RFaceID: Towards RFID-based Facial Recognition

CHENGWEN LUO, Shenzhen University, China
ZHONGRU YANG, Shenzhen University, China
XINGYU FENG, Shenzhen University, China
JIN ZHANG, Shenzhen University, China
HONG JIA, University of New South Wales, Australia
JIANQIANG LI, Shenzhen University, China
JIAWEI WU, Shenzhen University, China
WEN HU, University of New South Wales, Australia

摘要

如今，人脸识别已被广泛地应用于许多领域。然而，现有的基于视觉的主流面部识别有其局限性，如容易受到攻击，对光照条件敏感，以及隐私泄露的高风险等。为了解决这些问题，论文作者采取了一种完全不同的方法，并提出了 RFaceID，一种新颖的基于 RFID 的人脸识别系统。RFaceID 只需要用户在 RFID 标签矩阵前晃动他们的脸几秒钟就可以得到他们的脸。论文详细介绍了所做工作，包括理论分析和实验验证，研究了基于 RFID 的人脸识别的可行性；提出了多种数据处理和数据增强技术以尽量减少环境噪音和用户动态的负面影响；设计了一个深度神经网络 (DNN) 模型，用于脸部晃动事件的空间和时间特征；最后实施了该系统，并进行了广泛的评估，结果显示，RFaceID 对 100 个用户实现了 93.1% 的高人脸识别准确率。而本次课题的主要工作是，对该论文进行研究和学习，并在已经获得数据集和部分源码的情况下进行个人创新。

关键词： RFID；人脸识别；数据强化；神经网络

1 引言

近年来，由于在公共安全、数字支付、设备解锁等领域的广泛应用，人脸识别已经成为文献中研究最多的课题之一。在常见的人脸识别场景中，图像和视频的获取需要使用摄像头进行视觉输入，而使用摄像头进行人脸识别有一些局限性。例如，普通的摄像头（如电脑和智能设备上的摄像头）没有配备红外灯用于夜视仪，导致在恶劣的照明条件下识别精度较低。此外，使用摄像头进行视觉输入增加了泄露隐私的风险，使得在一些特殊场合可能无法使用。最近，研究人员还发现，这种基于视觉的人脸识别系统使攻击者很容易获得用户的脸部信息，并提取相关信息进行攻击（包括 2D、3D）。

而本课题将要复现的论文中则采取了一种截然不同的方法，使用 RFID 信号进行人脸识别。这种系统有几个优点。首先，保护隐私，由于人脸识别不需要采集图像或视频，这样的系统极大地降低了隐私泄露的风险。第二，对不同的光照条件具有鲁棒性，无线信号不受照明条件变化的影响，系统应在完全黑暗的环境中工作。第三，更可靠地抵御攻击，最近的研究表明，射频信号在传播过程中对它们所反射的材料很敏感，这使得基于无线技术的人脸识别系统对伪装攻击更加可靠，即使攻击者能生产和使用 3D 打印的面具。因此，基于 RFID 的人脸识别技术有可能成为目前流行的基于视觉的人脸识别技术的一个重要补充。

2 相关工作

2.1 使用射频信号进行人类活动感知

传感技术在人的活动识别方面，有许多引人注目的应用，如智能家用电器的人机互动、老年人护理、福利管理和安全监控。为了促进这些应用，已经开展了积极的研究来检查人类活动。通过不同角度的传感，包括在室内环境中准确地指出目标人物的位置，识别该人的常规活动或特定的身体姿态，以及监测他或她的生命体征 (例如，呼吸频率)。

