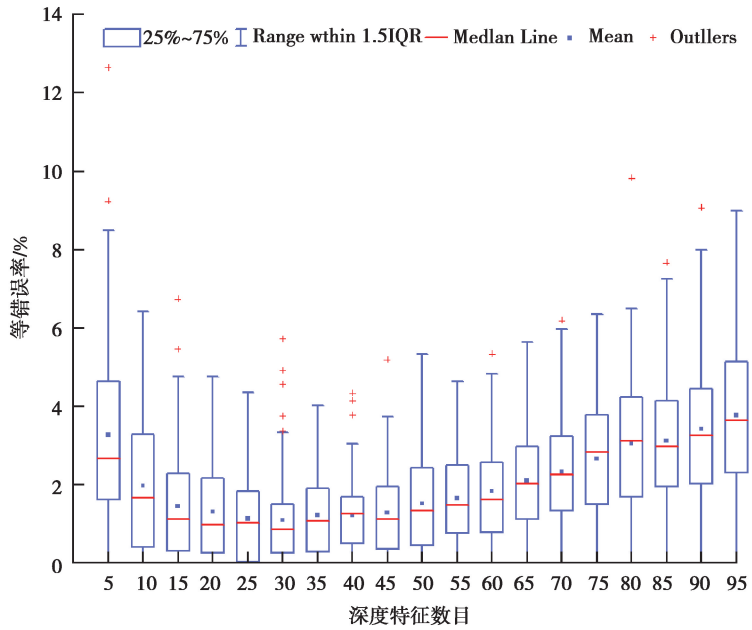


图4 不同数目的深度融合特征认证的等错误率

Fig. 4 Equal error rate under different numbers of deep fusion feature authentication

5.3 时间窗口大小的选定

时间窗口的大小决定了输入数据量的大小，对认证性能有着重要的影响。笔者研究了1～10 s，以1 s为间隔的时间窗口大小下认证的性能，结果如图5所示。可以看出，随着时间窗口大小的增加，等错误率均值逐渐下降，在5 s后，下降趋势变得平缓。时间窗口的大小同时也决定了认证的时间间隔，影响用户体验。在综合考虑认证性能和用户体验之后，将时间窗口大小设置为5 s，并在后续实验中默认使用这一设置。

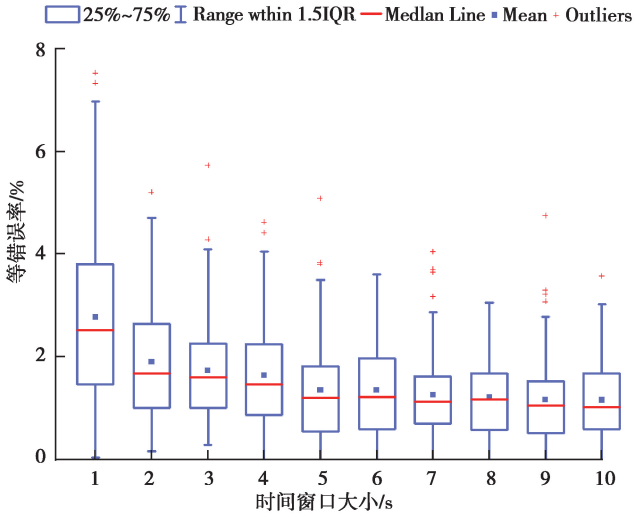


图 5　不同时间窗口大小认证的等错误率

Fig. 5　Equal error rate of authentication with different time window sizes

5.4　与人工特征及串并联融合的比较

为了验证文中提出的卷积神经网络进行深度融合特征提取，以及使用自适配权重特征融合策略的有效性，分别进行了串联融合策略下深度和人工特征提取的认证（记做串联方案）实验，以及并联融合策略下深度和人工特征提取的认证（记做并联方案）实验。进行深度特征提取时延续本文提出的方法，并在分类认证阶段沿用单分类支持向量机。进行人工特征提取时，选取了基于传感器认证常用的 10 个统计特征，诸如均值（mean）、标准差（standard deviation）、最大值（maximum）、最小值（minimum）、差值（range）、峰度（kurtosis）、斜度（skewness）以及 25%、50%、75%百分数（quartile）等，详情如表 1 所示。而在分类认证上除了延续使用单分类支持向量机，还使用了具有代表性的二分类器，诸如 k 最近邻（k-nearest neighbor，k-NN）、支持向量机（support vector machine，SVM）以及决策树（decision tree，DT）。出于比较的目的，其他方面的设置均保持一致。

