文章编号：2095-2163(2023)12-0087-06 中图分类号：TP391 文献标志码：A

基于多尺度卷积和 LSTM 的多模态隐式认证

金瑜瑶，张晓梅
（上海工程技术大学 电子电气工程学院，上海 201620）

摘 要：针对以往身份认证大多基于单一模态信号、准确率不够高等问题，提出了一种基于多尺度卷积和长短期记忆网络融合的多模态隐式认证方案（MMC-LSTM）。结合智能移动设备在多传感器下的运动特征和触摸特征作为多模态特征进行输入，根据并行的多尺度卷积层捕获多维度的行为特征，并使用长短期记忆网络弥补对短序列识别的不足，从而实现更准确的认证。为减少用户姿态转变带来的影响，构建了先识别不同姿态再进行认证的总体框架。实验结果表明，所提方案在公开数据集上的认证准确率可达到 98.2%，比单模态特征认证准确率提高了 1.3%，能有效提升身份认证的准确性。

关键词：多尺度卷积；LSTM；多模态特征；隐式认证；深度学习

Implicit authentication of multi-modal based on multi-scale convolution and LSTM

JIN Yuyao, ZHANG Xiaomei
(School of Electric and Electronic Engineering, Shanghai University of Engineering Science, Shanghai 201620, China)

Abstract: A multi-modal implicit authentication scheme (MMC-LSTM) based on the fusion of multi-scale convolution and long and short-term memory neural network is proposed to address the problem that most previous authentication is based on single-modal signals and the accuracy rate is not high enough. Combining the motion features and touch features of smart mobile devices under multiple sensors as multimodal feature inputs, extracting behavior characteristics of different dimensions in parallel based on multi-scale convolution with different-sized convolution kernels, and using long and short-term memory networks to compensate for the lack of recognition of short sequences, a more accurate authentication can be achieved. To reduce the impact of user posture shifts, a general framework of recognizing different postures before authentication is constructed. Experimental results show that the proposed scheme can achieve an authentication accuracy of 98.2% on public datasets, which is 1.3% higher than the accuracy of single-modal feature authentication and can effectively improve the accuracy of identity authentication.

Key words: multi-scale convolution; LSTM; multi-modal feature; implicit authentication; deep learning

0 引 言

随着全球移动互联网以及电子移动设备的普及，越来越多的人偏向把个人隐私和敏感数据保存在智能移动设备中（如：智能手机、智能手表等）。然而，这些信息一旦丢失或泄露，将会造成一定的经济损失和安全风险，因此有必要研究一种安全可靠的技术来保证当前用户身份的合法性。

隐式身份认证[1]相较于传统的显式身份认证[2-5]（包括口令、智能卡、指纹认证、面部识别等认证方式），其可以通过移动设备内置的传感器直接捕获行为数据，不需要用户完成特定操作，不必频繁使用口令密码，并且将会不间断、无干扰地对用户进行身份认证，因此具有较高的隐蔽性和安全性。当前的隐式认证方法主要分为 3 类，分别是基于步态特征[6-7]、基于击键特征[8-9]以及基于触屏特征[10-11]的认证方法。Chang 等人[12]提出了一个基于堆栈的深度学习网络，将用户产生的触摸数据进行特征提取和分类，利用用户触摸行为习惯达到隐式认证的目的。Matteo 等人[13]将智能手机绑定在用户裤子前袋中，通过内置的加速度和陀螺仪传感器来表征独特的步态行为特征，再利用卷积神经网络（Convolutional Neural Network, CNN）和支持向量机（Support Vector Machines, SVM）实现隐式认证。然而，由于环境的复杂性和灵活性，特征单一的单模态特征容易受到伪造[14]攻击，因此多模态融合认证

基金项目：国家自然科学基金（61802252）。
作者简介：金瑜瑶（1996-），女，硕士研究生，主要研究方向：身份认证、深度学习。
通讯作者：张晓梅（1981-），女，博士，副教授，主要研究方向：信息安全、身份认证。Email：xmzhang@ sues.edu.cn
收稿日期：2022-12-24