为了有效地进行人类活动识别，各种传感技术，包括运动传感器、基于视觉的传感器、基于声音的传感器和热释电红外传感器，被用来检测不同的人类活动和手势。基于运动传感器的方法通当需要个人佩戴号门的设备来跟踪身体话动，这在实践中并不总是很方便。依靠摄像头或可见光传感器的方法只能在特定的光线条件下工作，这很容易被低照度条件、烟雾或不透明的障碍物所干扰。此外，基于声音的方法的稳定性容易受到环境噪音和周围声音的干扰，而且由于声音信号的快速衰减，感应范围也受到限制。总的来说，上迹技术在复杂的硬件安装和多样化的维护需求方面涉及额外的开销。为了克服上述限制，我们需要一个低成本和非侵入性的解决方案来捕捉人类日常活动中的身体动作。最近，越来越多的研究工作集中在基于射频的技术来执行人类活动感应。人的存在和相关的身体运动将对无线信号产生相当大的影响，并导致接收信号的振幅和相位的显善恋化，这可以用来捕捉人类日常活动中的身体运动。[1]

2.2 RFID 的穿墙跟踪

RFID 正在发展成为识别和跟踪世界各地物体的主要技术推动者。这种广泛部署的原因是标签的简单性，它可以在大批量中实现非常低的损耗。RFID 系统的好处之一是，由于多路径效应，它可以在非视线性的情况下识别物体。最近，穿墙跟踪在民用领域获得了很多关注。许多应用将受益于这种无设备的追踪，例如老人监视、入侵者防护、游戏等。在[2]的工作中，提出了一个名为 Tadar 的采统，用于跟踪移动的物体，而无需使用 COTSRFID 阅读器和标签。它甚至可以穿墙和在封闭的门后工作。它的目的是实现一种低成本、紧凑、可用于民用目的的透视墙技术。

3 本文方法

3.1 系统概述

如图 1所示，该系统主要由两个阶段组成：离线模型训练阶段和在线人脸识别阶段。主要工作也集中在离线模型训练阶段，在这个阶段，会收集所有用户的脸部摇晃数据，并将所有这些收集到的人脸数据依次进行数据分割、数据强化、数据预处理和模型训练。

