基于CNN网络的通信干扰信号识别

张博轩[1]，王圣举[2]
（1.宁夏回族自治区无线电监测站，宁夏 银川 750004；2.长安大学电子与控制工程学院，陕西 西安 710064）

摘要：在现实生活中，通信干扰模式越来越复杂，要想有效抗干扰，干扰识别是关键。为了提高干扰信号的识别率，文章提出了一种基于卷积神经网络和短时傅里叶变换的干扰信号分类识别方法。首先利用短时傅里叶变换算法对干扰信号与二进制相移键控（Binary Phase Shift Keying，BPSK）通信信号的叠加信号进行时频分析，生成时频图像，将时频图像作为卷积神经网络的输入，卷积神经网络会自动对图像进行特征的提取和训练，实现对常见的通信干扰信号（连续波干扰、多音干扰、线性调频干扰、噪声调频干扰）的识别。仿真结果表明，文章算法对四种干扰信号的综合识别率达到了97.8%，在信干噪比为[0 dB，10 dB]的识别率为99.5%，与传统的识别算法相比，效果良好。

关键词：通信干扰；干扰信号识别；短时傅里叶变换；卷积神经网络

doi：10.3969/J.ISSN.1672-7274.2022.09.020

中图分类号：TN 97　　**文献标示码：**A　　**文章编码：**1672-7274（2022）09-0059-04

Communication Interference Signal Identification Based on CNN Network

Zhang Boxuan[1], WANG Shengju[2]
**(1. Radio Monitoring Station of Ningxia Hui Autonomous Region, Yinchuan 750004, China;
2.School of Electronics and Control Engineering, Chang'an University, Xi'an 710064, China)**

Abstract: In real life, communication interference patterns are becoming ever more complex. In order to effectively resist interference, interference identification is the key. In order to improve the recognition rate of interference signals, a classification and recognition method of interference signals based on convolutional neural network and short-time Fourier transform is proposed in this paper. First, the time-frequency analysis of the superimposed signal of interference signal and binary phase shift keying (BPSK) communication signal is performed by using the short-time Fourier transform algorithm, and the time-frequency image is generated. The time-frequency image is used as the input of convolutional neural network, which will automatically extract and train the features of the image, Realize the identification of common communication interference signals (continuous wave interference, multi tone interference, linear frequency modulation interference, noise frequency modulation interference). The simulation results show that the comprehensive recognition rate of this algorithm for the four kinds of interference signals is 97.8%, and the recognition rate at the signal to interference noise ratio of [0 dB, 10 dB] is 99.5%. Compared with the traditional recognition algorithm, the effect is good.

Key words: communication jamming; interference signal recognition; short-time Fourier transform; convolutional neural network

0 引言

随着日益复杂的电磁环境以及干扰技术的发展，通信干扰对正常的通信交流构成了严重的威胁[1]。复杂的电磁环境导致各个电磁器件不可避免地受到干扰，为了保证通信、雷达等设备的正常工作，我们可以提高设备的抗干扰能力，抑制干扰。干扰信号的检测与识别是抗干扰的前提和基础，只有知道是哪种干扰才能执行具体的抑制方法来应对干扰。传统的通信干扰识别方法依赖于通信技术人员的经验，存在耗时长、无法自动识别、识别率低等缺点[2]。对通信干扰识别的研究，可以减轻技术人员的负担，减少人为因素带来的负面影响，从而大大提高识别精度。

目前，对干扰信号识别的研究也越来越多。文献[3]利用基于特征的模式识别方法，选取了时域特征和频域特征分别进行识别，然后通过D-S证据理论融合的方法将时域特征和频域特征的识别结果进行综合，过程比较复杂。文献[4]使用支持向量机的方法对干扰信号的时频特征进行识别，识别精度较低。文献[5]提出了一种决策树自动化设计方法，降低了决策树的复杂度，但没有分析在低干噪比的情况。