显得更为重要。Sitová 等人[15]从智能手机内置的加速度、陀螺仪和磁力计传感器中获取 HMOG 特征，表征操作设备的手部运动速度和方向数据，并结合击键特征和 HMOG 特征使等错误率达到了 7.16%～10.05%。Volaka 等人[16]通过对比触摸屏数据、3 种运动传感器数据以及两者组合的性能选择最优输入。陀螺仪和触摸数据的组合实现了 88%的平均准确度，优于其单一特征实现的认证性能，但对比现有研究成果达到的认证性能仍存在较大差距。

此外，在实际应用场景中，用户灵活的姿态转变也极大地影响了身份认证的准确性。Qin 等人[17]融合多个 CNN 和时钟递归神经网络 CW-RNN 提取运动传感器的时域和频域特征，提出了新的认证框架 SSUI。该框架考虑到用户坐、站、行走和骑行 4 类使用场景，但仅实现了 95%以上的认证准确率。以上研究表明，CNN 对于运动传感器的特征提取具有较优的性能，而 RNN 可以增强模型处理时间序列的能力，但针对长时间序列的处理与不同姿势转变带来的特征偏移问题，简单的深度网络并不能满足实际认证需求。

为了解决上述问题，本文提出了一种多模态融合的隐式认证方法。该方法使用改进的多尺度卷积网络（Multi-scale Convolutional Neural Network，MCNN）以及长短期记忆（Long and Short-Term Memory，LSTM）模型，通过 MCNN 对预处理创建的三通道图像同时学习分段级特征。基于此，采用 LSTM 来捕获行为中所有时段间的时间依赖性，用于姿势识别，为两种场景中的姿态分别构建相应的子模型。最后，通过融入触摸数据策略，在 MMC-LSTM（Multi-modal based on Multi-scale Convolution and LSTM）模型中进行分类认证。在公开数据集上的实验结果表明，所提方法具有良好的性能。

1 相关知识

1.1 多尺度卷积模块

多尺度卷积能够模仿人类的视觉系统，当人视线中出现一幅图片时，会产生大量模糊到清晰的图像数组，而多尺度卷积网络则模拟了不同距离下景物在人类视网膜上形成的不同图片。本文使用的用户行为特征数据是多维的，多尺度卷积可以同时进行多个卷积操作，利用不同的卷积核来提取不同维度的行为特征，全面地进行分类。因此，根据特征特点，本文提出了一种适合多维行为特征分类的多尺度卷积模块，如图 1 所示。

首先，分别采用 3 种并行的不同尺度的卷积核来捕捉特征的多样性，接着通过特征联合层将多尺度特征进行特征融合，并输入 BN 批标准化层和 ReLU 激活层。BN 层可以加快训练速度和收敛速度，改善梯度爆炸和梯度消失问题，降低过拟合风险，而 ReLU 层能增加网络稀疏性，减少计算复杂度。最后通过最大池化层减少网络的参数量，防止网络过拟合。

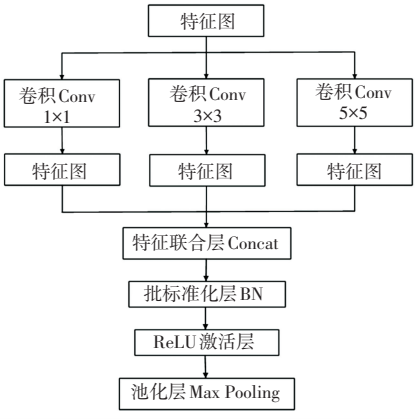

图 1 多尺度卷积模块

Fig. 1 Multi-scale convolution module

1.2 LSTM 模块

LSTM 网络是对 RNN 模型的一种有效改进，通过称为“门”的复杂结构和细胞状态，选择性地控制信息的添加和移除。LSTM 单元包括遗忘门（f_t）、输入门（i_t）和输出门（o_t），用于保护和控制单元的状态，在较长序列中有更好的记忆表现，相关表达如公式（1）所示：

$$\begin{cases} f_t = \sigma(\boldsymbol{W}_f \cdot [h_{t-1}, x_t] + \boldsymbol{b}_f) \\ i_t = \sigma(\boldsymbol{W}_i \cdot [h_{t-1}, x_t] + \boldsymbol{b}_i) \\ \tilde{C}_t = \tanh(\boldsymbol{W}_c \cdot [h_{t-1}, x_t] + \boldsymbol{b}_c) \\ C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t \\ O_t = \sigma(\boldsymbol{W}_o [h_{t-1}, x_t] + \boldsymbol{b}_o) \\ h_t = O_t * \tanh(C_t) \end{cases} \tag{1}$$

