文章编号：2095-4980(2022)12-1305-06

合作与欺骗信号共存下的CNN射频指纹识别方法

张雅琪，杨　春*，刘友江，杨大龙，秋勇涛
(中国工程物理研究院 电子工程研究所，四川 绵阳 621999)

摘　要：射频指纹是设备硬件的固有特征，与发射信号本身无关，因此常用于通信抗欺骗中。本文基于射频指纹的原理，采用神经网络对接收机所获得的原始信号样本进行处理，包括I/Q序列、幅度/相位、星座图的二值图和星座图的颜色密度图4种信号表现形式，达到抗欺骗效果。在信干噪比为-30~30 dB的情况下，信号的识别准确率最高可达99.93%。相较于现有文献，本文所提的基于深度学习的方法可适应不同信干噪比的通信场景，在欺骗信号与合法信号同时存在的复杂通信环境下实现抗欺骗。

关键词：抗欺骗；射频指纹；卷积神经网络；星座图；颜色密度图
中图分类号：TN929.5　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021356

Convolutional Neural Network Radio Frequency fingerprint identification method for co-existence of cooperative signal and spoofing signal

ZHANG Yaqi，YANG Chun*，LIU Youjiang，YANG Dalong，QIU Yongtao
(Institute of Electronic Engineering，China Academy of Engineering Physics，Mianyang Sichuan 621999，China)

Abstract：The radio frequency fingerprints are inherent features of the device hardware, and will not change with the transmitted signal, therefore they are often used in communication anti-spoofing. In this paper, the neural network is adopted to process the original signal samples obtained by the receiver, including I/Q sequence, amplitude/phase, binary image of constellation diagram and color density diagram of constellation diagram to achieve anti-deception effect. When the signal-to-interference and noise ratio is in the range of -30 dB to 30 dB, the signal recognition accuracy can reach up to 99.93%. Being different from the existing literature, the method can be adapted to the scenes with different signal-to-interference and noise ratios. This research shows that the proposed method is feasible to achieve anti-spoofing in a complex communication environment where spoofing signals and legal signals coexist.

Keywords：anti-spoofing；RF fingerprint；Convolutional Neural Network；constellation figure；color density figure

欺骗干扰是指接收或模拟通信信号，人为地发送参数相同的虚假信号，以对接收机造成干扰，使接收端得到错误的信息，做出错误的决策[1]。目前，抗欺骗干扰检测技术研究主要基于干扰信号和真实信号在整体波形上某些参数的差异[2]，如，绝对功率、到达时间、到达角等。由于传统方法对信号特定参数具有依赖性，一旦这些参数发生改变，应用就会受到限制。如信号功率检测技术[3]和信号质量监测技术，都只适用于一定功率范围内的欺骗干扰信号，随着欺骗信号的功率增加或减弱，这两种方法检测效果则会逐渐失效[4]。因此需要寻找新型的安全机制与传统方法相结合，在信号参数发生改变时，接收方仍能对信号是否受到欺骗进行有效识别，且该机制无法被模仿，更不能被绕过。

研究发现，无线设备在制造中会由于工艺等原因导致不同的硬件存在差异性，而这些差异会给无线信号带来不同程度的损伤[5]。因此对无线信号某些特征进行分析，便可以对信号来源加以辨别，这些特征被称为“射频指纹”。射频指纹目前主要用于对信号来源的识别[6]，军事上利用辐射源个体识别技术实现辐射源个体识别[7]。

收稿日期：2021-10-01；**修回日期：**2021-11-10
基金项目：中国工程物理研究院院长基金资助项目(YZJJLX2017006)
***通信作者：**杨　春　email:ychun2005@sina.com

而在实际场景下，同一时刻往往不只存在单一信号，当多个设备同时发送信号时，如何识别出正确信号仍是一个有待解决的问题。本文针对射频指纹在合法信号与欺骗信号同时存在的情形下的应用展开研究，利用接收到的信号本身提取出射频指纹，在存在不同程度的欺骗干扰和噪声环境下，对信号是否受到干扰进行有效识别。

本文在合法方和干扰方同时存在的通信环境下，设计出基于深度学习的分类模型，对合法方信号和非合法方信号进行有效区分；然后对模型性能进行多维度评估，调整训练参数以达到最佳识别效果，并对信号多种表达方式下的识别曲线进行对比分析。

