计算机科学
COMPUTER SCIENCE

基于深度学习的超高频标签识别系统

余加宝，姚俊梅，谢瑞桃，伍楷舜，马军超

引用本文

余加宝，姚俊梅，谢瑞桃，伍楷舜，马军超基于深度学习的超高频标签识别系统[J]．计算机科学, 2023, 50(6A): 220200151-6.

YU Jiabao, YAO Junmei, XIE Ruitao, WU Kaishun, MA Junchao. Tag Identification for UHF RFID Systems Based on Deep Learning [J]. Computer Science, 2023, 50(6A): 220200151-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.220200151

基于深度学习的超高频标签识别系统

余加宝[1]　姚俊梅[1]　谢瑞桃[1]　伍楷舜[1]　马军超[2]
1 深圳大学计算机与软件学院　广东 深圳 518000
2 深圳技术大学大数据与互联网学院　广东 深圳 518000
(1844782541@qq.com)

摘　要　无线射频识别(Radio Frequency Identification,RFID)系统最基本的功能是标签识别,然而身份验证系统无法检测到伪造或克隆标签,从而出现潜在安全隐患和个人隐私问题。目前有基于加密的认证协议和基于特征提取的解决方法,其中基于加密的认证协议方法不兼容现有的协议,基于特征提取的方法存在特征提取困难或者识别距离短等限制。文中基于标签物理层信号的真实性进行识别,结合深度学习技术,提出标签信号识别方法。其核心思想在于在RFID通信过程中,利用标签的后向散射信号提取与标签逻辑信息无关的信号,将提取的信号送入卷积神经网络进行相似度匹配,根据得到的相似度匹配分数与给定的阈值对比,最后实现标签的真实性识别。采用USRP N210作为RFID系统的阅读器,采用150个超高频商用标签作为信号的发射器,并在实际场景中采集真实的RFID信号。通过实验验证了基于深度学习的标签识别能达到94%以上的识别精度,在识别距离长达2m的情况下其等错误比率(EER)为0.034。

关键词:物理层识别;无线射频识别;深度学习;标签
中图法分类号　TP391

Tag Identification for UHF RFID Systems Based on Deep Learning

YU Jiabao[1],YAO Junmei[1],XIE Ruitao[1],WU Kaishun[1] and MA Junchao[2]
1 School of Computer and Software,Shenzhen University,Shenzhen,Guangdong 518000,China
2 School of Big Data and Internet,Shenzhen Technology University,Shenzhen,Guangdong 518000,China

Abstract　The most basic function of radio frequency identification(RFID) system is tag identification. However,the current authentication system cannot detect forged or cloned tags,which leads to potential security and privacy issues. At present,there are encryption based authentication protocols and feature extraction based solutions,among which encryption based authentication protocol is incompatible with existing protocols and feature extraction based authentication protocol has limitations such as difficulty in feature extraction or short recognition distance. This paper proposes a tag identification method for UHF RFID systems to overcome the two shortenings. The core idea is to first extract signals irrelevant to the logical information of tags from the backscattered RFID signals,and then send them to the convolutional neural network for similarity matching. According to the score of similarity matching and a given threshold,the authenticity of the tag is finally recognized. In this paper,we establish an experimental system which contains an USRP N210 used as the reader of the RFID system,and contains 150 UHF commercial tags to backscatter signals from the reader. We then collects the RFID signals based on this experiment. Experimental results show that the tag recognition accuracy based on deep learning can reach more than 94%,and its equal error ratio(EER) is 0.034 when the recognition distance is up to 2m.

Keywords　Physical-layer identification,Radio frequency identification,Deep learning,Tag

1　引言

万物互联概念的提出,代表着传统互联网时代进入物联网时代,物联网技术突飞猛进,数以万计的智能设备层出不穷,所有物品通过无线射频识别等方式实现智能化管理。RFID技术是物联网发展的关键部分,也是构建物联网体系最基础、最核心的技术,RFID技术的飞速发展无疑对物联网领域的进步具有重要的意义。目前的RFID技术被运用于物联网工程中的方方面面,如物流仓储、交通、国防、医疗等,其中物流过程中的货物追踪、信息自动采集、仓储管理应用、港口应用、邮政包裹等都需要应用RFID的技术。随着标签的价格降低,其应用范围会大大扩大,由RFID技术产生的安全

基金项目:国家自然科学基金(62072317,61802263);广东省自然科学基金(2017A030312008);深圳大学青年教师启动项目(2019052,860/000002110322);深圳技术大学新引进高端人才财政补助科研启动项目(20211061010016)
This work was supported by the National Natural Science Foundation of China(62072317,61802263),Guangdong Natural Science Foundation(2017A030312008),Faculty Research Fund of Shenzhen University(2019052,860/000002110322) and Natural Science Foundation of Top Talent of SZTU(20211061010016).
通信作者:马军超(majunchao@sztu.edu.cn)