针对上述的一些问题，为了提高识别精度，简化识别流程，本文提出了一种基于卷积神经网络和STFT时频分析的识别方法。首先对典型的4种干扰信号和BPSK通信信号进行时频分析得到时频图像，然后采用卷积神经网络实现对时频图像特征的自动提取，从而完成分类识别。

1 干扰信号与通信信号

通信干扰信号可分为压制性干扰和欺骗性干扰，本文对压制性干扰中的4种典型干扰信号和BPSK通信信号进行研究识别。当存在干扰信号时，通信系统接收到的信号为通信信号、干扰信号和信道噪声三者的叠加。

PSK信号利用载波的相位变化来传递信息。在BPSK中，通常用初始相位0和π分别表示二进制“1”和“0”。

（1）线性调频干扰（Linear Frequency-Modulated Interference, LFM）在一个连续的频带上阻碍有用的通信和信号检测，LFM信号的频率随着时间的变化而线性变化。

（2）连续波干扰又称为单音干扰（Single-tone interference, ST），在某个频点发射信号，阻碍通信和信号检测，是一个连续正弦波。

（3）多音干扰（Multitone interference, MT）在几个特定的频点发射信号，阻碍通信和信号检测。

（4）噪声调频干扰（Frequency-modulated Interference, FM）信号以噪声为调制信号对载波信号进行调频调制，使载波信号的幅度不变，频率随基带噪声随机变化。

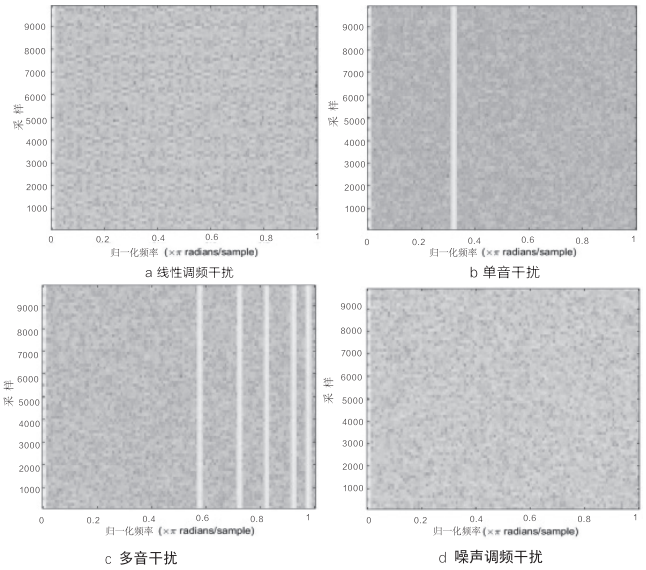
2 短时傅里叶变换

短时傅里叶变换（Short-Time Fourier Transform, STFT）是一种针对时变非平稳信号的时频分析方法[6]，其数学表达式为

$$\mathrm{STFT}_X(t,\omega)=\int_{-\infty}^{+\infty}X(t)g(t-\tau)\mathrm{e}^{-\mathrm{j}\omega t}\mathrm{d}t \qquad (1)$$

式中，$X(t)$是时域信号；$g(t-\tau)$为分析窗函数，其作用是取出$X(t)$在某时刻τ附近的一小段信号进行傅里叶变换值。当τ变化时，窗函数随τ移动，从而得到信号频谱随时间变化，这些不同时刻的傅里叶变换值之和就是$\mathrm{STFT}_X(t,\omega)$，也就是信号的时间频谱图。

选取Hamming窗作为窗函数，设置信干噪比为10 dB，利用STFT对干扰信号、通信信号和信道噪声三者的叠加信号进行时频分析，时频图如图1所示。



a 线性调频干扰　b 单音干扰　c 多音干扰　d 噪声调频干扰

图1 四类干扰信号的时频图

3 卷积神经网络模型

卷积神经网络一般由输入层、卷积层、池化层、全连接层和输出层组成[7]。卷积神经网络能够成功应用于图像识别的主要原因在于它的三个结构特点：局部连接、下采样和权值共享。这三个特点使得卷积神经网络既解决了全连接层训练时间长、计算量大的问题，又保证了特征识别的准确性。图2是本文应用于干扰识别的卷积神经网络模型。

