《网络空间安全系统设计》
课程报告

使用智能手机超声波窃取签名人身份

小组成员： 张立飞 余天航 李冲 李润锦 刘皓予

2024 年 4 月 9 日

西北工业大学网络空间安全学院

目录

一、研究背景

1.1 项目简介

手写签名已成为许多场景下的重要认证方式。然而，使用手写方式签名也可能带来潜在的安全漏洞，使攻击者能够窃取到签名人的身份。这种漏洞的基本原理是手写签名的动作会改变附近的信号模式，不同人签名的动作行为细节不同，这种信息变化可以被智能手机扬声器和麦克风扑捉到，并对具体行为进行分析，从而确定签名人身份。这种新的攻击可以使受害者在不知情的情况下从远程发起窃听。因此，本文基于手机超声波信号，通过信号检测、特征提取和机器学习构建了手写签名窃听模型，对模型性能进行了全局性评价和鲁棒性评价，结果表明，该模型对手写签名的窃听识别具有一定效果。

除了完成基本任务外，我们还使用创新的滑动窗口信号检测算法（Sliding Window Signal Detection Algorithm）进行了原始数据提取的优化，利用一种创新的离散信号处理方式来处理数据，提取特征，并分别使用了支持向量机（Support

Vector Machine，SVM)、随机森林（Random Forest）和贝叶斯（Naive Bayes）等传统的机器学习方法构建模型。此外，我们还使用了深度学习（Deep Learning）中的神经网络模型进行手写签名识别的任务。

1.2 相关工作

超声波信号是发声体所产生的能量在介质中的传播形式，在日常生活中普遍存在，属于机械波。近年来，随着计算机技术的不断进步和智能设备的普及，人机交互和普适计算等领域兴起，越来越多的研究者致力于声波感知研究。

目前，已有一些利用 rf 信号[1]、WiFi 信号[2]、声学信号[3]和智能手机上的传感器[4]进行呼吸监测的研究。这些研究揭示了通过声学信号来获取传统信息的想法是具有广阔前景的。

由于声学信号不需要特殊硬件就可以轻松获取，而且传输速度相对较慢，因此被用来跟踪细粒度的运动[5]，这也给我们通过手机检测超声波来进行手写签名识别所需数据的收集相关的想法。因此，本文主要通过上述思想，进行了手写签名超声波的提取，以识别不同身份的签名。

我们的创新点如下：

a. 提出了一种活动窗口的信号检测算法，能够更好的进行数据的提取与识别；

b. 我们同时考虑了收集到信号的时域与频域特征，使用一种时频域方法完成对字典中的离散的信号点的特征提取；

c. 使用了深度学习算法进行了手写签名识别模型的构建；

d. 在数据集的处理上提出了多种方法以适用于不同的信号处理算法；

e. 使用小波变换进行信号处理。

二、研究内容

2.1 研究方案

2.1.1 设计细节

A. **数据提取**

使用手机录音软件 AsthmaSensing-2 录下所有小组成员写下同一串字符的动作，每人写下 20 遍且每次之间间隔一小段时间，得到超声波数据并对其进行低通滤波和创新的信号检测算法，得到离散的信号点，再对信号点进行分割处理，甄别出每次写作时的信号点集合，同时截去中间停顿时产生的无效信号点，最终得到每个成员多次在滤去无效信号后的多次完整手写签名动作，在 python 中存储到字典中。

提取到的原始信号举例如下：

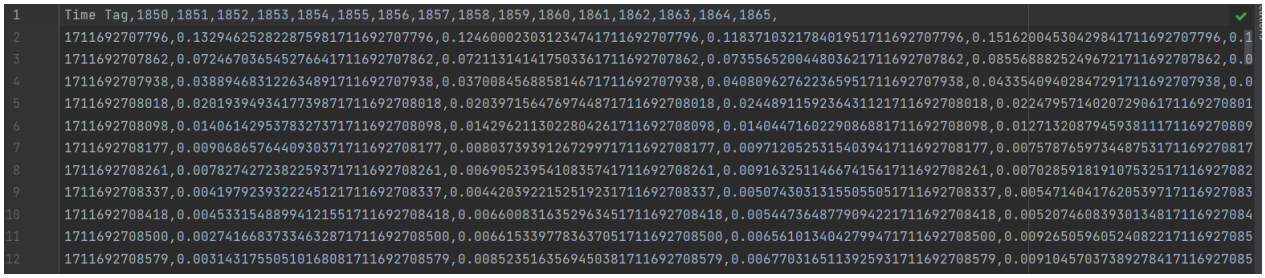

图 1 原始信号文件（部分）

B. 特征提取

对与完整的手写签名动作，使用时频域方法完成对字典中的离散的信号点的特征提取，并将得到的低频部分（近似系数）和高频部分（细节系数）进行归一化处理后相加，得到后的数据再进行归一化后保存到 txt 文件。