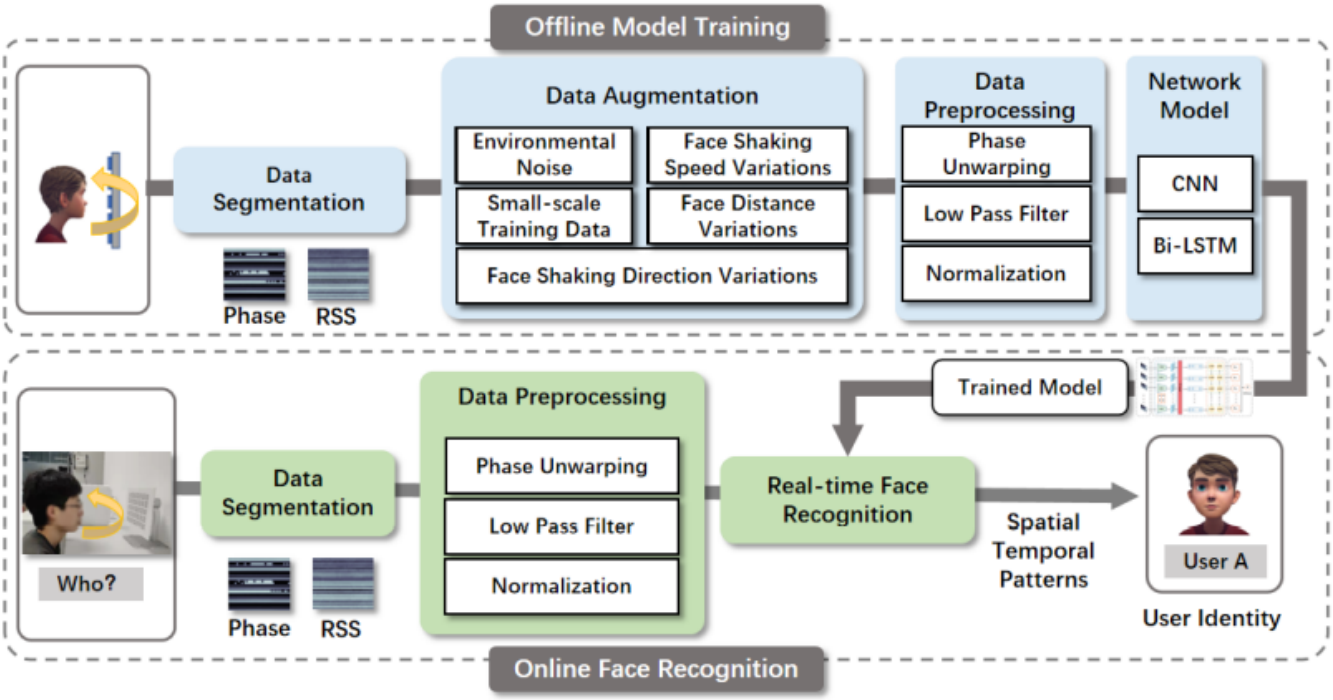

图 1: 系统概述

3.2 数据强化

在进行人脸识别时，人脸的特征可能会受到多种因素影响，如环境的变化和用户的动作。环境的变化包括背景物体产生的噪声。用户的动作包括了脸晃动的速度、脸摇晃的方向、脸部距离标签矩阵的距离等方面的变化。此外，还可能存在数据规模太小和过拟合的问题，因此提出了几种数据增强技术来解决以上问题。

3.3 数据预处理

在将数据用于训练建模之前，还需要对数据进行预处理。由于相位值的范围是 0∼2π, 一些标签的相位值会在 0∼2π 产生较大波动，即产生相位漂移问题，这将会对人脸识别的准确性带来负面影响，因此，文中使用 Unwarp 算法来纠正相位漂移问题。此外，为了减少环境噪声对相位和 RSS 的负面影响，文中使用了一个低通滤波器来平滑相位和 RSS 的数值。最后，相位和 RSS 值都被用于模型训练，但相位和 RSS 读数的数量级是不同的。为了避免模型训练过程中的来回震荡和不收敛，并提高模型的收敛速度，在数据预处理过程中还进行了特征归一化。

3.4 模型训练

该系统使用 DNN 模型来捕捉相位和 RSS 的空间和时间特征，如图 2所示，RFaceID 的神经网络由三部分组成：输入层、隐藏层和输出层。在输入层，使用由 RFID 阅读器捕获的所有标签的相位和 RSS 作为输入数据。然后，隐藏层中的全连接层被用来提取几何空间和脸部在每个时刻的不同角度的内部材料特征。接着，通过 Bi-LSTM 网络来捕捉摇脸的时间特征。最后，在输出层，用 softmax 函数来对 Bi-LSTM 层提取的特征进行多分类以实现人脸识别。