1 系统模型

考虑一个合法方和干扰方同时存在的通信环境，其中包含一个合法发射机和一个合法接收机，以及若干非法发射机(产生干扰信号)。本文研究最简单常见的干扰场景，即只有一个合法用户和一个非法用户，具体的系统模型如图 1 所示。

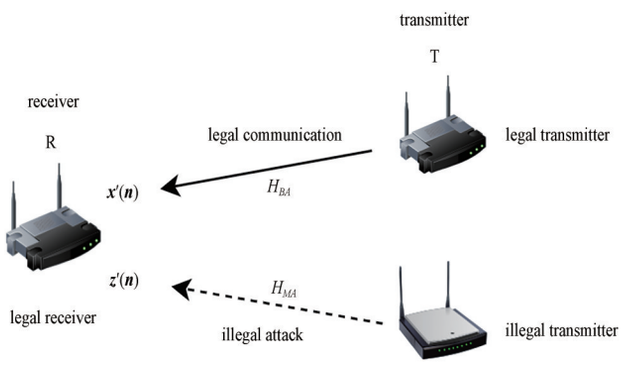


Fig.1 System model
图 1 系统模型

合法发射机和非法发射机同时发送信号，其中欺骗信号的功率大小不确定。仿真信道 H_{MA} 和 H_{BA} 中考虑高斯白噪声的影响，接收端接收到的信号会同时包含真实信号和欺骗干扰以及噪声，可表示为：

$$\boldsymbol{r}'(n)=\boldsymbol{x}'(n)+\boldsymbol{z}'(n)+\boldsymbol{n} \tag{1}$$

式中：$\boldsymbol{r}'(n)$ 为接收端接收到的信号；$\boldsymbol{x}'(n)$ 为接收到的真实信号；$\boldsymbol{z}'(n)$ 为接收到的欺骗信号；$\boldsymbol{n}$ 为等效输入的高斯白噪声。欺骗干扰模拟真实信号，与真实信号结构相同，但包含的信息却具有欺骗性。由于功率放大器工作在其非线性区域(即接近其最大输出功率)时，会在该区域发生输出信号的显著压缩，因此仿真实验中采用了 2 个不同的记忆多项式模型模拟不同的发射机。

2 基于卷积神经网络的射频指纹抗欺骗识别

基于卷积神经网络的通信抗欺骗干扰过程包括：通过随机信号发生器产生 2 组结构相同的随机信号，分别经过 2 个发射机前端；发射机采用仿真设计，使用 2 个不同参数的功率放大器模型；信号经过模拟高斯白噪声信道到达接收端，在接收端加入一个判别器，对解调后的符号信号进行分类。分类结果包括 3 类：合法信号、被噪声淹没的信号以及欺骗信号。过程图如图 2 所示。

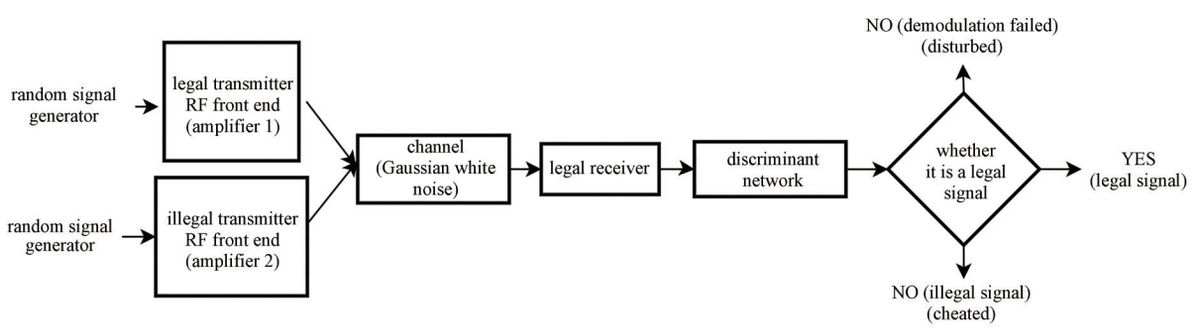


Fig.2 Flow chart of communication anti−spoofing based on convolutional neural network
图 2 基于卷积神经网络的通信抗欺骗干扰流程图