卷积层：利用卷积核提取图像特征，卷积核在图像中逐像素移动。卷积层的输出经过激活函数的作用后称为特征图。不同的卷积核提取不同的输入图像特征，卷积层的操作表示为

$$Z_n^l=f\Big(\sum_{m\in M_n}Z_m^{l-1}\otimes K_{mn}^l+b_n^l\Big) \qquad (2)$$

式中，$f(\cdot)$是非线性激活函数，本文使用的是ReLU激活函数，$\mathrm{ReLU}(x)=\begin{cases}0 & x<0\\ x & x\geqslant 0\end{cases}$，采用ReLU函数不仅计算比较简单，而且一定程度上缓解了梯度消失的问题[8]；Z_m^{l-1}为卷积神经网络第l-1层的第m个输入特征映射；K_{mn}^l是一个三维卷积核；b_n^l为第l层的每个输出对应的偏置。

池化层：使用最大池化可以降低卷积层对位置的敏感性，同时降低对空间采样表示的敏感性，保留更详细的图像特征信息。同时，避免了平均池化带来的模糊特征。

Dropout层：在深度学习的过程中，容易出现模型参数过多、训练样本不足的情况。Dropout模块通过丢弃部分神经元，使得某些隐层节点的值为零，减少了隐

层节点的相互作用，从而防止了过拟合的发生，增强了模型的泛化能力[9]。

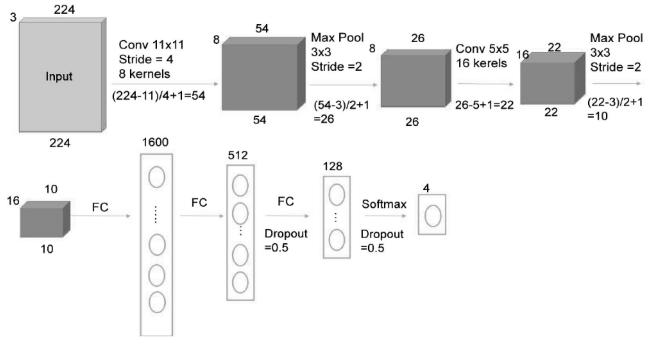


图2 用于干扰识别的神经网络模型

4 实验仿真与结果分析

4.1 数据集的生成

本文是对四类干扰信号进行识别，由于在实际生活中，对干扰信号的采集比较困难，这里采用MATLAB仿真生成干扰信号和通信信号，并对其两者的叠加信号进行STFT时频分析，从而得到时频图像。模型的输入数据为

$$y(t)=x(t)+j(t)+g(t) \tag{3}$$

式中，$x(t)$为BPSK通信信号；$j(t)$为干扰信号；$g(t)$为高斯白噪声；$y(t)$是要进行STFT时频分析的信号。

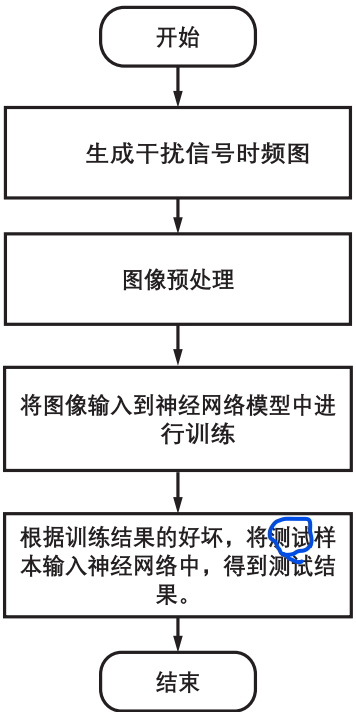


图3 实验流程图

这4类干扰信号和通信信号的叠加信号在信干噪比[-10 dB,10 dB]内每间隔5 dB生成训练数据和测试数据，在每种信干噪比下生成500张图片，一共有4×5×500个样本，其中90%为训练数据，10%为训练数据。