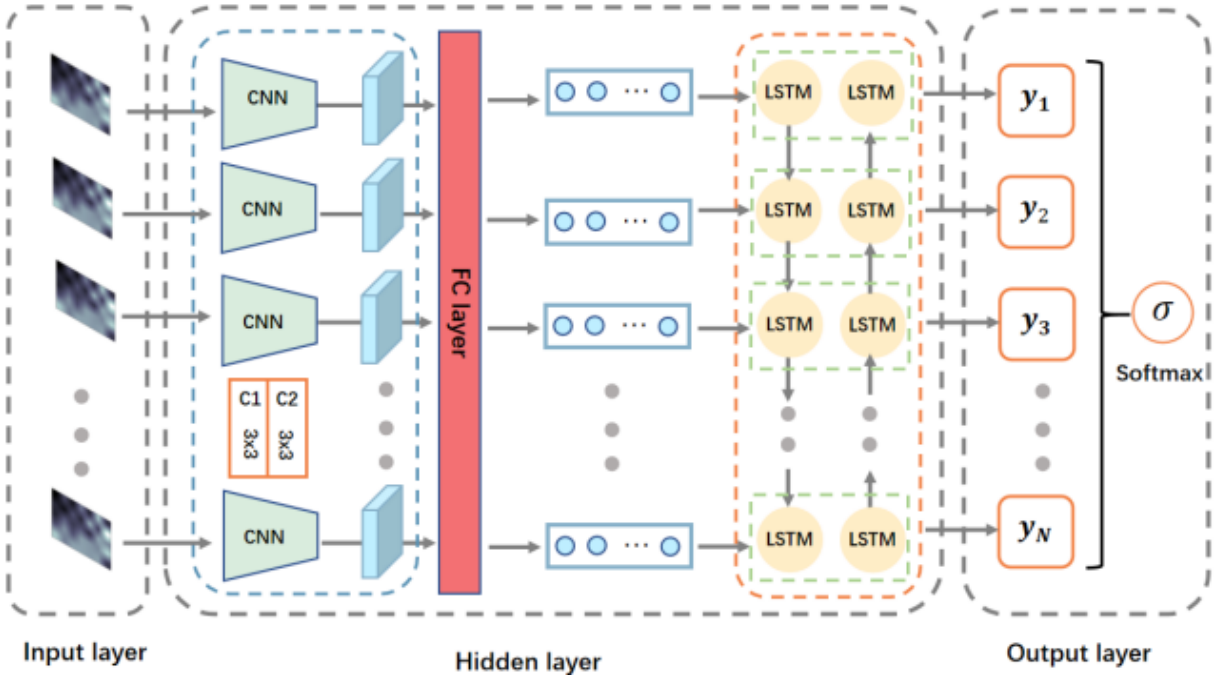

图 2: 神经网络模型

4 复现细节

这部分内容介绍的是本次课题我的个人工作情况，我实现了系统中的数据强化部分，下面是详细介绍。

4.1 环境噪声

由于背景物体产生的环境噪声影响，标签矩阵所采集到的相位和 RSS 通常是不稳定的。幸运的是，在实验中采集人脸数据时，人脸相对于标签矩阵的距离比其他的背景物体近得多，所以人脸对阅读器捕捉到的相位和 RSS 变化起着主导作用。为了补偿背景物体带来的随机噪声的干扰，需要在增强的数据集中随机加入均值为零、方差为 δ 的高斯噪声。如图 3所示，分别是相位和 RSS 加入高斯噪声前后的变化。