问题也更为突出。RFID 系统作为各种自动化管理的平台，其最基本的功能是标签识别。然而，存储在标签中的 id 信息被认为是一种裸数据，攻击者很容易假冒或者伪造一个与真实标签 id 相同的标签，RFID 系统很难验证从无线设备传输的标签身份的真实性。

由于标签的真实性和隐私性非常重要，近年来人们做了许多努力来提高 RFID 系统的安全性，相关的研究主要采用两种技术方案：基于加密的识别和认证协议以及基于特征提取的识别方法，通过分析通信信号获得与设备相关的特征。基于加密的识别和认证协议，主要通过修改现有的超高频 RFID 系统协议规范，提供基于加密算法更安全的认证协议。例如 Chao 等提出了一种基于现有 Gen2[1]（EPC Class1 Generation2）安全协议的新型通信模型，其中利用了一种基于分组密码准则的轻量级算法[2]；Mehmet Yavuz Yağcı 团队提出的方案是当标签每次被成功读取时，标签保存新的哈希值，修改后的哈希值是由随机文本的哈希组成的[3-4]；通过标签与后端数据库之间共享密钥的方式来防止伪造，并且利用每次查询来改变标签的响应，从而防止跟踪[5]；通过使用一个公共的密钥来保证标签通信过程中安全性。由于标签成本低、尺寸小，其计算能力和资源十分有限，这一限制使得传统的加密和安全协议的实现效率低下；其次，即使实现了传统的或者轻量级的基于加密的识别和认证协议，不恰当或者非标准化的算法也会导致攻击者拥有足够的资源破坏协议来找到底层数据。基于特征提取的识别方法是利用硬件的微小差异，通过分析通信信号获得与设备相关的指纹。比如 MPRMF[6] 在多个频率下测量标签的最小功率响应，用于进行标签识别[7]；利用专门定制的阅读器收集标签信号的时域和谱特征，其中时域特征包括 aTIE（Time Interval Error，时间间隔误差）和 $\bar{P}B$（Average baseband power，平均基带功率），aTIE 测量时钟的每个活动边缘与理想位置之间的距离，$\bar{P}B$ 测量标签信号的平均基带功率。GenePrint[8] 利用标签的前导码信号脉冲之间的内部相似性来提取硬件特征作为指纹，包括基于协方差的脉冲特征和基于功率谱密度的信号内部特征。基于特征提取的识别方法存在一些限制，比如 MPRMF 物理层识别特征对信号的传播距离敏感，并且需要在特定环境以及使用专门的设备来提取相应的特征；aTIE 特征熵值较低以至于限制了特征的唯一性，且该特征的提取需要专门定制的昂贵的设备；基于协方差的脉冲特征和基于功率谱密度的信号内部特征的提取算法复杂度较高，且该特征对环境的鲁棒性低，识别距离较短。

由于已有的相关工作[9-10]表明深度卷积神经网络在密集编码的时间序列进行学习是可行的，特别是在低信噪比下，这是一种很好的候选方法，因此本文提出了一种基于深度学习的超高频标签的物理层识别方法。此方法兼容当前的标签工业标准，可以顺利部署到现有的设备上。此外，深度学习基于多层非线性神经网络，结合大量训练数据，自动抽取特征并逐层抽象，直接从数据中获取特征，减少了为每个问题设计特征提取器的工作量。实验结果表明，基于深度学习的分类方法对超高频标签的分类表现出了更好的性能。

2 背景

2.1 网络模型

自 20 世纪 80 年代以来，从机器学习模型的层次结构上区分，机器学习的发展经历了浅层学习和深度学习两个阶段。上世纪 80 年代末期，反向传播算法（Back Propagation，BP）的发明促进了基于统计模型的机器学习出现[11]。人们发现，人工神经网络模型可以利用 BP 算法从大量训练样本中进行学习，并得到统计规律，这种人工神经网络模型大多是只含有一层隐藏层的浅层模型。上世纪 90 年代开始，最大熵方法（Logistic Regression，LR）、支撑向量机（Support Vector Machines）、决策树以及朴素贝叶斯等浅层模型在很多方面显示出优越性，由于理论上分析的复杂度，并且缺乏相应的训练经验和技巧，多层人工神经网络在这一时期并不活跃。

2006 年，多伦多大学教授 Hinton 和他的团队在顶级刊物《科学》上发表了对神经网络理念具有重大意义的文章[12]，深度学习这一概念被首次提出。他们指出多层神经网络在特征学习上高度依赖数据且有更优异的性能，其次多层神经网络可以利用逐层初始化来解决训练上存在的问题。这一理论的提出开启了机器学习的第二个阶段。

