



·电磁频谱作战与电磁安全·

基于融合特征的泄漏信号分类识别方法*

寇云峰¹, 戴 飞², 赵治国³, 吕剑明¹, 马 谢¹

(1. 成都新欣神风电子科技有限公司, 成都 611731; 2. 北京航空航天大学, 北京 100083; 3. 中国电子科技网络信息安全有限公司, 成都 610041)

摘 要: 随着移动通信、物联网、车联网、工业互联网等网络的发展, 电磁环境日益复杂, 非法电子设备也日渐增多, 各类信号耦合互调现象严重, 这给泄漏信号类型识别带来了难题。提出基于融合特征的泄漏信号分类识别方法, 综合运用高维度特征提取方法和图形化降维表征方法, 结合残差网络等深度学习模型与特征融合分析方法, 能够更综合地区分多类电磁泄漏信号, 特征抗噪声鲁棒性高, 方法可解释性好, 可支撑基于电磁信号类型识别的辐射源智能检测工程应用。

关键词: 电磁辐射; 泄漏信号; 信号识别; 特征提取; 智能检测

中图分类号: TN924; TP181

文献标志码: A

doi: 10.11884/HPLPB202436.230186

Leakage signal classification and recognition method based on fusion features

Kou Yunfeng¹, Dai Fei², Zhao Zhiguo³, Lü Jianming¹, Ma Xie¹

(1. Chengdu Xinxinshenfeng Electronics Co, Ltd, Chengdu 611731, China;

2. Beihang University, Beijing 100083, China;

3. China Electronics Technology Cyber Security Co., Ltd, Chengdu 610041, China)

Abstract: With the development of networks such as mobile communications, Internet of Things (IoT), V2X (meaning Vehicle to everything, including Vehicle to Vehicle and Vehicle to Infrastructure), and Industrial Internet of Things (IIoT), the electromagnetic environment is becoming increasingly complex, illegal electronic devices are also increasing day by day, and there are severe coupling and intermodulation of various signals, which bring difficulties to the identification of leaked signal types. This paper proposes a leakage signal classification and recognition method based on fused features. Comprehensively utilizing high-dimensional feature extraction methods and graphical dimensionality reduction characterization methods, and combining with deep learning models such as residual networks and feature fusion analysis methods, the method can distinguish more comprehensively multiple types of electromagnetic leakage signals. The features method has with high robustness against noise and good interpretability, and can support the intelligent detection engineering application of radiation sources based on electromagnetic signal type recognition.

Key words: electromagnetic radiation, leakage signal, feature extraction, classification recognition, intelligent detection

随着移动通信、物联网、车联网、工业互联网等网络的发展, 一方面, 电磁环境日益复杂, 计算机系统的微弱电磁辐射泄漏隐藏在各类无线发射中, 难以发现; 第二, 基于信号互调等新的携带方式的出现, 使得泄漏发射与无线发射互相耦合, 传播距离远且难以识别; 第三, 处理芯片、射频芯片的集成化和微型化, 容易被非法电子窃听设备利用, 构建发送、接收或是转发、组网的高隐蔽通道。因此, 对目标设备、处理器、接口等无意辐射泄漏信号进行分析, 实现泄漏信号识别的方法, 对保障关键信息基础设施以及维护国家网络空间安全都具有重要意义。

文献 [1-3] 通过主动激发等主动检测方法, 系统分析了泄漏信号的辐射源和传播通道等特性, 可以有效地提升泄漏信号的可解释性, 但没有具体提出识别方法。文献 [4] 基于电力线信号样本采集, 提出了服务器、台式机、手机、板卡、线路背景等信号类型的区分方法并进行了验证, 但因为其采用的图像是低维度的频谱灰度图, 因此基于特征的识别容易受到信号采集位置、设备间干扰的影响。文献 [5] 提出针对泄漏信号的机器学习方法, 但其只对显示器进行了分析。文献 [6] 侧重于基于电磁泄漏信号检测的信息设备信息泄漏威胁距离评估方法, 文献 [7-9] 提