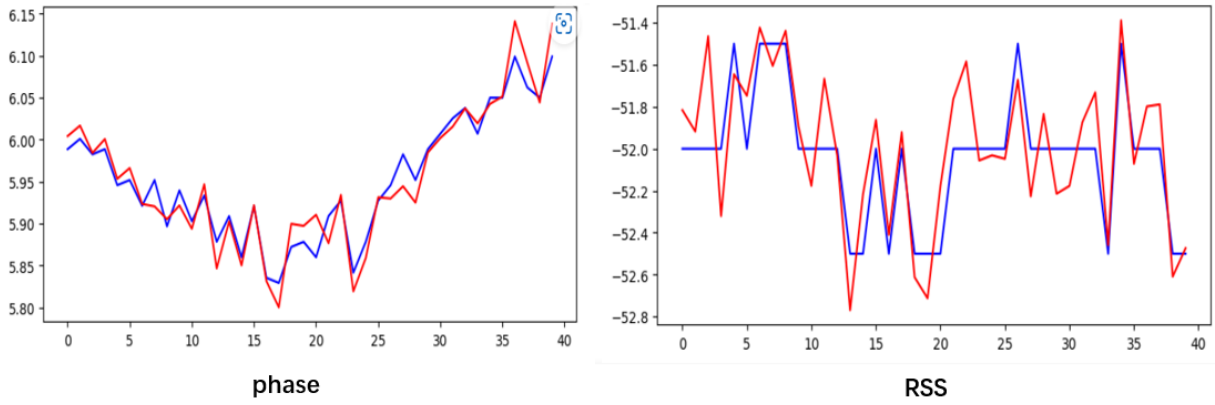

图 3: 加入高斯白噪声（蓝色为加入前，红色为加入后）

4.2 脸部晃动速度变化

当用户进行人脸识别时，即使是同一个用户，其脸部的晃动速度也会有所不同，脸部晃动速度的变化将不可避免地导致最终识别精度的下降。为了解决这个问题，我们在数据增强中引入了随机拉伸和压缩的相位和 RSS 序列。以模拟不同的人脸晃动的速度的影响。具体操作是对相位和 RSS 序列进行在（-30%,30%) 范围内的时间序列上的随机压缩和拉伸，分别对应慢速的人脸晃动和快速的人脸晃

动。如图 4所示，分别是相位和 RSS 序列经过拉伸和压缩前后的变化。

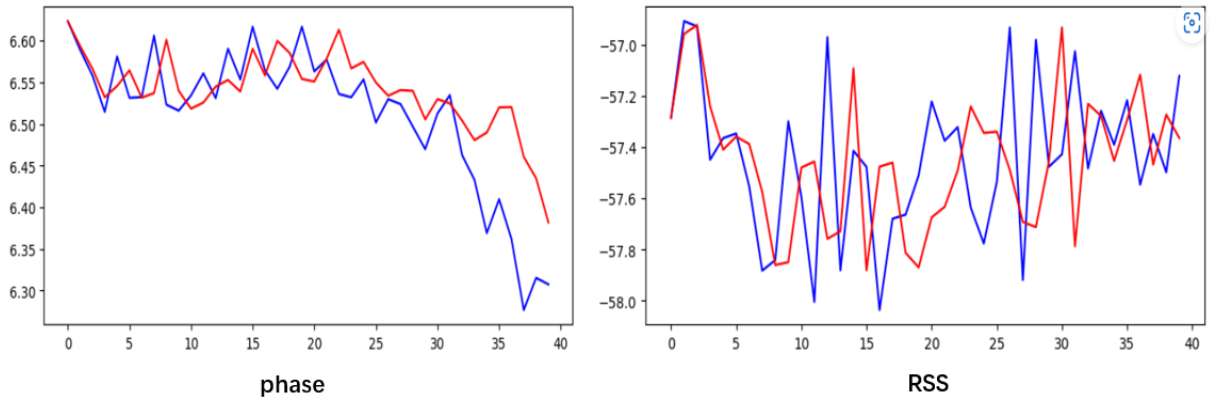

图 4: 在时间序列上进行随机拉伸和压缩（蓝色为处理前，红色为处理后）

4.3 脸部晃动方向变化

当同一个用户进行人脸识别时，人脸的方向摇晃的方向（例如，从左到右，和从右到左）也可能是不同的。这将导致不同的相位和 RSS 模式并影响最终的识别性能。幸运的是，相反的脸部晃动方向会导致相反的相位和 RSS 的变化模式。因此，我们在训练集中随机抽取 20% 进行翻转，以补偿脸部不同的晃动方向变化。如图 5所示，分别是相位和 RSS 序列经过随机翻转前后的变化。