表 1　人工设计的特征

Table 1　Characteristics of artificial design

特征	解释
均值	时间窗口内传感器数据的均值
标准差	时间窗口内传感器数据的标准差
最大值	时间窗口内传感器数据的最大值
最小值	时间窗口内传感器数据的最小值
差值	时间窗口内传感器数据最大值与最小值之差
峰度	时间窗口内传感器数据的宽度
斜度	时间窗口内传感器数据峰值的宽度
百分数	传感器数据序列的 25%、50%和 75%百分数

串联方案及并联方案与文中提出的方法认证的结果对比分别如图 6 和图 7 所示（图中 CNN 代表使用文中提出神经网络提取特征，并使用单分类支持向量机分类器的认证，OC-SVM、kNN、SVM 和 DT 分别代表

基于人工特征的提取，并使用各自二分类器的认证）。

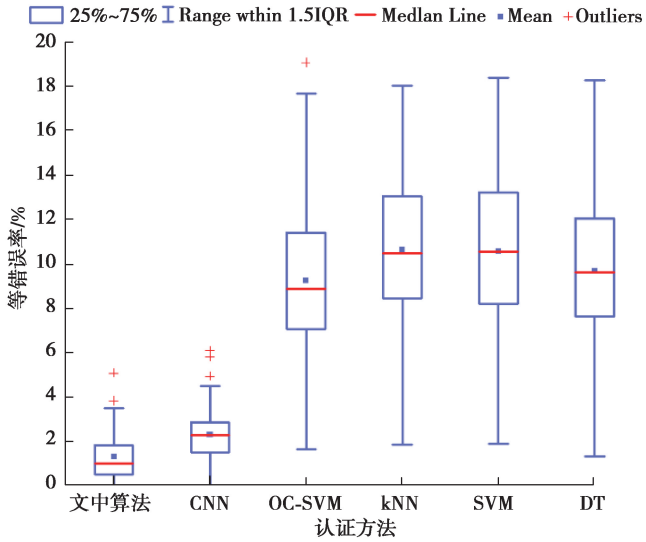


图6 与深度和人工特征在串联融合下的认证性能比较

Fig. 6 Comparison of authentication performance with serial fusion of deep and manual features

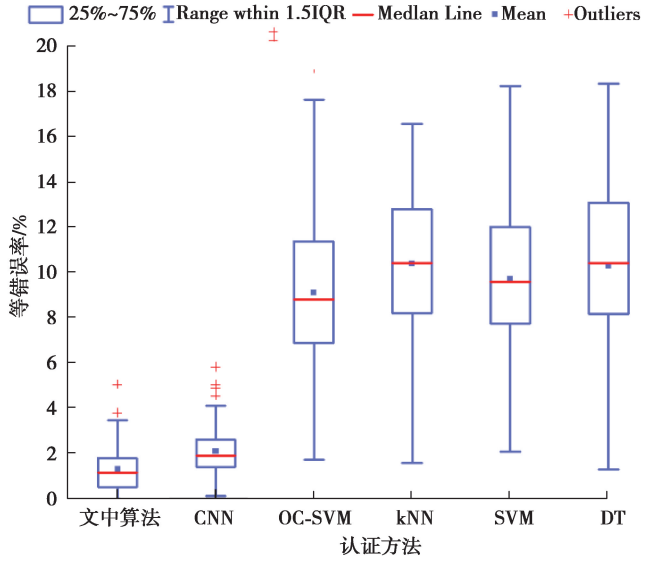


图7 与深度和人工特征在并联融合下的认证性能比较

Fig. 7 Comparison of authentication performance with parallel fusion of deep and manual features