仿真参数设置如下：线性扫频干扰的初始频率为（10 kHz, 20 kHz），调频率为（10 GHz, 100 GHz）。单音干扰的频率范围为（10 kHz, 20 kHz）。多音干扰的频率范围为（10 kHz, 20 kHz），音数目为（2, 7）。噪声调频干扰的中心频率为20 MHz，噪声有效带宽为（50 MHz, 100 MHz）调频斜率为（100 MHz, 200 MHz）。

4.2 实验流程

本文首先生成干扰信号和通信信号，将两者叠加后加入高斯白噪声，得到待处理的信号，然后使用STFT对信号进行时频分析，得到时频图像，调整图片大小为224×224并送入神经网络模型中，具体实现过程如图3所示。

4.3 实验结果及分析

根据仿真结果，可以得到各类干扰信号的识别率。图4是信干噪比为[-10 dB, 10 dB]的混淆矩阵图，矩阵显示的百分比为混淆矩阵的召回率。可以看到单音干扰被识别为线性扫频干扰的数量相对比较多一些，这是因为这两者的时频图具有一定的相似性。

图5是信干噪比为[0 dB, 10 dB]的混淆矩阵图，相比较于图4，识别率有所上升。因此，可以知道信干噪比越高即信道噪声越小，干扰信号的特征就越容易被神经网络识别，识别的概率随着增大。

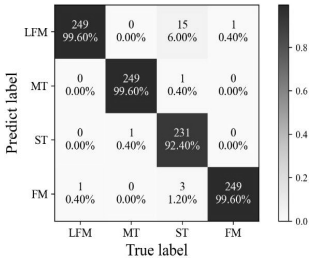


图4 测试集的混淆矩阵

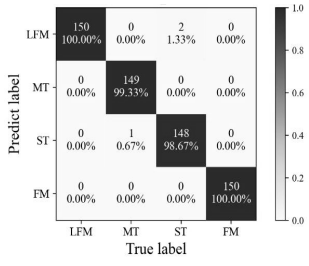


图5 [0 dB,10 dB]测试集的混淆矩阵

5 结束语

鉴于传统干扰信号识别方法比较复杂，并且识别效果不好，本文使用一种利用卷积神经网络和STFT时频分析的方法对几种常见的通信干扰信号进行识别分类。仿真结果表明，该方法对这4种通信干扰信号都具有较高的识别率，在信干噪比为[-10 dB,10 dB]范围内的综合识别率可达到97.8%，在信干噪比为[0 dB,10 dB]范围内的综合识别率为99.5%。与传统的识别方法相比此方法实现比较简单，并且识别率高。只是神经网络模型参数比较多，运算比较复杂，要用在实际工程中存在不少难题，同时，本文也没有对复合干扰信号进行识别，这些问题需要进一步研究。■

（下转第64页）

①威胁分类。网络威胁的常用手段包括分布式拒绝服务攻击、恶意软件、木马病毒、钓鱼邮件等。按照安全类型进行分类可分为3类，即恶意软件、网络攻击以及HTTP攻击。通过对其进行分类处理，显著提升了系统识别的效率和准确率。

②威胁汇总。实际情况下，不同传感器节点存在着是由同一攻击引发的可能性，这就需要对威胁进行汇总处理，首先是对攻击信息进行合并处理，以减小后续工作量，优化处理流程。

（4）规则生成。网络攻击防御系统会自动生成一个规则集，其中规定了对不同种类威胁的处置措施，值得注意的是，通过一些由于系统漏洞引发的网络攻击难以通过软件来拦截处理，针对该情形，需要特殊处置。

2.3 大数据网络防御系统核心功能设计

（1）数据采集与上报。在系统处于非正常运行状态下进行的检测，通常利用一些命令对系统当下运行状况作出分析、统计、处理、汇总，或者采用相应的监控操作进行探测，例如，使用vmatat命令来检测系统内存使用情况，利用bomon进行系统网络宽带占用情况的检查等。系统在对日志进行分析、分类处置后，会将这些日志存入临时文件夹内，等待下一步的处理。