近年来，深度学习是机器学习领域中最新的趋势之一，其中卷积神经网络（Convolutional Neural Network，CNN）在语音识别、计算机视觉以及自然语言处理等方面显示出巨大的优势。1998 年，Lecun 教授提出了 LeNet[13] 模型，首次将卷积神经网络成功应用于手写数字识别的分类任务上。2012 年，Krizhevsky 团队提出卷积神经网络模型 AlexNet[14]，并获得 ImageNet 图像识别大赛的冠军，使得 CNN 成为在图像分类上的核心模型。2014 年，Facebook 提出了 DeepFace[15]。作为卷积神经网络在人脸识别上的奠基项目，DeepFace 识别精度高达 97%，这也代表 CNN 在人脸识别中取得了优异的性能。2016 年，由谷歌旗下 DeepMind 公司的团队开发的 AlphaGo[16] 机器人战胜了世界围棋冠军，其主要采用的技术也是深度学习，同年，寒武纪公司发布“寒武纪 1A”，并将其作为深度神经元网络处理器。这代表深度学习在不断发展并扩大影响力。

卷积神经网络是深度学习中应用非常广泛的深度神经网络，它在图像识别、模式识别、目标检测等方面所表现的性能是稳定并且高效的。深度学习的学习方法可以分成监督学习和无监督学习，卷积神经网络属于监督学习，通过一系列方法将庞大的数据进行降维并最终得到相应的抽象特征。典型的卷积神经网络由输入层、卷积层、池化层、全连接层和输出层五大单元组成，如图 1 所示。输入层是卷积神经网络的数据输入层，一般的数据格式是四维向量形式；卷积层是整个网络结构的核心组成部分，其主要作用是进行特征提取，从前馈数据中得到更深层次的特征表达；池化层的作用是对输入的特征进行压缩，从而缩小特征图的大小，简化网络参数的数量，池化层采用两种方法，分别为最大池采样和均值子采样两种方法，这两种方法能有效预防网络出现过拟合现象；全连接层一般位于最后一层的卷积层和池化层处理后，用于将所有的特征连接起来，将得到的特征送入输出层，并在最后得到分类结果。

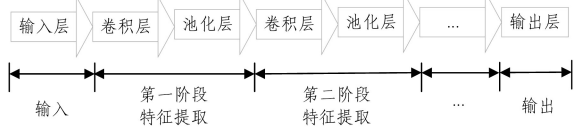


图 1 典型卷积神经网络结构示意图

Fig. 1 Schematic diagram of typical convolutional neural network

神经网络模型训练阶段主要包含前向传播和反向传播两个阶段。在前向传播阶段，过程包括输入层前向传播、卷积层前向传播、池化层前向传播、全连接层前向传播以及输出层前向传播。在反向传播阶段，对于卷积神经网络要解决的多分类任务，相应的模型使用交叉熵损失函数和 Softmax[17] 函数，通过梯度下降的 BP 算法，不断优化网络中的参数，从而得到性能最好的神经网络模型。对于 M 个输出的 Softmax 函数的定义如下：

$$z_i = z_i - \max(z_1, z_2, \cdots, z_m) \tag{1}$$

$$\sigma_i(z) = \frac{\exp(z_i)}{\sum_{j=1}^{M} \exp(z_j)}, i = 1, \cdots, M \tag{2}$$

其中，z_i 是第 i 个节点的分类结果，将其减去所有节点输出的最大值是为了保持数值的稳定。通过 Softmax 函数可以将多分类的预测结果转换为范围在[0，1]并且和为 1 的概率分布。

2.2 Gen2 协议规范

现有的超高频 RFID 系统通常遵循 Gen2 协议规范，该协议规范被认为是连接阅读器与无源超高频标签的最先进的通信标准。图 2 给出了阅读器与标签之间的成功读取过程，根据 Gen2 中的规范，每一次轮询从阅读器的 Query 查询命令开始，该 Query 命令包括时隙计数值 Q 和其他用于标签调制的参数，如反向散射链路频率。每个标签接收到 Query 命令后会随机选择[0，2^Q-1]范围中的数作为时隙计数器，查询帧会分成 2^Q 个时隙，并且相邻的两个时隙会由阅读器的 QueryRep 命令分隔。对于每个 QueryRep 命令，标签都会减少其时隙计数器的值。当时隙计数器的值为 0 时，标签将会回复一个 RN16 报文，如果没有发生碰撞状况，阅读器将发送一个 ACK 命令，其中包含一个相同的 RN16 报文作为确认信号。最后，被确认的标签将向阅读器回复包含标签 ID 的 EPC 信号。