首先，我们通过离散小波变换（DWT）的方法将信号分解成不同频率成分，并得到逼近系数（approximation coefficients）和细节系数（detail coefficients），其中，cA 包含了输入信号的低频部分信息，也就是信号的大体趋势或整体的结构信息；cD 则包含了输入信号的高频部分信息，代表了信号中的细节或者说局部的变化信息。

在归一化操作中，我们将收集到的数据按照一定规则映射到[0,100]范围内，并对每组数据中元素不一样的情况使用均值来填充 NaN 值并进行数据集的扩充。

C. 分类模型

将每个小组成员的 txt 文件读取后保存到字典中，并使用数据增强函数来增加原始特征数据的样本数量来提高机器学习模型的泛化能力。然后将每个人的特征数据构建成一个 DataFrame，添加一个'Person'列，用于标识出数据属于哪一个成员，接着合并所有人的 DataFrame，然后从合并后的的 DataFrame 提取去除'Person'列的所有列即特征数据作为 x 和’Person’列作为目标标签 y。接着用均值填充特征数据中的缺失值，并划分训练集占比 80%，测试集占比 20%后，使用支持向量机（Support Vector Machine，SVM）、随机森林（Random Forest）和贝叶斯（Naive Bayes）等传统的机器学习方法来进行训练和预测。

2.1.2 相关算法

2.1.2.1 基本算法

A. 支持向量机算法

支持向量机（SVM），这是一种基于间隔最大化的监督学习算法。我们使用线性核函数 kernel='linear'初始化 SVM 模型，并利用训练数据 X_train 和 y_train 进行模型训练。模型训练完成后，我们对测试集 X_test 进行预测，并计算了预测结果 svm_y_pred 与真实标签 y_test 之间的准确率 svm_accuracy。此外，我们还生成了一个分类报告 svm_report，以评估模型在各个类别上的性能。

SVM 算法的基本思想是将数据映射到高维空间中，并在该空间中找到一个超平面，使得各类数据点到该超平面的距离最大。具体来说，对于给定的训练数据集，SVM 会通过计算每个样本点与超平面之间的距离，进而确定最佳的决策

边界。为了避免过拟合和提高泛化性能，SVM 还引入了核函数，可以将线性不可分的数据映射到高维空间，从而实现非线性分类。

该过程如图 2 所示。

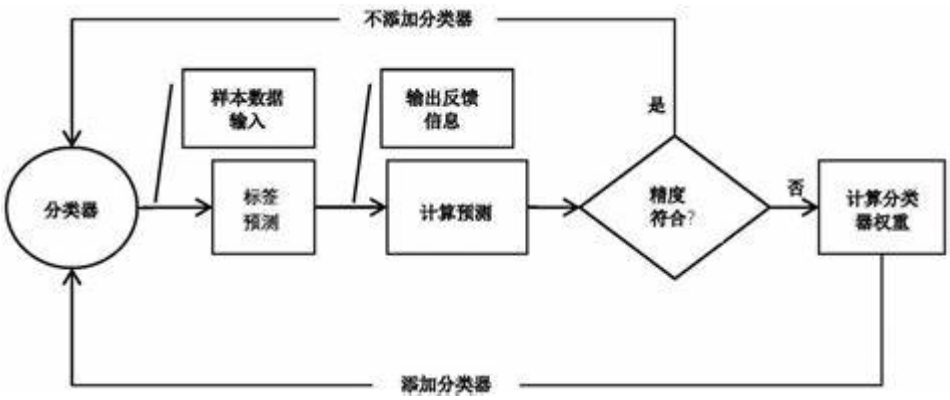

图 2 支持向量机流程图

B. 随机森林算法

随机森林（Random Forest）是一种集成学习算法，通过构建多个决策树进行训练，然后对多个决策树的结果进行集成来提高模型的性能。

我们使用随机森林分类器 rf_model 初始化模型，并利用训练数据 X_train 和 y_train 进行模型训练。模型训练完成后，我们对测试集 X_test 进行预测，并计算了预测结果 rf_y_pred 与真实标签 y_test 之间的准确率 rf_accuracy。