* 收稿日期: 2023-06-19; 修订日期: 2023-09-21
联系方式: 寇云峰, 4156512@qq.com

出了不同板卡、恶意软件等电磁泄漏信号特征,并提取了基于深度学习的识别方法。文献[10-15]从泄漏信息的不同物理信号类型层面进行了分析,但解析方法尚不统一。

为了充分提取与利用信号特征并结合数学化、图形化特征的可解释性,同时利用深度学习的深度提取与分类能力,可以结合这些特点,提出更为综合的识别方法。本文基于高维特征提取与图形可视化降维呈现,提出了基于深度残差网络 ResNet18 模型的初级分类识别和基于多个特征的融合分析方法,采集了五类典型泄漏与环境信号并构建了信号样本集,然后通过不同噪声强度下的结果进行对比分析,同时与三种单特征模型的预测准确率结果进行对比。结合特征图呈现与混淆矩阵结果可以分析得出:造成误识别的原因是因为信号具有相似特征;双谱特征对本文分析的几种信号具有较高的区分度,对融合模型具有较大的贡献。

1 算法模型

1.1 模型架构

该方法的特征提取过程采用了小波变换(WT)、Hilbert-Huang 变换(HHT)和双谱分析的方法,这些方法可以提取信号的时频信息和非线性特征。具体而言,小波变换可以将信号分解成多个频带,每个频带中的信号具有不同的尺度和频率特征;HHT 则可以将信号分解成多个固有模态函数,这些函数可以反映信号的非线性特征;双谱分析则可以分析信号的相位关系,进一步提取信号的非线性特征。通过这些特征提取方法,生成对应的二维投影特征图,并使用了初级分类器为深度残差网络的融合特征双阶段分类识别方法。

该算法的流程图如图 1 所示:

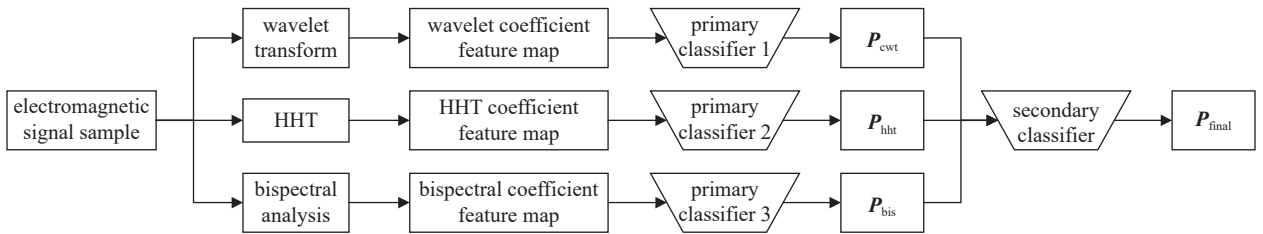


Fig. 1 Algorithm flowchart

图 1 算法流程图

第一步,对电磁信号样本进行三通道变换,生成系数矩阵的三维图像,然后将这些图像投影到适当的二维平面上,得到三通道的投影图片特征。这些特征包含了信号的时频信息和非线性特征,可以更准确地反映信号的特点。

第二步,将三通道的图片特征分别输入到三个以 Softmax 为输出层的深度残差网络(即初级分类器,采用 ResNet18 模型)中进行分类识别。深度残差网络采用了残差学习的思想,可以有效地减轻梯度消失问题和网络深度带来的负面影响,进而提高网络的分类性能。每个深度残差网络都以 Softmax 为输出层,可以将输入的特征向量映射为概率分布,分别得到三个以概率表示的特征向量 P_{cwt} 、 P_{hht} 和 P_{bis} 。

第三步,将这三个特征向量的均值作为次级分类器的最终输出,即求它们的均值,得到最终分类预测结果 P_{final} ,可以得到电磁信号的分类识别结果,即

$$P_{final} = (P_{cwt} + P_{bis} + P_{hht})/3 \quad (1)$$

次级分类器是求三个初级分类器的均值,这样可以综合利用三个特征图像的信息,得到更可靠的分类预测结果。

2 特征提取

2.1 基于小波变换的特征图提取

小波变换(WT)通过对时间(空间)频率进行局部化分析,能够凸显信号区域性的细微特征。连续小波变换可定义为

$$C(\text{scale}, \text{position}) = \int_{-\infty}^{\infty} f(t)\psi(\text{scale}, \text{position}, t)dt \quad (2)$$