接收机接收到信号之后，提取出信号的 I/Q、幅度/相位、星座图等，组成数据集送入判别网络中。其中星座图包括二值图像和颜色密度图，颜色密度图中颜色会随着点的密度发生变化，相比于二值图像，可以反映出更多细节信息。射频指纹识别主要分为 3 步：信号预处理、特征提取和分类识别。信号预处理阶段主要任务是在接收信号中截取感兴趣的区间，对该区间的信号进行归一化、去噪等预处理。对于图片，为了减少变量维度，加快训练速度，本文将星座图的二值图和颜色密度图均变为灰度图。特征提取阶段是对原始接收信号进行不同的处理和变换，有利于之后的分类识别。在深度学习方法中，由于判别网络自身可以对信号进行复杂特征的提取，

因此研究重点不再是特征提取[8]。分类器包括传统机器学习方法和深度学习方法。传统机器学习中已有大量成熟的分类器可供选择，如，K 近邻(K Nearest Neighbor，KNN)[9]、决策树、支持向量机(Support Vector Machine，SVM)等方法；在深度学习中，需要重点研究的是网络结构的设计，如何优化网络是决定最终识别准确率的重要环节之一。

针对输入为 I/Q 和幅度/相位的情况，在 AlexNet 网络的基础上，本文参考文献[10]中所用的网络结构，实现对欺骗信号和合法信号的分类。由于卷积神经网络(CNN)会以一个固定大小的窗口在输入数据上进行滑动，窗口大小会对识别效果产生一定的影响。输入 CNN 中的是一段固定窗口长度的原始 I/Q 样本序列或幅度/相位数值，将每个复值的实部和虚部分开，变成一个二维实值，然后将其输入至第一个卷积层中。卷积层是 CNN 的核心，其主要目的是从输入数据中提取特征，由一组对输入数据执行卷积运算的空间滤波器组成。为了降低前一卷积层的特征图维数，同时不丢失重要信息，在卷积层后加入最大池化层，减少网络中的参数和计算量。第二个池化层的输出作为全连接层的输入，全连接层为传统的多层感知器，其神经元与前一层中的所有激活步骤完全连接，主要目的是对从前面的卷积层中提取的高级特征执行分类任务。网络具体结构如图 3 所示，CNN 的超参数选择与窗口大小设置在实验部分进行论证。

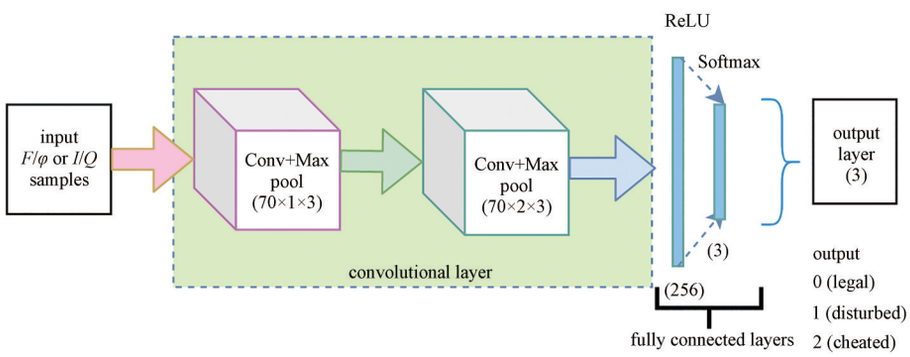


Fig.3 Network structure when input are I/Q or amplitude/phase sequences
图3 输入为I/Q或幅度/相位时的网络结构

当输入为图片时，参考著名的 LeNet−5 网络，将图像处理为矩阵。卷积层的卷积核大小设置为[5×5]，用于提取图片中的局部特征。最大池化层的卷积核大小设置为[5×5]，步长为 2，用于减少网络参数，防止过拟合。最后一个全连接层的输出值使用 Softmax 进行分类，其结构如图 4 所示。