其中，$\boldsymbol{W}_f$、$\boldsymbol{W}_i$ 和 $\boldsymbol{W}_c$、$\boldsymbol{W}_o$ 分别表示遗忘门、输入门和输出门的权重矩阵；$\boldsymbol{b}_f$、$\boldsymbol{b}_i$ 和 $\boldsymbol{b}_c$、$\boldsymbol{b}_o$ 分别表示遗忘门、输入门和输出门的偏置向量；x_t 是 t 时刻的信息输入；h_{t-1} 是前一时刻的输出；C_t 是 t 时刻的细胞状态；σ 是 sigmoid 函数；⊙是矩阵相乘。

虽然本文通过数据到图像的方法将原始传感器信号转换为二维图像，但转换后的图本质上是时间序列的另一种表现。两个相邻 map 之间仍然存在时间联系，因此使用 LSTM 加 Softmax 层取代传统

CNN 网络中的全连接层作为认证网络的分类器。

2　基于多尺度卷积和 LSTM 多模态隐式认证方案设计

2.1　认证方案总体框架

本文所提出的认证方案，首先需要采集用户操作期间运动传感器和触摸屏产生的两个维度的信号。由于数据采集过程中可能存在噪声干扰、信号偏移等问题，故本文通过异常值剔除、小波去噪和平均映射，对原始数据进行预处理，并对触摸数据进行数据增强，最后将其转换为图像作为 MMC－LSTM 模型的输入。考虑到用户在与智能设备进行交互时会产生不同的姿态，该认证方案设计了场景感知模块，将其分割为静态场景和动态场景，传感器特征作为判断不同姿态场景的依据，为两类场景构建相应的认证模型。其中，静态场景是指较为稳定的身体状态（如：站、坐）；动态场景指的是行为幅度较大的运动状态（如：行走、上下楼等）。训练好的分类模型直接用于身份认证，并将融合后未参加训练的多模态数据用于识别用户的合法性，以此提高认证的性能。本文使用 HMOG 公开数据集[18]验证所提方案性能，总体框架如图 2 所示。

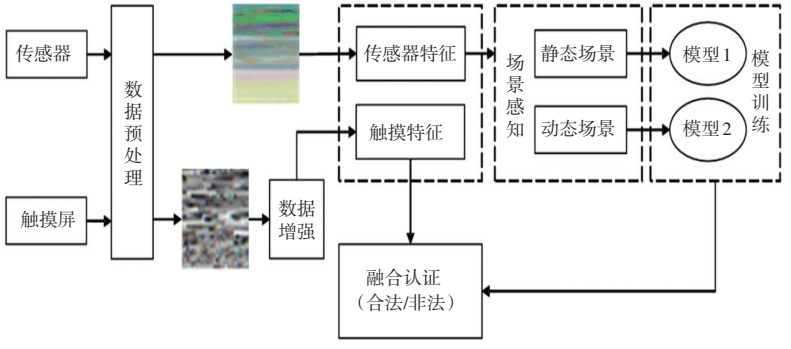

图 2　隐式认证框架

Fig. 2　Implicit authentication framework

2.2 多模态数据预处理

2.2.1　数据集构建

2.2.1.1　传感器数据

当用户携带智能设备或与其交互时，行为方式、触摸姿势、运动速度的改变，都会导致内置传感器的数值发生细微变化。加速度计记录用户较大的运动模式，如手臂姿势、走路姿势等；陀螺仪记录用户细微的运动模式，如握持姿势造成的设备旋转角速度；磁力计记录环境磁场强度的变化。三个传感器的数值变化可以综合表征用户运动过程中的场景信号，分别由 X、Y、Z 三轴所构成的 9 列阵列信号表示，如公式(2)、公式(3)所示：