可以看出在串联和并联融合策略下，不同认证性能整体上具有类似的趋势。具体来说，基于人工设计的特征在认证性能上都具有较高的等错误率，与使用其他二分类器相比，单分类支持向量机的等错误率更低一些，这也验证了选择单分类支持向量机用于认证分类的有效性。使用卷积神经网络进行特征提取，与人工特征的认证相比，都具有更低的等错误率，而文中提出的自适配权重融合策略与串联和并联方案相比，进一步降低了等错误率，具有最好的认证性能。

5.5 不同数目传感器融合的比较

文中提出的特征融合是对加速度计、陀螺仪和磁力计3种传感器的融合，为进一步验证认证系统的有效性，进行了：①3项用3种传感器分别提取特征（无特征融合）的认证实验；②3项两两组合2种传感器提取深度特征并融合的认证实验。这6项实验得到的认证性能，与文中所提方法的认证性能对比结果如表2所示。由表2可知，实验②比实验①的认证性能都有所提升，并在融合陀螺仪和磁力计传感器提取特征的时候达到较低的3.12%的等错误率，3.13%的错误接受率和3.10%的错误拒绝率。而对3种传感器进行特征融合，其等

错误率、错误接受率和错误拒绝率都出现了显著降低，达到了所有特征融合方案中最低的 1.20%、1.32%和 0.88%。

表 2　不同传感器深度特征融合的性能比较

Table 2　Performance comparison of deep feature fusion of different sensors　%

传感器	S_{FAR}	S_{FRR}	S_{EER}
加速计	5.20	5.12	5.14
陀螺仪	5.45	5.44	5.44
磁力计	5.13	5.01	5.11
加速计＋陀螺仪	3.22	3.10	3.13
加速计＋磁力计	3.34	3.30	3.32
陀螺仪＋磁力计	3.13	3.10	3.12
加速计＋陀螺仪＋磁力计	1.32	0.88	1.20

5.6　与现有相关工作的对比

将文中方法与现有的基于融合的持续身份认证相关工作[15,16,20]，从传感器、特征类型、融合方式、分类器、认证准确性等方面进行了对比，结果如表 3 所示。

表 3　与现有相关认证方法的比较

Table 3　Comparison with existing authentication methods

方法	传感器	特征类型	融合方式	分类器	性能
文献 [20]	Acc，Gyr，Mag，Ori	人工特征	数据级融合	HMM	$S_{EER}=4.76\%$
文献[16]	Acc，Gyr	人工特征	决策级融合	kNN，SVM	$S_{FAR}=7.50\%$，$S_{FRR}=6.64\%$
文献 [15]	Acc，Gyr，Mag	人工特征	特征级融合(串联、并联)	SVDD	$S_{BER}=1.47\%$，$S_{BER}=1.49\%$
文中方法	Acc，Gyr，Mag	CNN 特征	特征级融合(自适配权重)	OC-SVM	$S_{EER}=1.20\%$

由表 3 可知，文献[20]中使用多传感器的数据级融合方式并使用隐马尔科夫(Hidden Markov model，HMM)分类器的认证实现了 4.76%的等错误率。文献[16]使用 k 最近邻和支持向量机分类器并使用决策级融合的认证实现了 7.50%的错误接受率和 6.64%的错误拒绝率。文献[15]使用特征融合的方式，并在串并联策略下使用支持向量数据描述分类器(support vector data description，SVDD)，分别实现了 1.47%和 1.49%的均衡错误率(balanced error rate，BER)，其认证性能相比数据级和决策级认证具有显著的提升。相比其他工作提取人工特征，文中提出的方法则利用 CNN 提取深度特征，融合方式上采用特征级融合，并使用新的自适配权重融合策略，进一步提高了认证性能，在所有方法中达到了最低的 1.20%的等错误率。表 3 中，Acc、Gyr、Mag、Ori 分别代表加速度计、陀螺仪、磁力计和方向传感器。

6　结　论

针对目前持续认证方中的问题，提出了自适配权重特征融合的持续认证方法。经过实验验证，该认证方法实现了 1.20%的认证等错误率，与提取人工特征或深度特征，并结合串并联特征融合策略的认证相比显著降低了等错误率。对比了不同数目传感器融合的认证，3 种传感器的融合实现了最好的认证性能。与现有其

他融合方式认证的对比，显示了该方法具有较好的优越性。在未来的工作中，将在现有特征融合研究的基础上，结合数据级，决策级等其他融合方式，以进一步提高持续认证系统的认证性能。

参考文献：

[1] Abuhamad M, Abusnaina A, Nyang D H, et al. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: a contemporary survey[J].IEEE Internet of Things Journal, 2020, 8(1): 65-84.