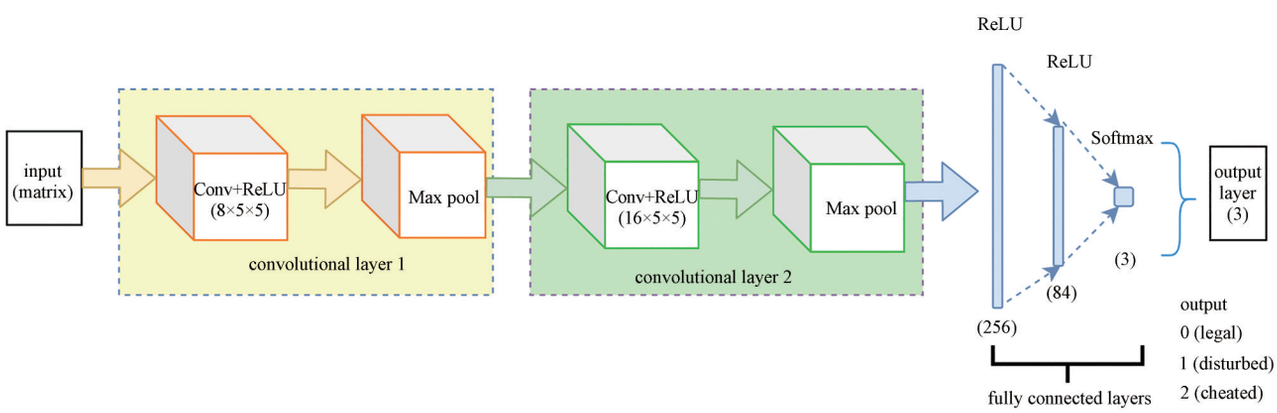


Fig.4 Structure of CNN when the input are images
图4 输入为图像时CNN的结构

3　仿真结果与分析

分析在抗欺骗场景下，信干噪比变化范围为−30~30 dB 时，利用信号的 4 种表示方法(I/Q、幅度/相位、星座图的二值图、星座颜色密度图)的性能，针对不同的变量对提出的网络进行参数优化。

3.1　数据集

由于合法信号和非法信号到达的接收机相同，因此仿真中只考虑发射方射频前端的区别。合法信号与非法

信号分别经过2个不同的射频前端后，由于高斯白噪声的影响，最终会出现不同信干噪比(Signal to Interference plus Noise Ratio，SINR)。信干比(Signal−Interference Ratio，SIR)、信噪比(Signal to Noise Ratio，SNR)以及信干噪比如式(2)~(4)所示。

$$R_{\mathrm{SN}}=10\lg\frac{p_{\mathrm{S}}}{p_{\mathrm{N}}} \tag{2}$$

$$R_{\mathrm{SI}}=10\lg\frac{p_{\mathrm{S}}}{p_{\mathrm{I}}} \tag{3}$$

$$R_{\mathrm{SIN}}=10\lg\frac{p_{\mathrm{S}}}{p_{\mathrm{N}}+p_{\mathrm{I}}} \tag{4}$$

式中p_{S},p_{N},p_{I}分别为信号功率、噪声功率和干扰功率，由此信干噪比可表示为：

$$R_{\mathrm{SIN}}=10\lg\frac{1}{\left(\dfrac{1}{10^{\frac{R_{\mathrm{SI}}}{10}}}+\dfrac{1}{10^{\frac{R_{\mathrm{SN}}}{10}}}\right)}=10\lg\frac{10^{\frac{R_{\mathrm{SI}}+R_{\mathrm{SN}}}{10}}}{10^{\frac{R_{\mathrm{SI}}}{10}}+10^{\frac{R_{\mathrm{SN}}}{10}}} \tag{5}$$

依据系统模型生成通信信号的数据集，调制方式使用16QAM。数据集中包括训练集、验证集与测试集。由于网络结构中有一些超参数需要自行设置，因此选用不同的参数在训练集上进行训练，将训练得到的模型用于验证集，选出最好的模型。该模型在理论上是一个能够有效区分信号是否受到干扰的判别器，而模型的泛化能力最终需要通过在测试集上的表现进行判断。训练集要尽可能包括所有可能遇到的情况，根据实际中最常遇到的情形，SNR取值范围为0~33 dB，SIR取值范围为−30~33 dB，二者均以1为步径遍历所有值。按照长期演进(Long Term Evolution，LTE)物理上行共享信道(Physical Uplink Shared Channel，PUSCH)调制方式及对应的误差向量幅度(Error Vector Magnitude，EVM)标准性能评估，为保证接收机正常解调，16QAM调制时，EVM限值为12.5%。将解调后的符号信号与发送信号比对，算出EVM值。与合法信号对比，EVM≤12.5%的认为是成功解调且未被欺骗的信号，作为样本1；与非法信号对比，EVM≤12.5%的认为是成功解调但被欺骗的信号，作为样本2；与合法信号和非法信号对比，EVM>12.5%的认为是被噪声干扰导致无法解调的信号，作为样本3。测试集和验证集本着尽量接近真实情况的原则，在可能遇到的SNR和SIR的情况中均匀随机取值。