$$\begin{cases} acc_i = [acc_i^X, acc_i^Y, acc_i^Z]^{\mathrm{T}} \\ gyr_i = [gyr_i^X, gyr_i^Y, gyr_i^Z]^{\mathrm{T}} \\ mag_i = [mag_i^X, mag_i^Y, mag_i^Z]^{\mathrm{T}} \end{cases} \tag{2}$$

$$D_i = [acc_i, gyr_i, mag_i]^{\mathrm{T}} \tag{3}$$

其中，acc 代表加速度计；gyr 代表陀螺仪；mag 代表磁力计；D_i 表示第 i 个用户的原始运动传感器数据。

2.2.1.2　触摸数据

在智能设备的触摸屏中，可以获取用户执行滑动和点击操作的时间戳、x 和 y 方向上的位置、触摸面积和压力等数据。滑动操作可视为由一系列的触摸点组成，在不同操作场景下，用户产生的滑动操作存在个体差异性。例如：滑动轨迹不同、轨迹长度不同、触摸时间不同等。当用户产生滑动操作时，本文将触摸时间戳（t_i）和触摸点在屏幕上的 x、y 方向位置（x_i、y_i）作为三维信号用于输入，用数学符号表示为

$$S_i = [t_i, x_i, y_i],\ i = 1, 2, \cdots, n \tag{4}$$

用户的点击特征是由手掌大小、手指长度、指尖大小等决定的，当用户产生点击特征时，本文将触摸点位置（x_i、y_i）和接触面积（c_i）三维信号作为模型的输入，从中提取用户的使用习惯和触摸位置特征，丰富用户身份特征，用数学符号表示为

$$T_i = [x_i, y_i, c_i],\ i = 1, 2, \cdots, n \tag{5}$$

2.2.2　信号去噪

设备内置的传感器在采集过程中，会受到高频电子噪声和随机噪声的干扰，因此必须采取相应的手段，对运动传感器数据进行平滑去噪处理，以确保后续认证的准确性。在本文中，使用小波去噪来去除信号中的噪声。相较于传统的低通滤波器，小波去噪能保证在消除噪声的同时，最大可能地保留原

始数据信号形状、宽度等分布特征。具体步骤如下：

(1)对含噪声的信号进行小波变换；

(2)对变换得到的小波系数进行处理，以去除其中包含的噪声；

(3)对处理后的小波系数进行小波逆变换，得到去噪后的信号。

在此随机截取了某个用户加速度计 X 轴的数据，去噪前后的信号变化如图 3 所示。

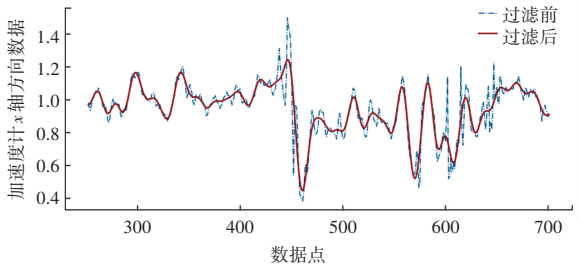

图 3 信号在小波去噪前后的比较

Fig. 3 Comparison of signals before and after wavelet denoising

2.2.3 二维图像转换

大多数深度学习框架均是基于 CNN 进行搭建，但深度网络对于一维信号的处理并不理想，为了更好地利用深度网络在图像处理方面的优势，本文将多模态数据在馈送到网络模型之前，先转化为二维图像数据后，再输入到模型中。针对一维信号，至少每 200 个数据点内会有 1~2 个交互动作产生，故本文按照长度为 200 的滑动窗口截取信号，同时为了降低数据顺序的依赖性，设定相邻窗口之间重叠率为 50%，意味着前一个样本与当前样本包含 50%的重叠数据。再将提取的子列信号组成对应的特征矩阵，最后通过平均映射得到二维图像。转换过程如图 4 所示。