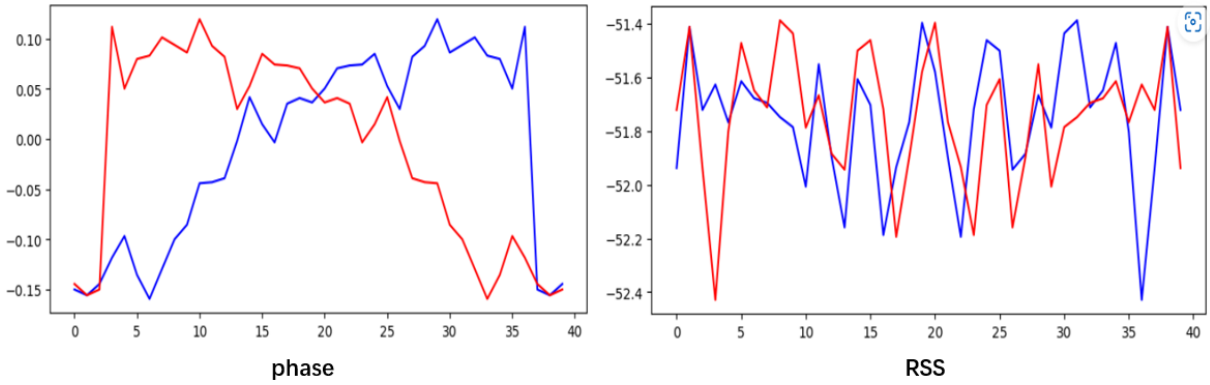

图 5: 对数据进行随机翻转（蓝色为处理前，红色为处理后）

4.4 脸部相对标签矩阵距离变化

当同一个用户进行人脸识别时，人脸距离标签矩阵的不同将直接影响到阅读器捕捉到的相位和 RSS 序列。根据公式，相位值与距离成正比，而 RSS 值与距离成反比。因此在数据强化中，我们对所有相位和 RSS 序列随机进行在 (-20%,20%) 范围内的放大或缩小。如图 6所示，分别是相位和 RSS 序列经过随机放大或缩小前后的变化。

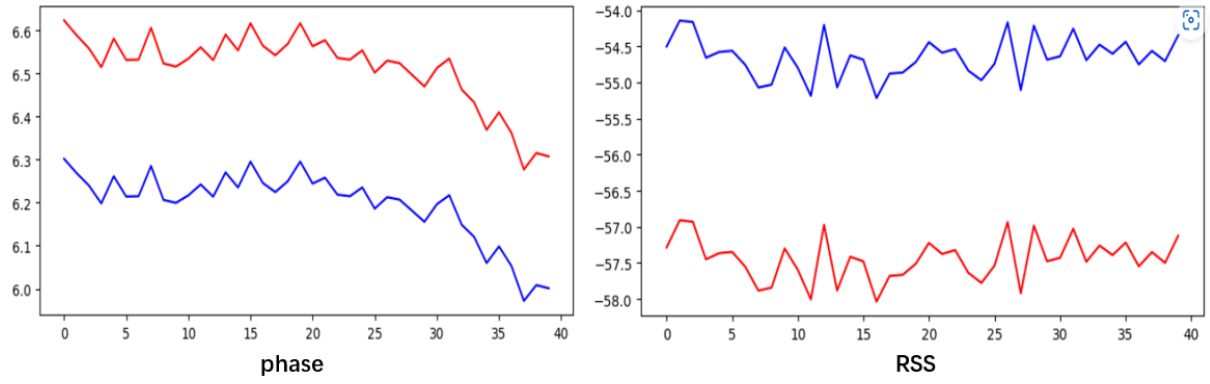

图 6: 对序列进行随机放大或缩小（蓝色为处理前，红色为处理后）

4.5 实验环境搭建与使用说明

本次课题所采用的实验环境为：win10 操作系统下，tensorflow 环境下的 jupyter notebook，加上一些常见的数据处理包。如图 7是程序界面的展示，只要点击运行即可。