在接收端采集到解调后的符号信号后，将信号I/Q值分开，组成一个二维实数矩阵，作为信号特征值。此外，研究中还提取了信号的幅度/相位值，画出解调信号星座图，并将星座图分为二值图和颜色密度图两种表现形式。最终生成训练集中总样本数为15 474 816个符号数，3 838张图片(包括星座二值图和星座颜色密度图)。验证集中有1 612 800个数据，400张图片。测试集中包含4 032 000个数据，1 000张图片。

3.2 不同信号表示方法准确率对比

选用信号的I/Q值、幅度/相位值、星座图的二值图和星座图的颜色密度图4种表示方法，输入至网络中进行训练，得到不同数据集训练下的收敛曲线，如图5所示。图中横坐标为训练次数，纵坐标为识别准确率。

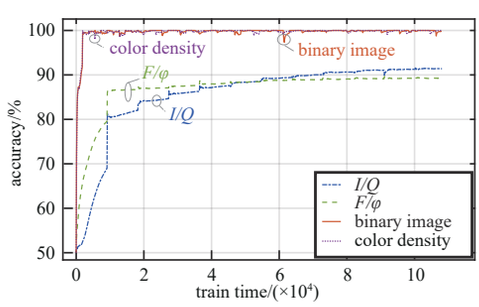


Fig.5 Convergence curves comparison of various signal representation methods

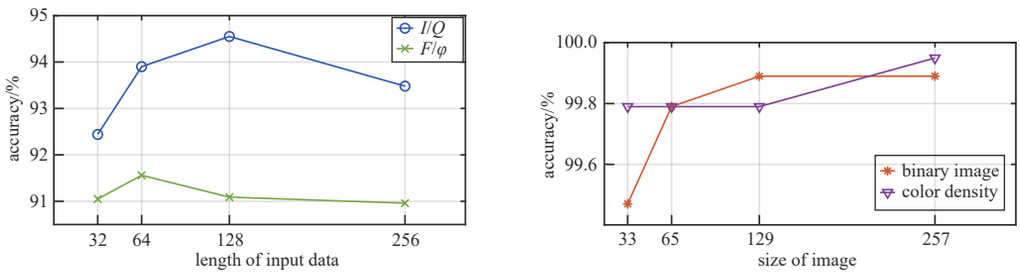
图5 各种信号表示方法的收敛曲线对比

以上结果中，所有数据训练过程中的损失函数使用交叉熵，优化函数为Adam，原始学习率均取0.000 1。参考文献[10]，将I/Q和幅度/相位每次输入序列大小暂定为2×64，图片输入大小为257×257。从图中可以看出，训练中图片作为输入时，最终收敛的准确率整体要高于数据，且收敛速度也更快。说明将信号映射至星座图会使不同设备的非线性特征更为明显，从而有利于抗欺骗识别。并且一张星座图中包含4 032个星座点，而单次输入序列大小有限，包含的信息远不如星座图中丰富。当输入为序列时，单次输入的信号长度会对识别性能产生影响，但并非长度越大，识别效果越好。

3.3 不同训练参数下模型性能对比

对于I/Q和幅度/相位作为输入的模型，CNN会以一个固定大小的窗口在数据上进行滑动，窗口大小决定了单次输入网络的数据量。鉴于实验中采用的是16QAM调制方式，为尽可能包含足够的信息，选取32,64,128和

256的数据长度，在验证集上进行准确率比较，得到数据大小和准确率关系如图6(a)所示。当输入为星座二值图或星座颜色密度图时，其图片像素大小会对学习效果产生一定的影响。图片太小，容易丢失重要信息，模糊设备的射频指纹特征；图片太大，会增加计算量，甚至导致内存不足，因此需要研究不同图像大小对模型识别精确度的影响。不同图像质量和识别准确率之间的关系如图6(b)所示。