该过程如图 3 所示：

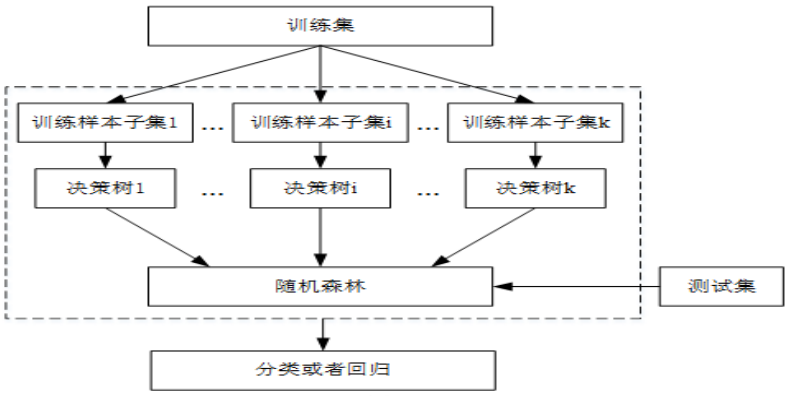

图 3 随机森林算法流程图

C. 朴素贝叶斯算法

贝叶斯（Naive Bayes）是一种基于贝叶斯定理和特征之间条件独立性假设的监督学习算法。我们使用高斯朴素贝叶斯（Gaussian Naive Bayes）初始化贝叶斯模型 nb_model，并利用训练数据 X_train 和 y_train 进行模型训练。模型训练完成后，我们对测试集 X_test 进行预测，并计算了预测结果 nb_y_pred 与真实标签 y_test 之间的准确率 nb_accuracy。此外，我们还生成了一个分类报告 nb_report，以评估模型在各个类别上的性能。

该过程如图 4 所示：

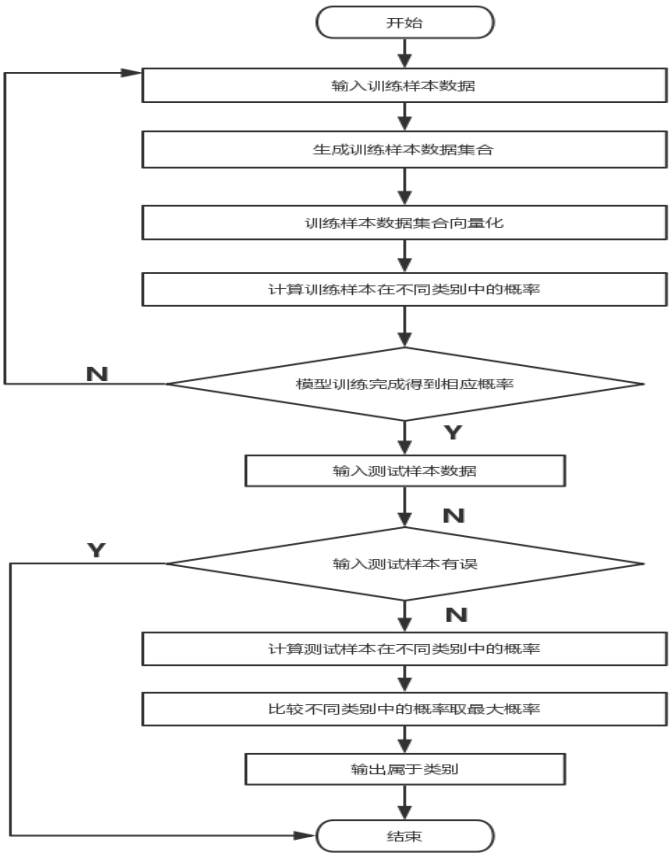

图 4 朴素贝叶斯算法流程图

2.1.2.2 创新算法

A. 滑动窗口信号检测算法

为了从噪声背景中准确地检测出有意义的信号变化我们设计了一种高效且直观的滑动窗口信号检测算法来识别时间序列数据中的关键变化点。

这个算法的核心思想以下原则：在连续的数据流中，显著的事件或行为通常会导致数据的急剧变化，通过在数据上滑动一个固定大小的窗口，并计算窗口内数据的变化幅度，可以定量地评估这些变化。当这个变化幅度超过某个预定的阈值时，就可以认为在该窗口的中心位置的点位是有效的观测点，从而将其标记为检测点。

通过选择窗口大小和阈值，我们的算法可以适应不同的信号特性，并有效地减少误检率，确保检测结果的可靠性，从复杂的数据中准确地识别出关键的信息，以便于后续特征提取与算法模型的训练。

具体的，该算法流程与伪代码如下：

Algorithm 1 Sliding Window Detection Algorithm

Require: Signal, Window Size, Threshold

Ensure: Detections

for i from $half\_window$ to $length(signal) - half\_window$ **do**
  $window\_start \leftarrow i - half\_window$
  $window\_end \leftarrow i + half\_window$
  $window\_diff \leftarrow \max(signal[window\_start : window\_end]) - \min(signal[window\_start : window\_end])$
  if $window\_diff > threshold$ **then**
    Add i to $detections$ {Mark as point of action start}
  end if
end for