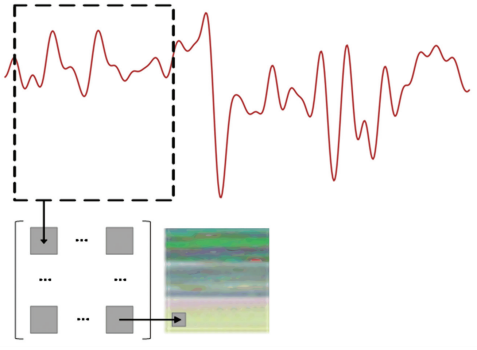

图 4 一维信号转为二维图像过程

Fig. 4 The process of converting 1D signal to 2D image

2.2.4 触摸数据增强

深度学习方法的性能通常依赖于大量的训练数据，在实际操作场景中，触摸行为发生频率低且单个操作单元时间长，无法获取足够多的时间序列数据，因此需要对触摸数据进行数据增强。本文利用翻转、旋转、明亮度改变、像素平移、添加噪声等多种图像增强的方式，来提取原始图像数据中转换不变的数据特性，在其基础上产生更多数据样本，从而实现对触摸数据的扩充。

2.3 MMC-LSTM 模型设计

本文提出的隐式身份认证模型主要由多尺度卷积模块和长短期记忆模型组成，两者的融合能够更全面、更高效地对多模态特征进行提取。传统的卷积算法仅采用单个尺寸的卷积核进行特征挖掘，对于运动传感器和触摸行为信号来说，会损失许多深层行为特征。为了更好地提取身份信息，本文构建了多尺度卷积模块，利用大小为 1、3、5 的卷积核进行特征提取，并且每个多尺度模块中都执行了池化操作，加快网络训练速度。

MMC-LSTM 模型由 2 个多尺度卷积模块、2 个池化层、1 个卷积层和 2 个 LSTM 层堆叠，以及 Softmax 层组成。卷积操作后使用 BN 算法加快网络学习速率，每层的激活函数均采用 ReLU 函数，使用 LSTM 模块代替全连接层执行分类。LSTM 包含了对序列信息的选择性传输、添加或删除，将选择后的特征输入到 Dropout 层，避免网络过度拟合，提高模型的鲁棒性。网络结构如图 5 所示，其中 MSConv 代表多尺度卷积模块，Conv 代表卷积层。

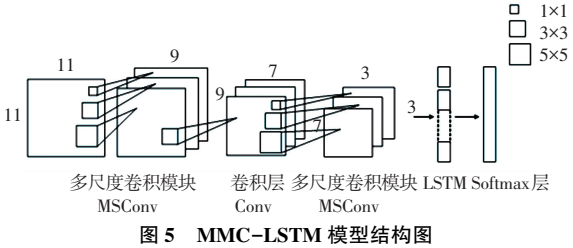

图 5 MMC-LSTM 模型结构图

Fig. 5 The model structure of MMC-LSTM

3 实验与分析

本文实验均在 PyTorch 框架下运行。Batch_size 设定为 64；学习率设定为 0.000 1。模型实验选择 Adam 优化器，损失函数为分类交叉熵损失函数。

3.1 数据来源

本文使用公开数据集 HMOG(Hand Movement, Orientation, and Grasp)[18] 研究隐式认证方法。该数据集以不引人注目地捕捉用户轻触屏幕时产生的细微手部微动作和方向模式，包括运动传感器读数以及触摸屏幕数据。在数据收集中，志愿者将被随机分配在坐姿或者行走状态下的任务，数据集满足本次实验所需。

3.2　评价指标

本文选用生物认证系统广泛使用的评估指标：准确率（*Accuracy*）、错误拒绝率（*FRR*）和错误接受率（*FAR*），利用 *AUC* 值来评价该方案的性能。如公式（6）所示：

$$FRR = \frac{FN}{TP + FN}$$

$$FAR = \frac{FP}{FP + TN}$$

$$AUC = \frac{\sum_{i}^{P} r_i - \frac{P(P+1)}{2}}{P \times N} \tag{6}$$

其中，在本文模型中，*FN* 为假负例，即真实值为合法，预测值为非法的样本；*FP* 为假正例，即真实值为合法，预测值为非法的样本；*TP* 为真正例，即真实值和预测值都为合法的样本；*TN* 为真负例，即真实值和预测值都为非法的样本。