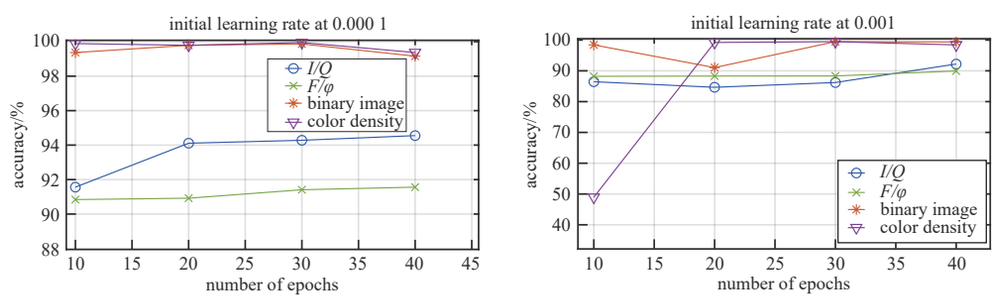
(a) accuracy under different input sequence sizes　　(b) accuracy under different image sizes

Fig.6 Comparison of recognition accuracy under different input data sizes

图6 不同的输入数据大小下识别准确率对比

从图中可以发现，输入为I/Q时，数据长度为128时效果最好；输入为幅度/相位时，数据长度为64时准确率最高。可见，单次输入数据量并非是越大越好，数据量太少，无法完全反映非线性特征；数据量太多，会造成信息冗余，识别率反而下降。输入为图像时，当像素值选为129时，星座图二值图像的CNN模型识别率达到最佳，继续增大像素其准确率不会再增大；当像素值选为257时，星座颜色密度图识别效果最好。这是由于星座图的颜色密度图比二值图中包含更多的细节信息，因此需要更大的像素值才能达到最优的识别效果。

在CNN模型中，不同的参数，如学习率、迭代次数(epoch)大小都将影响模型最终的训练结果。对epoch从10到40，以及初始学习率取0.000 1和0.001时的性能进行评估，得到各特征在验证集上的准确率对比，如图7所示。



(a) accuracy when the learning rate is 0.000 1　　(b) accuracy when the learning rate is 0.001

Fig.7 Variation curve of recognition accuracy under different CNN parameters

图7 不同CNN参数下的识别准确率变化曲线

可以发现，对于I/Q特征和幅度/相位，当学习率为0.000 1，epoch为40时，在验证集表现最好；对于星座二值图和星座颜色密度图，学习率为0.000 1，epoch为30时，效果最好，此时随着epoch数量增加，准确率不仅没有上升，还会由于训练次数过多造成过拟合，导致泛化能力下降。

3.4 模型性能评价

由于不同的分类算法在数据集上的表现效果不同，需要选取合适的评价指标对分类结果做出判断。结合通信抗欺骗研究的特点，本文将识别准确率和系统被欺骗的概率作为判别标准。识别准确率是指分类正确的样本数在所有样本数中所占的比例，通常识别准确率越高，分类器越好；系统被欺骗的概率是指被分为合法信号的样本中实际为欺骗信号的概率，欺骗信号所占的比例越小，分类器效果越好。根据这两个评价指标得到不同输入特征的性能对比，如表1所示。

表中对比了信号的4种表示方法(I/Q、幅度/相位、星座二值图以及星座颜色密度图)的模型性能。在SINR为−30~30 dB时，信号4种表示方法在最优系统参数配置下，最佳识别准确率分别为94.55%,91.56%,99.59%和99.93%。在所有成功解调的信号中，合法信号在其中的比例仅为70.13%，即系统有29.87%的可能性会被欺骗。可见基于射频指纹的识别中，各种特征作为输入时均具有一定的抗欺骗效果，其中采用星座颜色密度图效果最好，仅有0.03%的概率被欺骗。

4 结论

本文提出一种基于CNN的射频指纹识别方法，并成功地在不同SINR场景下实现对合法信号和欺骗信号的识别。本方法将接收机中接收到的原始采样信号以4种不同的表示方法放入CNN中，提取其指纹特征并进行抗欺骗识别。在4种信号表示方法中效果最好的为星座图的颜色密度图，使用该方法得到的识别准确率为99.93%，该方法在理论上基本可以避免被欺骗。本研究结果是在仿真中得到，实际情况更为复杂，因此算法在实际的工程应用中会存在很多约束，如何改进算法以更接近实际应用情况，将是下一步的研究重点。

表1 不同输入特征性能对比

Table1 Performance comparison of different input features

feature	recognition accuracy rate/%	probability of the system being cheated/%
I/*Q*	94.55	5.00
F/*φ*	91.56	11.45
binary image	99.59	0.31
color density	99.93	0.03

参考文献：

[1] 何亮,李炜,郭承军. 生成式欺骗干扰研究[J]. 计算机应用研究, 2016,33(8):2405-2408. (HE Liang,LI Wei,GUO Chengjun. Study on GPS generated spoofing attacks[J]. Application Research of Computers, 2016,33(8):2405-2408.) doi:10.3969/j.issn.1001-3695.2016.08.036.