B. 离散信号处理算法

为了方便从信号检测算法处理后得到的离散数据中得到完整签名动作并进行特征提取，我们设计了两个部分对信号进行处理。

离散信号处理算法包含两个部分：首先将刚开始采集数据和即将完成数据时的检测点截断（这两个阶段易受干扰），接着将一定范围内连续的检测点截取出来一个片段作为一次签名过程；然后将处理后的离散信号进行时频域分析处理，将信号执行离散小波变换拆解为低频部分和高频部分，并对两个参数进行相关处理提取出特征数据。

通过修改两个参数在合成后的数据中的占比来减少误判率以提高准确性，确保能从离散信号中提取出关键的分析数据，以便于后续的算法模型训练。

具体的，算法流程的伪代码如下：

Algorithm 2: Discrete-signal-processing

Requre: Detections，Start-detection, Max-val, Min-val

Ensure: Detection-lists

```
for i frpm Detecitons do
    if i>start-detection then
        add i to p-range
    end
    if p-range'size > 1 then
        add i to Detection-lists and clear p-range
    end
end
for p-range from Detection-lists do
    'db1'Discrete wavelet transform and Normalize to 1 to 100
end
for p-range from Deteciton-lists do
    for i in p-range do
        i ← i+100
    end
    Normalize to 1 to 100
end
```

C. 深度学习算法

我们基于 TensorFlow 框架实现了多层感知机（MLP）和一个基本的全连接前馈神经网络，通过从输入数据中自动学习特征来解决分类问题，进行手写签名的识别。其过程分为数据预处理、模型构建、训练和评估，通过深度学习模型能够捕捉到手写签名中的复杂模式，从而实现对不同人签名的分类。

我们首先通过从文本文件中加载特征数据来开始数据预处理过程，其中包含了每个人的签名动作产生的数据集合。为了提升模型的泛化能力，我们采用了数据增强技术，即通过在原始特征值上添加小的随机扰动来生成更多训练样本。接着，我们将特征数据（X）和目标标签（y）进行分割，并对标签进行编码，以适应模型训练的需求。最后，我们将数据集划分为训练集和测试集，旨在通过这种方式对模型进行训练和评估。

模型的构建是围绕着一个由三层全连接层组成的网络结构展开的，其中前两层采用 ReLU 激活函数，而最后一层则使用 Softmax 激活函数来执行多类分类。在编译模型时，我们选用了 Adam 优化器和稀疏分类交叉熵损失函数，目标是最小化训练过程中的损失。

训练阶段，模型在训练集上进行训练，同时在验证集上进行验证，这一步骤有助于监控并防止过拟合的发生。完成训练后，我们利用测试集对模型进行了评估，不仅计算了准确率，还细致地分析了其他关键的分类性能指标，如精确度和召回率等，以全面评价模型的性能。

本算法完整流程以伪代码形式给出，如下：

Algorithm3: Deep Neural Network

---

1. **Data Preprocessing**
   - (a) Load features from files.
   - (b) Enhance data to increase sample variability.
   - (c) Split data into features (X) and labels (y).
   - (d) Encode labels for classification.
   - (e) Divide dataset into training and testing sets.
2. **Model Construction**
   - (a) Initialize Sequential model with input layer.
   - (b) Add Dense layers with ReLU activation (except last layer with Softmax).
3. **Model Compilation**
   - (a) Compile using Adam optimizer and sparse categorical crossentropy loss.
4. **Training and Evaluation**
   - (a) Train model on training set with validation split.
   - (b) Evaluate model accuracy on test set.
5. **Results Visualization** (Optional)
   - (a) Plot training and validation loss curves.