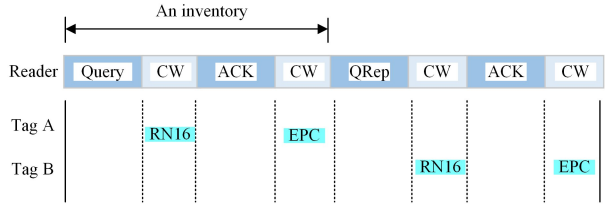


图 2 阅读器与标签之间的通信过程

Fig. 2 Communication process between reader and tag

3 基于深度学习的超高频标签的识别系统

本文提出了一种基于深度学习的超高频标签的识别系统，其系统设计方案如图 3 所示，主要包含信号采集模块、信号预处理模块、标签信号识别模块。信号采集模块采集原始的 RFID 通信信号，包括阅读器命令和标签响应；信号预处理模块从原始信号中提取标签信号；标签信号识别模块对标签进行相似度评分并设定阈值进行决策。

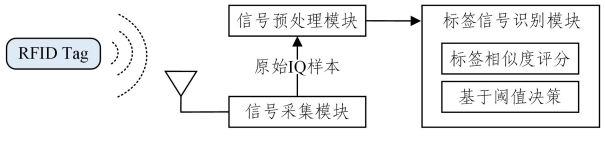


图 3 系统设计图

Fig. 3 System design drawing

3.1 信号采集模块和信号预处理模块

(1)信号采集模块

信号采集装置模块通过搭建一个超高频 RFID 信号采集系统来采集信号。本文利用 USRP 和 SDR 构建了符合 Gen2 协议的阅读器，其阅读器内部结构如图 4 所示[18-19]，包含 USRP 接收器、匹配滤波器、标签响应判断器、标签解码器、阅读器逻辑器和 USRP 发送器。本文采用来自两个制造厂商的 3 种不同型号的 150 个商用超高频标签作为信号的发射器，根据 EPC 协议来采集阅读器与标签通信过程中的信号，而信号采集模块采集到的原始信号包含阅读器命令和标签响应。

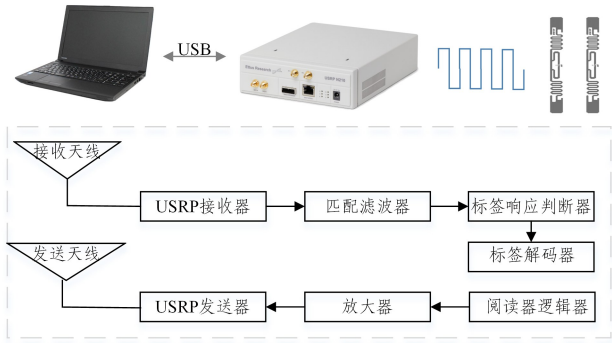


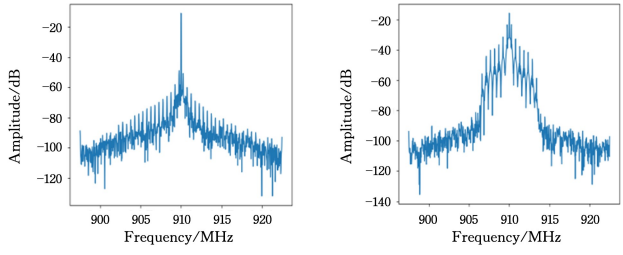
图 4 阅读器内部结构图

Fig. 4 Internal structure diagram of reader

(2)信号预处理模块

信号预处理模块根据信号采集模块采集到的原始信号提取出确切的物理层信息。为了减少逻辑数据的影响，本文选择提取标签响应信号中的 RN16 前导码信号。为了精确地将 RN16 信号从原始信号中提取出来，本文提出利用一个滑动窗口来遍历整个信号。主要步骤如下：

(1)通过观察标签的信号和阅读器的信号的频域图，图 5(a)为阅读器信号，图 5(b)为标签信号的频域图，可以发现阅读器信号和标签信号的频域图存在明显的差异，可以利用快速傅里叶变换检测该窗口中的信号能量是否符合标签的信号模式，用以区分阅读器信号和标签信号。



(a)标签信号的频域图　　(b)阅读器信号频域图

图 5 阅读器信号和标签信号的频域图

Fig. 5 Frequency domain diagram of reader signal and tag signal

(2)由于标签的 RN16 信号与标签的 ID 信号在频域上有相同的模式，需要进一步区分，因此，设置的滑动窗口的大小为略大于 RN16 信号的长度，如图 6 为标签滑动窗口的操作。可以看出滑动窗口的前端与后端是载波信号，满足这个条件的为候选窗口，而不满足这个条件的为非候选窗口，因此可以提取出整个 RN16 信号。为了获得更精确的 RN16 前导码信号，需要设置与 RN16 前导码信号长度相等的窗口大小，精确地定位标签响应的瞬态点。