（2）规则生成与部署系统。首先对规则进行分类并委托给相应的线程去处理。例如，针对恶意软件攻击的威胁会分发给恶意软件威胁的线程进行处理。该方式的有益效果是既保证了内存warm，又保证了系统处理的时效性，提高了运行效率。系统中的所有类型的规则都被存入数据库中的不同列表内，可通过SQL语句进行查询。

3 网络攻击防御系统测试与验证

为了验证本文开发的防御系统的可靠性与实用性，笔者对开发系统进行了测试与验证。选择CentOS 6.5服务器系统环境对系统进行测试，测试流程依据OpenStack文件严格执行，在该环境中重点测试系统的网络性能，该过程重点测试当服务器中的任意一台主机遭到恶意攻击时，可利用本文设计的大数据分析网络防御系统进行有利防护。另外，应用OpenStack作为实验环境，建立小型的测试平台实现对大数据网络攻击防御系统的测试与验证，测试工具主要选用Wireshark抓包、iptables防火墙以及bmon监测工具，测试验证结果表明，本文设计开发的大数据网络攻击防御系统软件对网络攻击防御效果显著，具有实际推广应用价值。

4 结束语

随着计算机技术、大数据技术及云计算等技术的高速发展，网络攻击渠道也不断增多，攻击方式也日趋多样化，感染的速度也更快，网络安全问题日益突出，亟须利用有效的防御系统阻止网络攻击行为的发生及危害的进一步扩大。一直以来，远程网络攻击防御系统的设计与开发是一项关键内容，利用大数据分析技术本文开发的防御系统应用效果良好，具有一定的实际应用价值。■

参考文献

[1] 朱海鹏，赵磊，秦昆，等．基于大数据分析的电力监控网络安全主动防护策略研究[J]．电测与仪表，2020,57(21):133-139.
[2] 马浩．基于大数据的网络安全防御系统研究与设计[J]．网络安全技术与应用，2019(4): 52-53.
[3] 任恒妮．大数据时代计算机网络安全防御系统设计研究分析[J]．电子设计工程，2018,26(12): 59-63.
[4] 冯贵兰，李正楠，周文刚．大数据分析技术在网络领域中的研究综述[J]．计算机科学，2019,46(6):1-20.
[5] 孙护军．基于大数据分析的增强型网络文档分类模型[J]．计算机工程与设计，2019,40(3):755-761.

（上接第61页）

参考文献

[1] 赵国庆．雷达对抗原理[M]．西安：西安电子科技大学出版社，2012.
[2] Cong X, Zhang P, Han Y. A jamming identification method based on deep learning for networking radars[C]//2021 2nd International Symposium on Computer Engineering and Intelligent Communications (ISCEIC). IEEE, 2021: 352-256.
[3] 袁冠杰，王虹，陈静，等．基于特征提取融合判决的卫星干扰识别算法[J]．微波学报，2021, 37(S01): 241-244.
[4] 李宝鹏、彭志刚、高伟亮．基于时频特性分析的雷达压制干扰信号识别[J]．电光与控制，2020, 27(9): 14-18.
[5] 魏煜宁，张劲东，李勇，等．雷达干扰信号识别决策树的自动化设计方法[J]．电光与控制，2020, 27(4): 82-86.
[6] Durak, Lütfiye, Arikan, et al. Short-Time Fourier Transform: Two Fundamental Properties and an Optimal Implementation[J]. IEEE Transactions on Signal Processing, 2003, 51(5): 1231-1242.
[7] 邱锡鹏．神经网络与深度学习[M]．北京：机械工业出版社，2020.
[8] Glorot X, Bordes A, Bengio Y. Deep sparse rectifier neural networks[C]. Proceedings of the fourteenth international conference on artificial intelligence and statistics. JMLR Workshop and Conference Proceedings, 2011: 315-323.
[9] Hinton G E, Srivastava N, Krizhevsky A, et al. Improving neural networks by preventing co-adaptation of feature detectors[J]. arXiv preprint, 2012: 1207.0580.