2.2 实验结论

2.2.1 数据与性能分析

A. 数据分析

我们将每个模型的识别效果分别平行运行了 5 次，对比了不同算法对手写模型识别的准确率等指标，得出每一次不同结果的性能分析如下图：

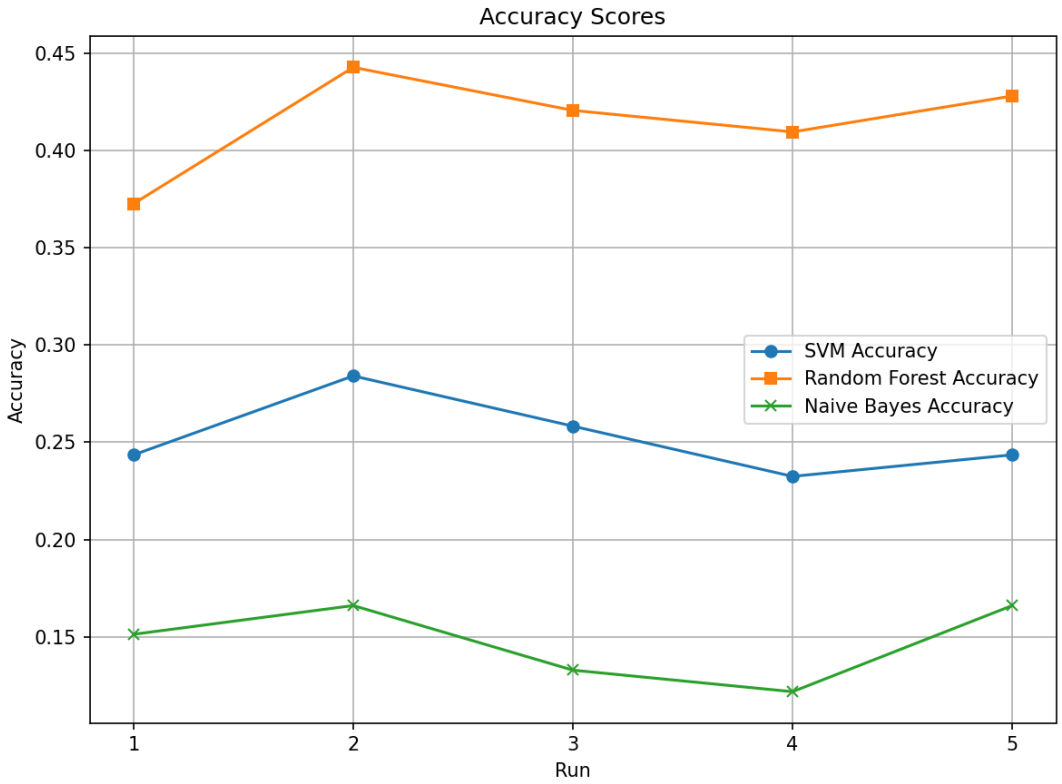

图 5 三种算法的准确率对比图

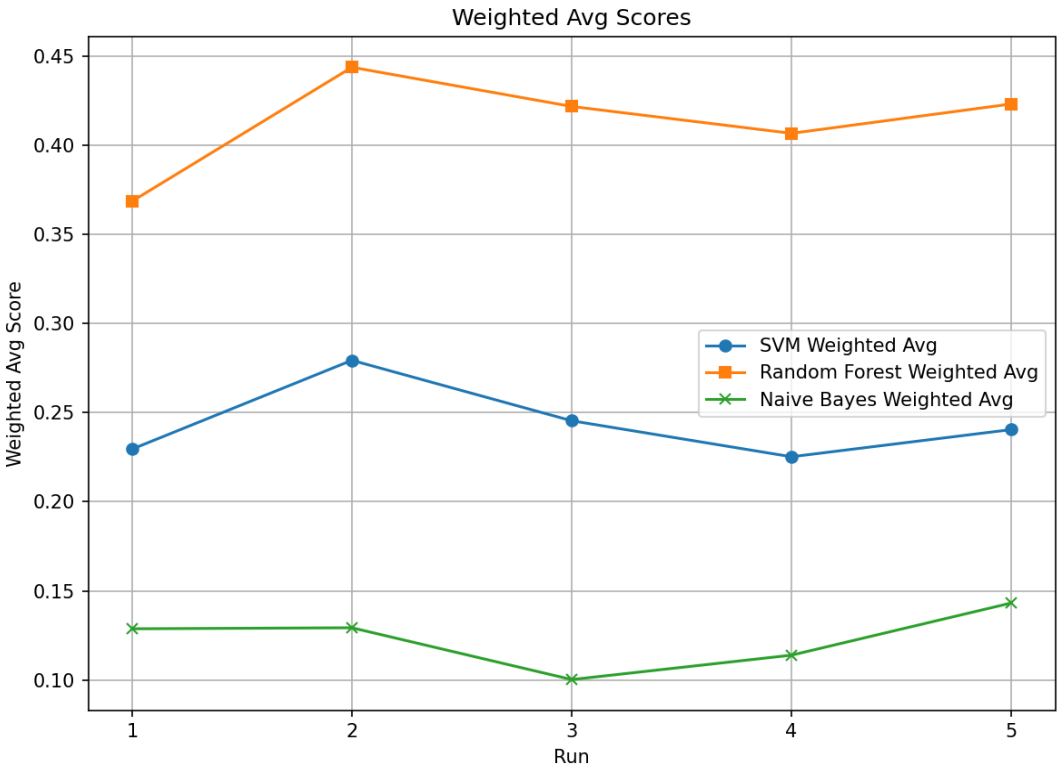

图 6 三种算法的加权均值对比图

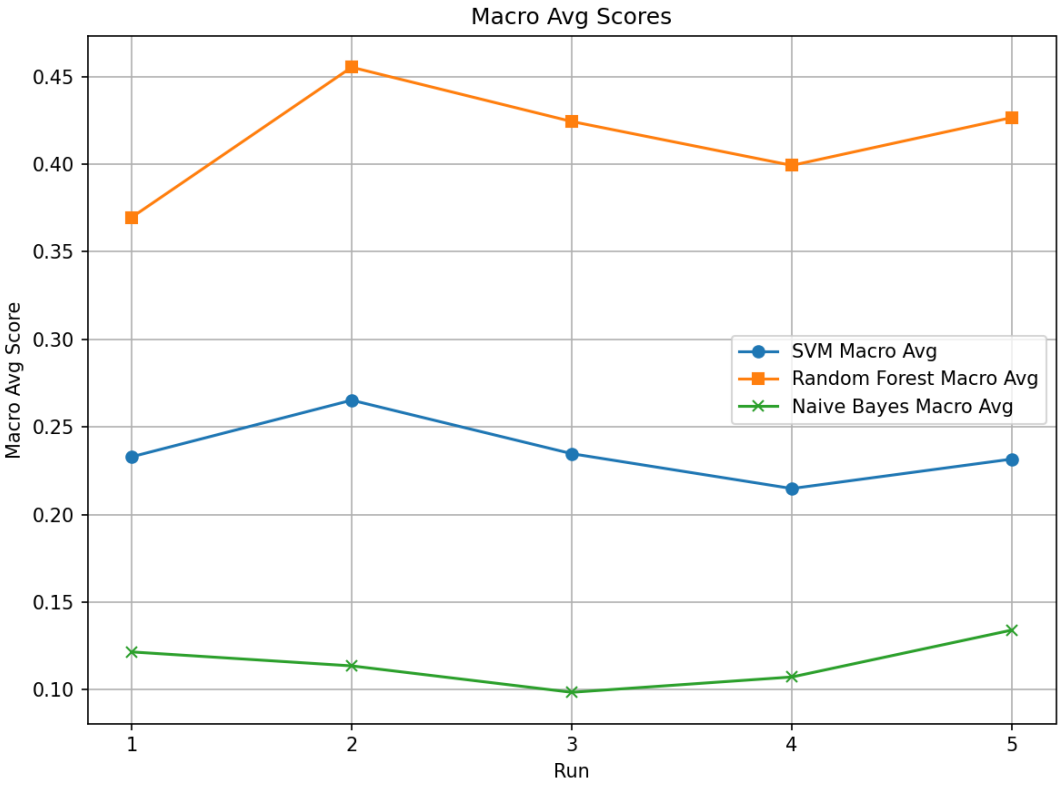

图 7 三种算法的宏均值对比图