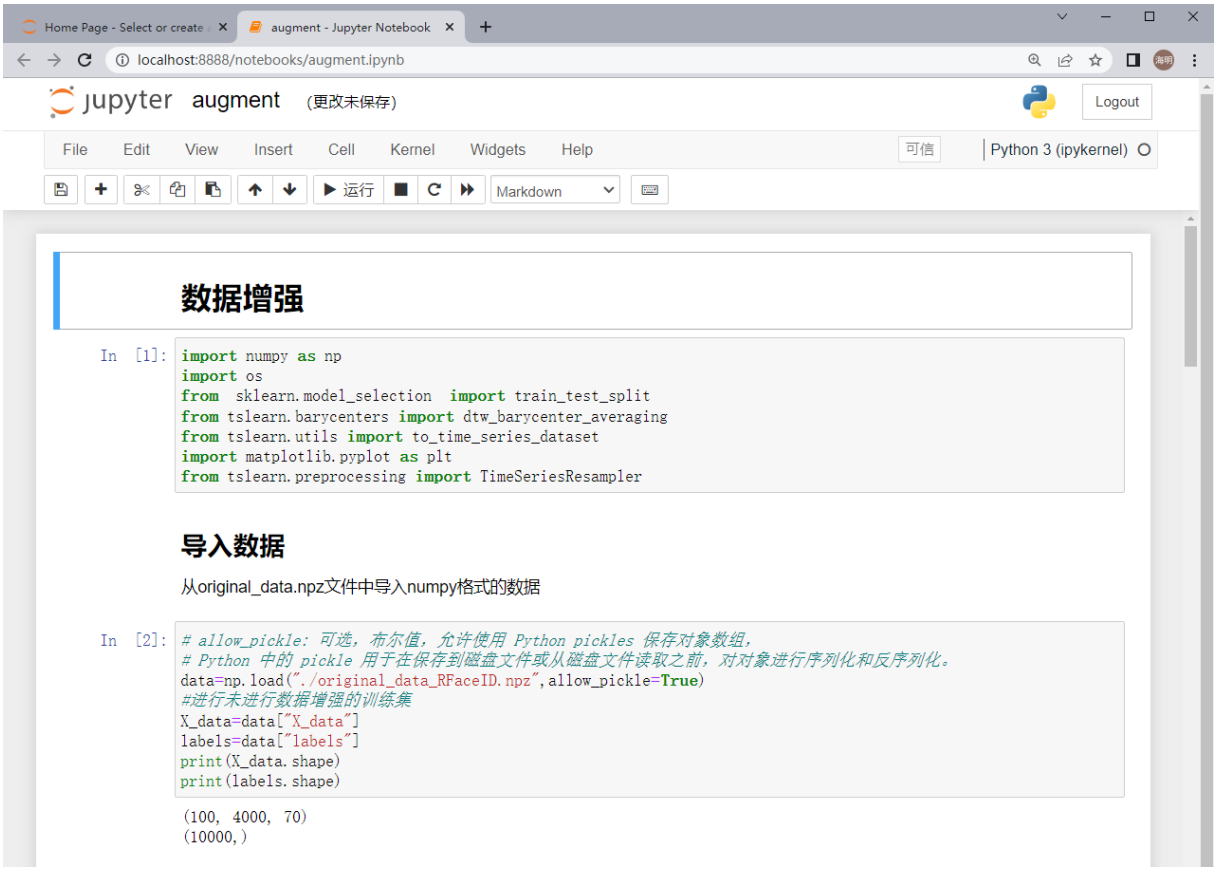

图 7: 操作界面示意

5 实验结果分析

首先展示实验结果，如图 8所示。其中左边的结果是使用未经过数据强化的训练集和测试集，进行模型训练后测试产生的准确率。右边的结果是使用经过数据强化的训练集和测试集，进行模型训练后产生的准确率。可以看到两个准确率相差无几。我认为数据强化的工作是否具有提高人脸识别精确度的意义仍需要大量实验进行证明。目前存在的局限性是，我们只拥有一套在理想环境下采集的人脸数据，这一套数据既作为训练集也作为测试集。因此如果用数据强化后的数据作为训练集，而使用未经过数据强化的数据作为测试集，则会导致结果精度的急剧下降。我们需要一些在非理想环境下采集的数据，如人脸距离标签矩阵距离较远，背景物体移动产生较大噪音，脸部摇晃比较不规律等。有了这些数据，就可以用它们作为测试集，验证数据增强是否对实际人脸识别过程中的不利因素有补偿的作用。