[2] Mahfouz A, Mahmoud T M, Eldin A S. A survey on behavioral biometric authentication on smartphones[J]. Journal of Information Security and Applications, 2017, 37: 28-37.

[3] Nickel C, Wirtl T, Busch C. Authentication of smartphone users based on the way they walk using k-nn algorithm[C]// 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing. IEEE, 2012: 16-20.

[4] Hoang T, Choi D, Nguyen T. Gait authentication on mobile phone using biometric cryptosystem and fuzzy commitment scheme[J]. International Journal of Information Security, 2015, 14(6): 549-560.

[5] Shih D H, Lu C M, Shih M H. A flick biometric authentication mechanism on mobile devices[C]// 2015 International Conference on Informative and Cybernetics for Computational Social Systems (ICCSS). IEEE, 2015: 31-33.

[6] Lin C C, Chang C C, Liang D, et al. A new non-intrusive authentication method based on the orientation sensor for smartphone users[C]// 2012 IEEE Sixth International Conference on Software Security and Reliability. IEEE, 2012: 245-252.

[7] Volaka H C, Alptekin G, Basar O E, et al. Towards continuous authentication on mobile phones using deep learning models[J]. Procedia Computer Science, 2019, 155: 177-184.

[8] Giorgi G, Saracino A, Martinelli F. Using recurrent neural networks for continuous authentication through gait analysis [J]. Pattern Recognition Letters, 2021.

[9] Xiaofeng L, Shengfei Z, Shengwei Y. Continuous authentication by free-text keystroke based on CNN plus RNN[J]. Procedia Computer Science, 2019, 147: 314-318.

[10] Sitová Z, Šeděnka J, Yang Q, et al. HMOG: New behavioral biometric features for continuous authentication of smartphone users[J]. IEEE Transactions on Information Forensics and Security, 2015, 11(5): 877-892.

[11] Prakash A. Continuous user authentication based score level fusion with hybrid optimization[J]. Cluster Computing, 2019, 22(5): 12959-12969.

[12] Do S, Hoang T, Luong C, et al. Using keystroke dynamics for implicit authentication on smartphone[J]. Journal of Korea Multimedia Society, 2014, 17(8): 968-976.

[13] Lamiche I, Bin G, Jing Y, et al. A continuous smartphone authentication method based on gait patterns and keystroke dynamics[J]. Journal of Ambient Intelligence and Humanized Computing, 2019, 10(11): 4417-4430.

[14] Buriro A, Crispo B, Gupta S, et al. Dialerauth: A motion-assisted touch-based smartphone user authentication scheme[C] // Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy. 2018: 267-276.

[15] Li Y, Zou B, Deng S, et al. Using feature fusion strategies in continuous authentication on smartphones[J]. IEEE Internet Computing, 2020, 24(2): 49-56.

[16] Gao L, Lian Y, Yang H, et al. Continuous authentication of mouse dynamics based on decision level fusion[C]// 2020 International Wireless Communications and Mobile Computing (IWCMC). IEEE, 2020: 210-214.

[17] Zhang Q, Li H, Sun Z, et al. Deep feature fusion for iris and periocular biometrics on mobile devices[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(11): 2897-2912.

[18] Yang Q, Peng G, Nguyen D T, et al. A multimodal data set for evaluating continuous authentication performance in smartphones[C]// Proceedings of the 12th ACM Conference on Embedded Network Sensor Systems. 2014: 358-359.

[19] Ma N, Zhang X, Zheng H T, et al. Shufflenet V2: Practical guidelines for efficient cnn architecture design[C]// Proceedings of the European Conference on Computer Vision (ECCV). 2018: 116-131.

[20] Shen C, Li Y, Chen Y, et al. Performance analysis of multi-motion sensor behavior for active smartphone authentication [J]. IEEE Transactions on Information Forensics and Security, 2017,13(1): 48-62.

（编辑 詹燕平）