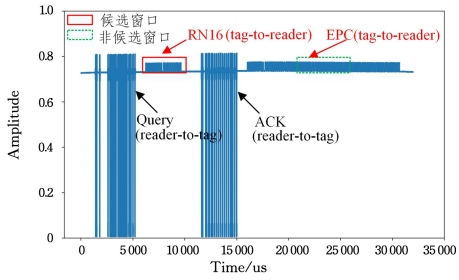


图 6 RN16 滑动窗口定位操作

Fig. 6 RN16 Sliding window positioning operation

(3)数据集组成

本文的信号采集设置主要包括阅读器天线与标签之间的距离以及阅读器天线与标签之间的角度变化，如图 7 所示。设定 1.2 m 处为基准点，在基准点采集用于构建评估系统分类精度性能实验的数据集；同时固定标签与阅读器天线的角度为 90°，在距离为 1.0 m，1.5 m，2.0 m 处采集信号构建评估识别距离对系统性能影响程度实验的数据集；固定标签与阅读器天线的距离为 1.5 m，在标签与阅读器天线的角度为 60°，90°，120°处采集信号构建评估阅读器与标签之间的角度对系统性能影响程度实验的数据集。

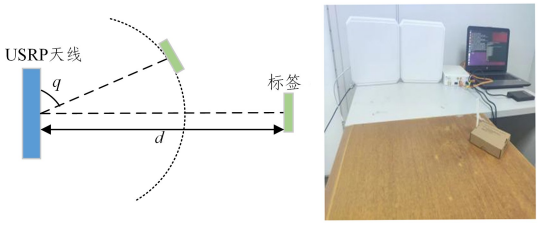


图 7 信号采集设置

Fig. 7 Signal acquisition setting

具体的数据集参数如表 1 所列，实验采集的数据集包含 Alien 9740，Impinj E44，Impinj H47 3 种不同型号的标签各 50 个，总共 150 个超高频标签，并且每个标签采集的信号数量为 5000 个，一共包括 75 万个信号样本。本文通过仿真的阅读器每秒读取 100 个标签信号，每一轮读取 1000 个标签信号，当数据越大时，所需的信号采集时间也会相应增加。

表 1 数据集信号及其组成

Table 1 Data set signal and its composition

标签类型	标签数量	位置	角度	每个标签采集的信号数量
Alien 9740	50	(1.0 m, 1.5 m, 2.0 m)	(60°, 90°, 120°)	5000
Impinj H47	50			
Impinj E44	50			

3.2 标签信号识别模块

(1)卷积神经网络模型结构

标签信号识别模块将提取的 RN16 前导码信号送入卷积神经网络进行相似度匹配，根据得到的相似度匹配分数与给定的阈值进行对比，若匹配分数大于阈值则决策为合法标签，否则决策为非法标签。经过大规模训练与反复调试，最终采用的卷积神经网络结构如图 8 所示。

信号采集模块采集的原始的信号样本存储为 32 位的浮点数，需要构建适用于神经网络模型训练的向量集。将 IQ 数据流转换成神经网络常用的四维向量形式 $N_{example} \times Dim_{channel} \times Dim_{IQ} \times Dim_{value}$，其中 $Dim_{IQ}=2$ 存储 I 和 Q 两个通道的数据，$Dim_{value}=1200$ 意味着每个数据向量包括 1200 个样本点，1200 个点是 RN16 前导码长度，$Dim_{channel}=1$ 代表单色样本类型，$N_{example}$ 代表向量数量。

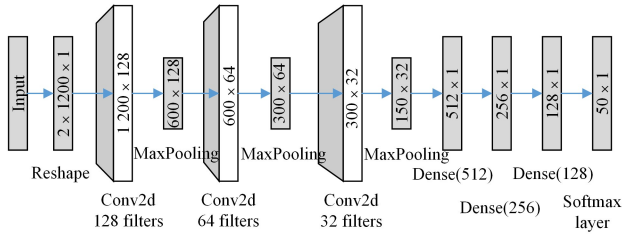


图 8 卷积神经网络结构图

Fig. 8 Convolutional neural network structure diagram

本文训练的卷积神经网络采用 3 层卷积层和 4 个全连接层，除了最后一个输出分类层采用 Softmax(归一化指数函数)函数，其他层都采用 ReLu(Rectified Linear Unit，线性整流函数)函数作为激活函数。其中 3 个卷积层分别包含 128，64，32 个过滤器，池化层采用最大池采样方法，4 个全连接层分别包含 512，256，128，50 个神经元，由于每种标签模型有 50 个标签，因此输出维度选择分类的类型数目为 50，输出值为候补标签与合法标签的相似度匹配分数。为了防止过拟合的出现，采用了正则化的方法，在全连接层应用了 dropout(弃权)技术，这是一种能有效提高泛化能力、降低过拟合的方法。训练模型使用交叉熵损失函数和 Adam(Adaptive Momentum Estimation)优化器来进行。