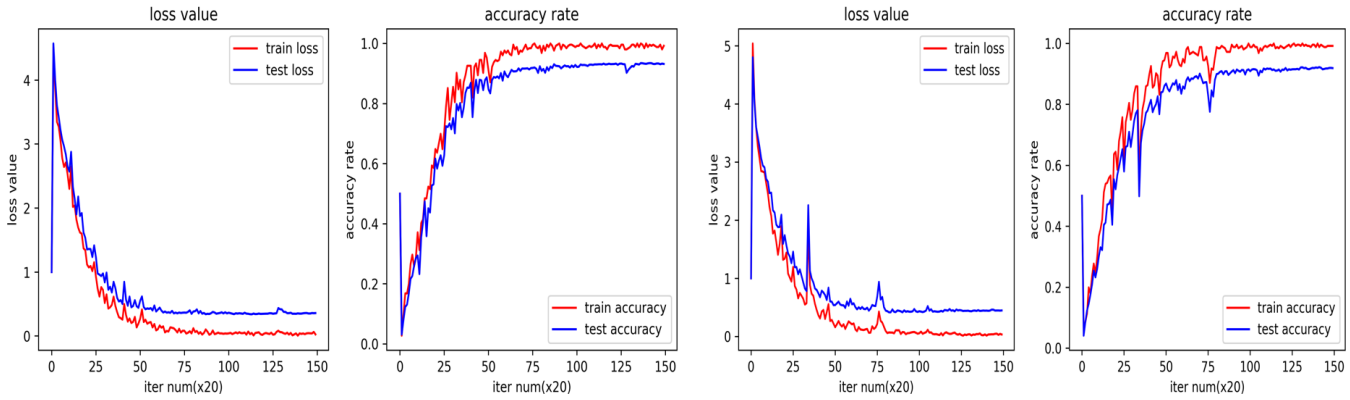

图 8: 实验结果示意

6 总结与展望

RFaceID 提出了一种新的基于 RFID 的面部识别方法。一个 RFID 阅读器、天线和一个 RFID 标签矩阵来收集用于人脸识别的 RFID 物理层信息。与使用单相机的最先进的基于视觉的方法相比较最先进的基于视觉的方法，使用一个摄像头，RFaceID 的部署是更昂贵的，并产生了额外的硬件成本。由于对硬件的额外依赖，RFaceID 也不能很容易地与目前的设备（如智能手机）集成，而且对 RFID 设备的预先部署的要求也限制了 RFaceID 的应用场景。与目前基于视觉的方法相比的方法相比，RFaceID 的人脸识别准确率较低，而且容易受到人脸外观变化的影响，比如说戴口罩。此外，胡须、小胡子等引起的自然面部变化也可能降低系统性能，需要在今后的工作中加以探索。尽管有上述限制，射频识别仍然有多种好处，如隐私保护、不依赖照明条件等，这使它成为一种新的补充方法，以加强目前现有的面部识别系统。RFaceID 可以与其他传感器集成，以进一步提高其在实践中的可用性，如 WiFi 和毫米波雷达可以可以与 RFaceID 集成，以进一步提高系统的准确性、稳健性和安全性，特别是当用户戴着帽子或口罩时。

参考文献

[1] LIU J, LIU H, CHEN Y, et al. Wireless Sensing for Human Activity: A Survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 1629-1645. DOI: 10.1109/COMST.2019.2934489.

[2] YANG L, LIN Q, LI X, et al. See Through Walls with COTS RFID System![C/OL]//MobiCom '15: Proceedings of the 21st Annual International Conference on Mobile Computing and Networking. Paris, France: Association for Computing Machinery, 2015: 487-499. https://doi.org/10.1145/2789168.2790100. DOI: 10.1145/2789168.2790100.