AUC 值的意义为随机选一对正例和负例，正例得分大于负例得分的概率，式中 P 为正例个数，N 为负例个数，i 为 P 中一个正例的序号，r_i 表示为第 i 个正例的序号。

3.3　MMC-LSTM 模型性能分析

为了验证所提 MMC-LSTM 模型的有效性，基于同一数据集在 CNN、LSTM 网络上进行了对比试验，以准确率和 *AUC* 值作为评估指标，对比实验的结果见表 1。LSTM 对于时间序列较长的数据集占有较大的优势，但是触摸数据长度较短，限制了 LSTM 模型的作用。传统的 CNN 能够提取到相关的时空特征，但是识别类间相似特征的能力不足，认证结果也不理想。表 1 结果表明，基于多尺度卷积和 LSTM 的模型，相比传统 CNN 和 LSTM 认证精度分别提高了 3.3%和 4.6%，达到 98.2%，且 *AUC* 值也达到了 0.968。说明多尺度特征学习能够增强模型的输入信息，平衡序列长度带来的误差，改善不同姿势转换时产生的数据偏移，提高模型的分类性能。

表 1　不同模型的准确率和 *AUC* 值对比

Table 1　Comparison of accuracy and *AUC* values of different models

模型	准确率/%	*AUC*
CNN	94.9	0.914
LSTM	93.6	0.892
MMC-LSTM	98.2	0.968

3.4　多模态认证性能比较

本文融合了运动传感器数据和触摸屏数据，作为多模态数据表征用户的行为特征。其中，运动传感器体现了用户与智能设备交互时运动状态的变化，不同轴向的数值变化幅度也反映出用户触摸设备的接触角度和接触压力；触摸屏数据展现了用户触摸屏幕的位置、触摸面积，由此反映了用户的触摸行为习惯。仅单一运动传感器数据和融合多模态触摸屏数据后的认证准确率曲线如图 6 所示。可以看出，本文所提出的 MMC-LSTM 模型对于单一运动传感器数据的认证就能实现较好的身份认证性能，在融合触摸屏数据后，认证性能进一步提升。并且对比表 2 可知，多模态下准确率比单模态提高了1.3%，同时，FAR 和 FRR 均低于单一模态数据的认证。由此表明，本文提出的多模态数据集可以更好地增强用户的信息表征。

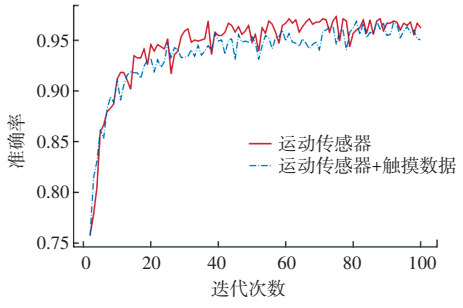

图 6　单模态与多模态认证的准确率曲线对比

Fig. 6　Comparison of accuracy curves for single-modal and multi-modal authentication

表 2　单模态与多模态认证性能对比

Table 2　Comparison of performance for single-modal and multi-modal authentication

数据类型	准确率/%	FAR/%	FRR/%
运动传感器	96.9	2.9	3.2
运动传感器+触摸数据	98.2	1.3	2.4

3.5　与现有研究成果比较

为了验证本文方案的有效性和优越性，本文从数据源和模型方面与其他研究进行对比。表 3 中，文献[15]和文献[19]仅使用运动传感器数据进行身份认证。文献[15]利用人工手动提取相关特征，得到 7.16%（行走）和 10.05%（坐姿）的等错误率，此方法不仅数据维度少，而且需要耗费大量人力资源。文献[19]虽然使用了卷积神经网络进行认证，但是认证精度较低。文献[20]融合了运动传感器和触摸数据，通过深度学习模型执行身份识别，但该模型无法准确地提取多模态深层特征，导致平均准确率仅为 88%，比本文方案的准确率低了近 10%。