(2)模型训练以及参数优化过程

实验将采集的标签信号数据集按照 8∶2 的比例分成训练集和测试集，然后将其送入卷积神经网络模型进行参数的学习。其中训练集包含 600000 个样本，测试集包含 150000 个样本。综合模型训练的速度，我们选择批处理数为 256，一轮迭代次数大约为 2300 次，训练轮数为 20。模型训练过程的损失函数变化如图 9 所示，其中红色曲线为训练集损失函数，紫色为测试集损失函数，训练轮次大约为 8 次时参数趋于收敛。当参数收敛时，测试集的识别精度达到 99%以上，即能得到一个有效识别标签信号的卷积神经网络模型。

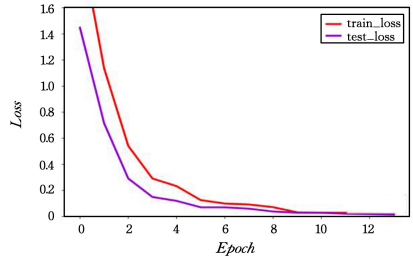


图 9 模型训练过程的损失函数(电子版为彩图)

Fig. 9 Loss function of model training process

4 实验结果与分析

4.1 实验过程

本文在有 WiFi 和蓝牙信号等无线射频信号噪声的室内环境中实施和评估该系统。该实验设备由一个 USRP N210 通用软件无线电外设和 150 个商用的超高频标签组成，其中 USRP 使用的天线为 Laird S9028PCL，是一个增益为 12 dbi 的圆极化天线。

我们进行了两组实验来评估本文系统的性能。每组使用

不同的标签模型，每个标签收集 5000 个 RN16 前导码，阅读器与标签之间的通信信道是固定的，中心频率为 910 MHz。第一组实验中，本文设置阅读器与标签之间的距离为 1.0 m，1.5 m，2.0 m，引起信号的平均基带功率的变化，也导致环境噪声的增加，从而带来了负面影响，据此来评估识别距离对系统的分类精度的影响。第二组实验中，我们设置阅读器天线与标签之间的方位为 60°，90°，120°，以进一步研究系统识别的鲁棒性。

4.2 评价指标与方法

本文最后分别评价此系统对标签分类和识别的性能。对于分类，本文评估系统能够将相同标签的 RN16 前导码归结为同一类的能力。对于识别，本文通过设定一个给定的阈值对识别性能进行评估。

(1)分类评估。本文使用 CCR(Correctly Classified Rate，正确分类率)来评估模型分类的能力。每个标签被单独分为一类，CCR 以神经系统模型的分类结果为度量，其结果是正确分类的实例的百分比。

(2)为了评价识别性能，本文通过计算 EER(Equal Error Rate，等错误比率)作为性能指标。具体执行如下，对每个候补标签的识别，需要先经过系统的预处理模块，然后转换数据格式后进入标签信号识别模块进行相似度评分，评分越高，标签与真实标签越相似。本文定义了 FAR(False Accept Rate，错误接受率)和 FRR(False Reject Rate，错误拒绝率)两个度量。对于给定阈值，FAR 是对应不同的标签但是匹配分数高于阈值的百分比，FRR 是对应相同的标签但是匹配分数低于阈值的百分比。当 FAR 与 FRR 相等时将其作为阈值，即 EER 对应的值。

4.3 结果分析

通过修改实际采集信号的距离和角度来验证本文设计方案的性能，并与传统的基于特征的分类方法进行对比，进一步验证本文提出系统的性能。为了研究标签在不同识别距离的分类性能，基于深度学习的分类模型的性能如图 10 所示，在距离为 1.0 m 的情况下，3 类标签的平均分类精度能达到 97%以上，但是在距离 1.5 m 时分类精度有了小幅度的下降，在识别距离为 2 m 时，Impinj E44 标签分类精度最高，其分类精度超过 94%，3 类标签的平均分类精度在 93%以上。实验结果说明了基于深度学习的分类模型适用于不同厂家的多种标签。