[2] 李艳莉,田晓,韦顺军. 雷达欺骗干扰特征提取与综合感知方法综述[J]. 电讯技术, 2018,58(4):477-486. (LI Yanli,TIAN Xiao, WEI Shunjun. Review of radar deception jamming feature extraction and integrated sensing methods[J]. Telecommunication Engineering, 2018,58(4):477-486.) doi:10.3969/j.issn.1001-893x.2018.04.020.

[3] 刘丁浩,吕晶,马蕊,等. 卫星导航系统欺骗与抗欺骗技术研究与展望[J]. 通信技术, 2017,50(5):837-843. (LIU Dinghao,LYU Jing,MA Rui,et al. The research and prospect of spoofing and anti-spoofing technology in the satellite navigation system[J]. Communication Technology, 2017,50(5):837-843.) doi:10.3969/j.issn.1002-0802.2017.05.001.

[4] 申成良. GPS 接收机抗欺骗式干扰实验研究[D]. 成都:电子科技大学, 2018. (SHEN Chengliang. Experimental research on GPS receiver anti-spoofing jamming[D]. Chengdu,China:University of Electronic Science and Technology of China, 2018.)

[5] BRIK V,BANERJEE S,GRUTESER M,et al. Wireless device identification with radiometric signatures[C]// Proceedings of the 14th ACM international conference on Mobile computing and networking. San Francisco,California,USA:ACM, 2008:116-127.

[6] 曾勇虎,陈翔,林云,等. 射频指纹识别的研究现状及趋势[J]. 电波科学学报, 2020,35(3):305-315. (ZENG Yonghu,CHEN Xiang,LIN Yun,et al. Review of radio frequency fingerprinting identification[J]. Chinese Journal of Radio Science, 2020,35(3):305-315.) doi:10.13443/j.cjors.2019070501.

[7] DUDCZYK J,KAWALEC A. Specific emitter identification based on graphical representation of the distribution of radar signal parameters[J]. Bulletin of the Polish Academy of Sciences:Technical Sciences, 2015,63(2):391-396. doi:10.1515/bpasts-2015-0044.

[8] KULIN M,KAZAZ T,MOERMAN I,et al. End-to-end learning from spectrum data:a deep learning approach for wireless signal identification in spectrum monitoring applications[J]. IEEE Access, 2017(6):18484-18501. doi:10.1109/ACCESS.2018.2818794.

[9] 陈翔,郝晓军,许雄,等. 基于时域RF-DNA的功率放大器射频指纹识别[J]. 太赫兹科学与电子信息学报, 2020,18(1):129-135. (CHEN Xiang,HAO Xiaojun,XU Xiong,et al. RF fingerprinting extraction of power amplifier based on time domain RF-DNA fingerprint[J]. Journal of Terahertz Science and Electronic Information Technology, 2020,18(1):129-135.) doi:10.11805/TKYDA2018318.

[10] RIYAZ S,SANKHE K,IOANNIDIS S,et al. Deep learning Convolutional Neural Networks for radio identification[J]. IEEE Communications Magazine, 2018,56(9):146-152. doi:10.1109/MCOM.2018.1800153.

作者简介：

张雅琪(1998-)，女，在读硕士研究生，主要研究方向为智能信号处理.email:zhangyaqi19@gscaep.ac.cn.

杨 春(1972-)，男，博士，研究员，主要研究方向为通信与信息系统.

刘友江(1986-)，男，博士，研究员，主要研究方向为智能化无线电系统.

杨大龙(1987-)，男，博士，副研究员，主要研究方向为宽带无线传输接收处理技术和飞行自组织网络.

秋勇涛(1991-)，男，博士，副研究员， 主要研究方向为电子与信息.