此外，在深度学习的性能上，除了上述指标，我们还对整个过程的准确率等指标和 loss 值的变化进行了观测，结果如下图：

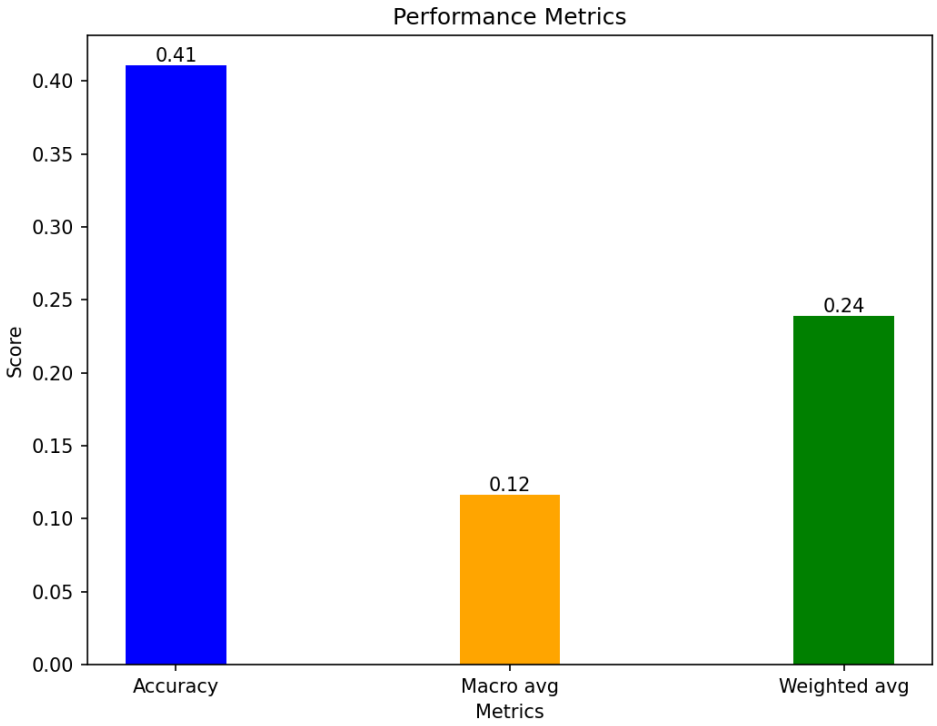

图 8 深度学习的三种指标

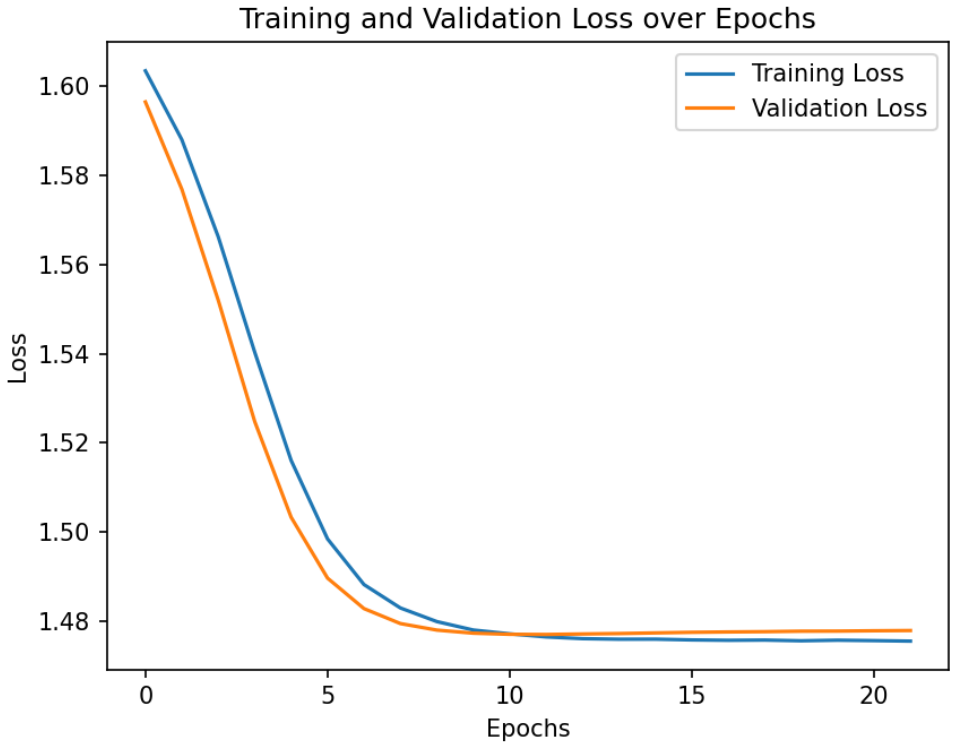

图 9 深度学习下的 loss 变化图

结果表明，在手写速度适中，距离较近的情况下，我们的手写签名识别模

型具有一定准确性和优良的性能。

对上述性能对比图进行分析，我们发现使用 SVM 模型的识别准确率是最高的，其次，在相同参数下，几种模型的识别准确率呈现出了较大的变化，原因是我们并未对每一种模型做出更加特异性的数据处理，所有的数据处理方式是相同的，这也导致不能很好地兼顾各种模型；此外，我们在数据采集、特征提取等过程中的参数调整还有很大的进步空间，预计如果可以调整到最优的参数组合，识别准确率或将达到 90%或更高，而这也是我们需要继续研究的地方。

B. 书写速度、远近的影响

为了对比不同书写速度和远近对识别准确率和相关性能的影响，我们将 A 部分的结果表示为 100%，在书写速度越来越快、距离越来越远的情况下，分别计算上述指标，得到了在不同条件下的性能结果如下图：