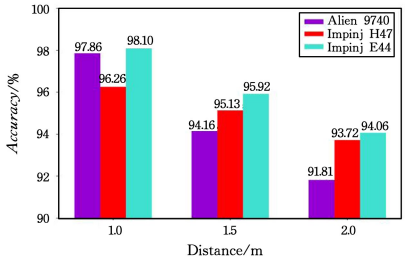


图 10 基于 CNN 不同距离下的分类精度(90°)

Fig. 10 Classification accuracy based on CNN at different distances(90°)

通过修改阅读器的天线与标签之间的角度，研究标签在不同识别角度的分类性能，如图 11 所示，在 60°，90°，120°的平均分类精度能超过 94%。但是不同类型的标签的分类精度有一定的差别，其中标签型号为 Alien 9740 的标签在 120°的分类精度相比其他类型的标签较低，但是其分类精度也在 92%以上，在实际的应用中可以通过缩短标签与阅读器的距离来提升分类精度。

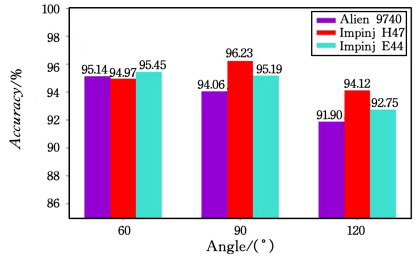


图 11 基于 CNN 不同角度下的分类精度(1.5 m)

Fig. 11 Classification accuracy based on different angles of CNN(1.5 m)

进一步研究深度学习模型在阅读器与标签识别距离为 2.0m 的识别性能，其受试者工作特征曲线如图 12 所示。由图可以看出，3 类标签的受试者工作特征曲线区别不大，在错误接收率很小的情况下，该分类模型仍能达到很高的正确接收率。其中 Impinj E44 标签的识别性能最好，在错误接受率为 0.045 时，其正确接收率为 1。实验结果说明在长达 2m 的识别距离下，基于深度学习的分类模型的识别性能是可信的。

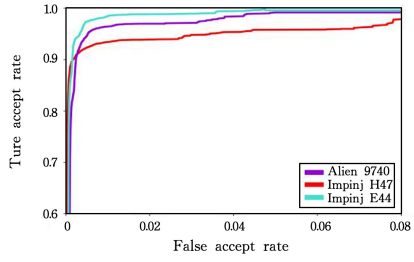


图 12 在小错误接收率的正确接收率(2.0 m)

Fig. 12 True reception rate in small error rate(2.0 m)

我们研究深度学习模型在阅读器与标签识别角度为 60°，90°，120°的识别性能，其受试者工作特征曲线如图 13 所示。在错误接收率很小的情况下，该分类模型仍能达到很高的正确接收率，其中阅读器与标签的识别角度为 60°和 90°时性能最好。实验结果说明在不同的识别角度下，基于深度学习的分类模型的识别可信度很高。

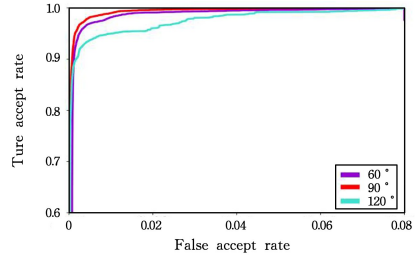


图 13 在小错误接收率的正确接收率(不同角度)

Fig. 13 True reception rate in small error rate(on different angles)

验证阅读器与标签识别角度为 1.0 m，1.5 m，2.0 m 时的识别的性能，结果如图 14 所示。基于深度学习的分类模型识别的平均 EER 为 0.023，说明在错误接收率为 2.3%的情况下，其正确识别率大于 97%。当识别距离为 1.0 m 时，其识别性能最好，当距离增加到 2.0 m 时，其 EER 最大为 0.0455，因此，当候补标签的匹配分数大于 EER 时则接收为合法标签，当候补标签的匹配分数小于 EER 时则决策为非法标签。

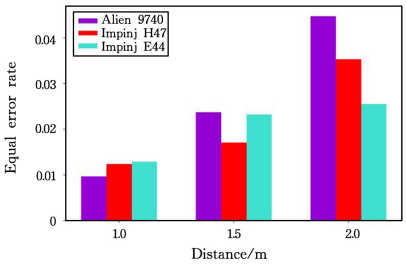


图 14 在不同距离下的 EER

Fig. 14 EER at different distances

验证阅读器与标签识别角度为 60°,90°,120°时的识别的性能,结果如图 15 所示。基于深度学习的分类模型识别的平均 EER 为 0.035,最坏的情况下的 EER 为 0.059。当识别性能出现一定程度下降时,可以适当减少识别的距离来提高识别的可信度。因此在一般情况下,可以通过设置阈值为 0.059,当候补标签的匹配分数大于 EER 时接收为合法标签,否则为非法标签。