综上所述，本文采用多模态融合的身份认证比单一模态效果更好，且所提出的 MMC-LSTM 模型具有更强大的特征提取能力，能挖掘出多模态数据更多的潜在特征，也拥有更强的场景自适应能力。

表 3 相关工作对比

Table 3 Comparison of related work

相关研究	输入数据源	特征提取方式	模型	行为场景	实验性能
文献[15]	Acc, Gyr, Mag	人工	Scaled Mantattan	坐姿/行走	EER:7.16%~10.05%
文献[19]	Acc, Gyr, Mag	网络	CNN	坐姿/行走	Acc:97.8%
文献[20]	Touch,Acc, Gyr, Mag	网络	三层	坐姿/行走	Acc:88% EER:15%
本文	Touch,Acc, Gyr, Mag	网络	MMC-LSTM	坐姿/行走	Acc:98.2%

4 结束语

本文提出基于运动传感器和触摸屏特征的多模态隐式认证方案,通过深度学习的方法,融合多尺度卷积和长短期记忆网络建立模型,提取用户在不同姿态下的运动行为特征区分场景状态,再使用多模态特征融合,实现了隐式身份认证的目的。实验结果表明,该方案能有效阻止非法用户入侵移动设备,无论与单模态数据相比,还是与其他模型相比,认证准确率都更高。而如今每个用户会拥有不同的移动设备,例如智能手机、智能平板等,未来的研究将优化本文模型并应用于多个设备,从而达到用户可以在不同设备上进行身份认证的目的。

参考文献

[1] 杨建强, 方磊. 基于用户使用移动设备习惯的隐式认证初探[J]. 计算机时代, 2012(3):7-9.

[2] 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.

[3] SIMANJUNTAK G D, RAMADHANI K N, 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.

[4] 陈虹旭,李晓坤,郑永亮,等. 基于深度学习的指纹识别方法研究[J]. 智能计算机与应用,2018,8(3):64-69.

[5] 周航, 蔡茂国, 吴涛, 等. 一种改进的多任务级联网络人脸检测算法研究[J]. 智能计算机与应用, 2021,11(3): 172-176.

[6] TRIVINO G, ALVAREZ A, BAILADOR G. Application of the computational theory of perceptions to human gait pattern recognition[J]. Pattern Recognition, 2010, 43(7):2572-2581.

[7] 李文娟,沈澍,孙绍山,等. 智能设备上步态识别系统设计与实现[J]. 计算机技术与发展,2022,32(12):57-62.

[8] LEE H, HWANG J Y, LEE S, et al. A parameterized model to select discriminating features on keystroke dynamics authentication on smartphones[J]. Pervasive and Mobile Computing, 2019, 54: 45-57.

[9] 芦效峰,张胜飞,伊胜伟. 基于 CNN 和 RNN 的自由文本击键模式持续身份认证[J]. 清华大学学报(自然科学版),2018,58(12):1072-1078.

[10] 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.

[11] 庞永春,孙子文,王尧. 基于手机触摸屏传感器多点触摸身份认证算法[J]. 计算机应用,2015,35(6):1780-1784.

[12] CHANG I, YAW L C, SEOKMIN C, et al. Kernel deep regression network for touch-stroke dynamics authentication[J]. IEEE Signal Processing Letters, 2018, 25(7):1109-1113.

[13] MATTEO G, MICHELE R. IDNet: Smartphone-based gait recognition with convolutional neural net-works[J]. Pattern Recognition, 2018, 74(1):25-37.

[14] 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.

[15] 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, 2016, 11(5):877-892.

[16] 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.

[17] QIN Z, HU L, ZHANG N, et al. Learning-aided user identification using smartphone sensors for smart homes[J].IEEE Internet of Things Journal, 2019, 6(5): 7760-7772.

[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. New York, NY, USA: Association for Computing Machinery, 2014:358-359.

[19] CENTENO M P, GUAN Y, MOORSEL A V. Mobile based continuous authentication using deep features[C]// Proceedings of the 2nd International Workshop on Embedded and Mobile Deep Learning. New York, NY, USA: Association for Computing Machinery, 2018: 19-24.

[20] 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.