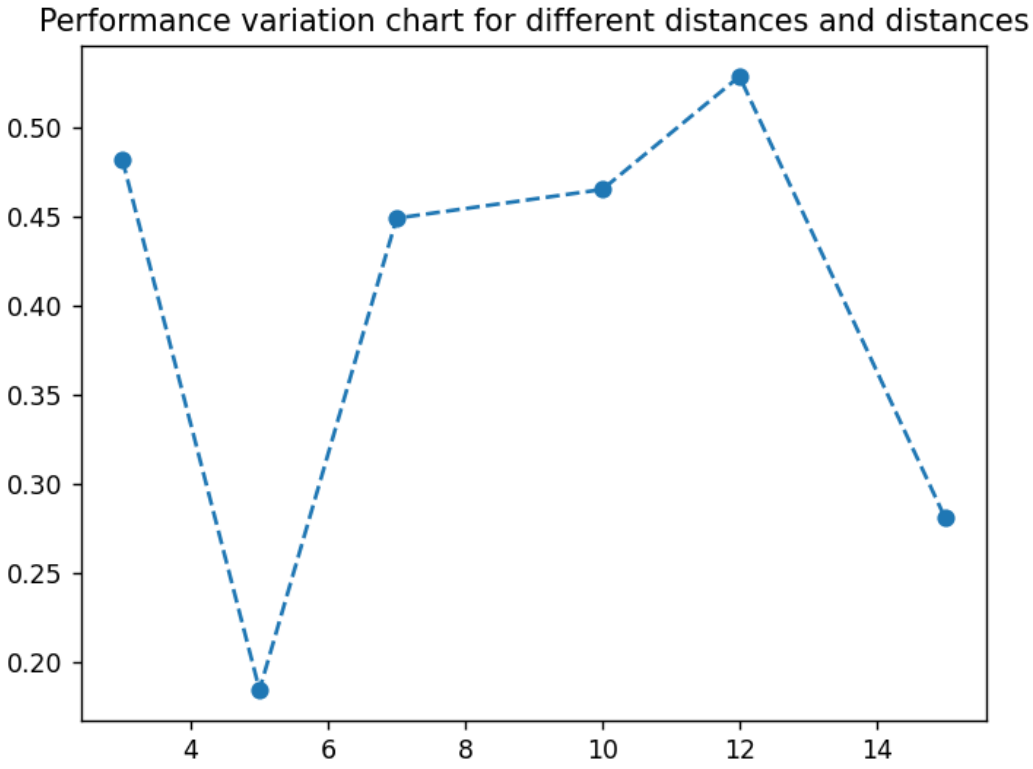

图 9 不同远近条件性能指标变化图

结果表明，在书写速度过快和距离过远时，识别的准确率出现下降，相关性能也同时出现了不同幅度的降低，这是因为书写太快或者距离过远将导致收音不清，以及后续处理上特征提取不到位，进而影响后续结果。

此外，我们还测试了在不同人数时的识别准确率，结果显示，在其余参数相同时，人数为 5 时的识别准确率相比于 4 个人的准确率下降了近一半，这说明我们的模型在参数设置上还有很大的调整余地和进步空间，这也是我们今后需要改进的地方。

2.2.2 结论

基于手机超声波信号，我们通过信号检测、特征提取和机器学习完整构建了手写签名窃听模型，对模型性能进行了全局性评价和鲁棒性评价，并给出了相关性能对比图，结果表明，该模型对手写签名的窃听识别具有一定效果。

对于实验中数据结果不理想的问题，我们分析原因如下：

a.进行原始数据处理时，滤波相关参数选择不理想，导致监测点选取不理想；

b.对于一些特殊的离散点（如极端数值）使用的处理方式在一定程度上可以减轻其影响，但不能完全消除；

c.由于硬件录音设备的局限性和周边环境的影响，导致收集到的音频白噪声在一定程度上很大的影响了后续的数据处理工作；

d.在进行深度学习与其他算法的模型训练时，有关超参数的选取不恰当；

e.时间局限性导致我们无法更精准的对比不同参数组合导致的性能差异。

针对以上不足，我们将会在后续进行修正，尽量使模型达到更理想的效果。

综上，我们完成了基本工作，并在此基础上进行了相应创新工作，对结果进行了分析，并提出了后续改进的地方。

三、成员分工及个人课程目标达成情况

成员分工情况如下：

负责部分
项目整体协调，分类模型与 Ml、DL 相关算法实现，部分数据提取,文档撰写
信号时频域特征提取，部分数据与性能分析，文档撰写
部分数据处理、部分模型性能分析、文档撰写
部分数据处理，文档撰写
初期规划，采集数据，提出建议

参考文献：

[1]Neal Patwari, Lara Brewer, et al. 2014. Breathfinding: A wireless network that monitors and locates breathing in a home. IEEE Journal of Selected Topics in Signal Processing 8,1 (2014), 30–42.

[2]Fadel Adib, Hongzi Mao, et al. 2015. Smart homes that monitor breathing and heart rate.In Proc. ACM CHI'15, Seoul, Korea.
[3]Rajalakshmi Nandakumar, Shyamnath Gollakota, and Jacob E Sunshine. 2019. Opioid overdose detection using smartphones. Science translational medicine 11, 474 (2019),eaau8914.
[4]Heba Aly and Moustafa Youssef. 2016. Zephyr: Ubiquitous accurate multi-sensor fusionbased respiratory rate estimation using smartphones. In Proc. IEEE INFO-COM'16,San Francisco, CA, USA.
[5]Sangki Yun et al. 2017. Strata: Fine-Grained Acoustic-based Device-Free Tracking. InProc. ACM Mobisys'17, Niagara Falls, USA.