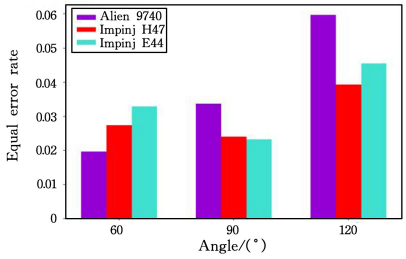


图 15 在不同角度下的 EER

Fig. 15 EER at different angles

结束语 本文提出了基于深度学习的超高频标签的物理层识别方法,并从分类和识别两方面评估系统的性能。通过实验验证,基于深度学习的标签识别能达到 94% 的识别精度,且在识别距离长达 2 m 的情况,仍能保持很高的识别性能。与传统的机制相比,所提方法在低信噪比的情况下仍能达到很高的识别性能。

参 考 文 献

[1] EPCglobal, Specifification for RFID Air Interface EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz-960 MHz, 2008.

[2] HUI Y C, WANG Y M. Secure RFID system based on light-weight block cipher algorithm of optimized S-box[C]// IEEE. 2010.

[3] YAGCI M Y, AYDIN M A. Implementation of Passif Secure RFID Protocol[C]// 2018 3rd International Conference on Computer Science and Engineering(UBMK). 2018.

[4] ZHAO F, LI H, YU F. An Efficient and Secure Protocol for Low-cost RFID Systems[C]// 2009 International Conference on Computer and Communications Security(ICCCS). 2009.

[5] KERSCHBAUM F, SORNIOTTI A. RFID-based supply chain partner authentication and key agreement[C]// Second ACM Conference on Wireless Network Security. 2009.

[6] SENTHILKUMAR C G P, THOMPSON D R, DI J. Fingerprinting RFID Tags[J]. IEEE Transactions on Dependable & Secure Computing, 2011, 8(6): 938-943.

[7] ZANETTI D, DANEV B, CAPKUN S. Physical-layer identification of UHF RFID tags[C]// Proceedings of the 16th Annual International Conference on Mobile Computing and Networking. 2010.

[8] HAN J, QIAN C, YANG P, et al. GenePrint: Generic and Accurate Physical-Layer Identification for UHF RFID Tags[J]. IEEE ACM Transactions on Networking, 2016, 24(2): 846-858.

[9] O'SHEA T J, CORGAN J, CLANCY T C. Convolutional Radio Modulation Recognition Networks[C]// International Conference on Engineering Applications of Neural Networks. 2016.

[10] OSHEA T, HOYDIS J. An Introduction to Deep Learning for the Physical Layer[J]. IEEE Transactions on Cognitive Communications & Networking, 2017, 3(4): 563-575.

[11] RUMELHART D E, HINTON G E, WILLIAMS R J. Learning Representations by Back Propagating Errors[J]. Nature, 1986, 323(6088): 533-536.

[12] HINTON G E, SALAKHUTDINOV R R. Reducing the Dimensionality of Data with Neural Networks[J/OL]. https://www.science.org/doi/10.1126/science.1127647.

[13] LECUN Y, BOTTOU L, BENGIO Y, et al. Gradient-based learning applied to document recognition[C]// Proceedings of the IEEE. 1998: 2278-2324.

[14] KRIZHEVSKY A, SUTSKEVER I, HINTONG E. Imagenet classification with deep convolutional neural networks[J]. Advances in Neural Information Processing Systems, 2012, 25: 1097-1105.

[15] TAIGMAN Y, YANG M, RANZATO M, et al. Deepface: Closing the gap to human-level performance in face verification[C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. 2014: 1701-1708.

[16] SILVER D, HUANG A, MADDISONC J, et al. Mastering the game of Go with deep neural networks and tree search[J]. Nature, 2016, 529(7587): 484-489.

[17] BAI Z, WANG L, CHEN J N, et al. Optimization of deep convolutional Neural Network for Large-scale Image classification [J]. Journal of Software, 2018, 29(4): 10.

[18] KARGAS N, F MAVROMATIS, BLETSAS A. Fully-Coherent Reader With Commodity SDR for Gen2 FM0 and Computational RFID[J]. Wireless Communications Letters IEEE, 2015, 4(6): 617-620.

[19] BUETTNER M, WETHERALL D . A software radio-based UHF RFID reader for PHY/MAC experimentation[C]// 2011 IEEE International Conference on RFID. 2011.

YU Jiabao, born in 1996, master. His main research interests include wireless device identification and deep learning.

MA Junchao, born in 1983, associate professor, Ph. D, senior engineer. His main research interests include big data, interest of things, and wireless ad hoc and sensor networks.