式中: $\psi(t)$ 是基函数, scale 是缩放因子, position 是平移因子。

该算法选用 Morlet 小波作为基函数,因为 Morlet 小波是常用的复值小波,采集的泄漏信号数据也是复信号。通过对信号进行 Morlet 小波变换,得到小波系数矩阵,然后做出系数矩阵的三维图像,最后将其时间域投影到频域(YZ 平面),得到二维投影特征图,淡化时间维度的影响,突出频率与系数的关系。投影方向及投影后的二维图如图 2

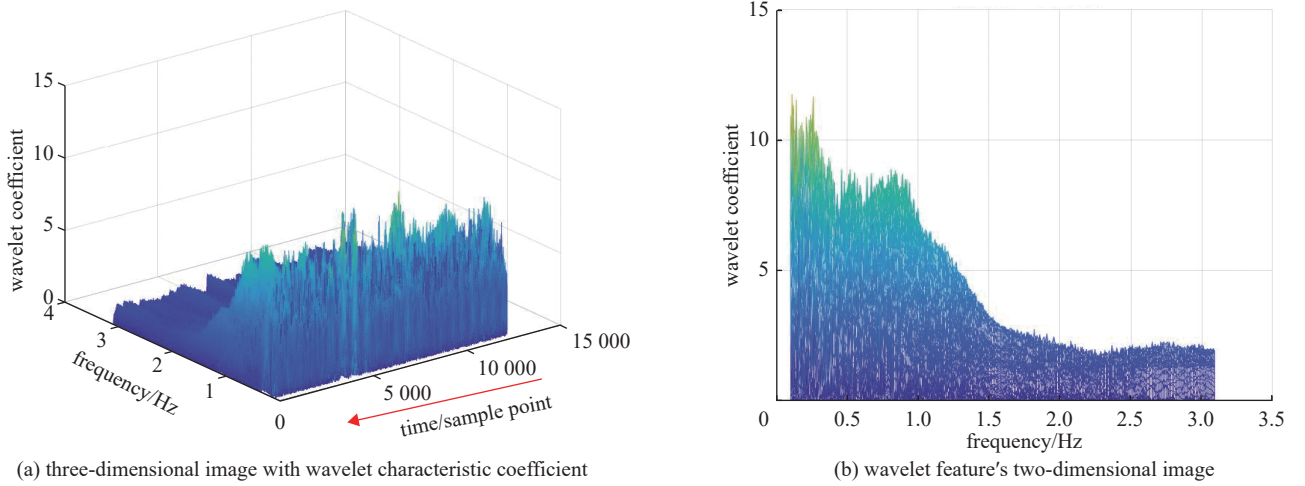


Fig. 2 Wavelet feature projection

图2 小波特征投影图

所示。

2.2 基于 Hilbert-Huang 变换的特征图提取

HHT 相比傅里叶变换和小波变换这类传统方法, 彻底摆脱了线性和平稳性束缚, 更适用于分析非线性非平稳信号。HHT 首先对信号进行经验模态分解(EMD), 得到一系列的本征模态函数 IMF, 然后对 IMFs 进行 Hilbert 变换, 得到 Hilbert 系数矩阵, 该过程可定义为

$$s^k(t) = \sum_{i=1}^n c_i(t) + r_n(t) \quad (3)$$

原始信号 $s^k(t)$ 可以表示为 IMF 分量 $c_i(t)$ 和余项 $r_n(t)$ 的组合, 然后对每个 IMF 分量进行 Hilbert 变换

$$\tilde{c}_i(t) = \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{c_i(\tau)}{t-\tau} d\tau \quad (4)$$

构造解析函数

$$Z_i(t) = c_i(t) + j\tilde{c}_i(t) = a_i(t)\exp(j\phi_i(t)) \quad (5)$$

式中: $a_i(t)$ 、 $\phi_i(t)$ 和 $\omega_i(t)$ 分别表示瞬时振幅、相位和频率, 即

$$a_i(t) = \sqrt{c_i(t)^2 + \tilde{c}_i(t)^2}, \quad \phi_i(t) = \arctan\left(\frac{\tilde{c}_i(t)}{c_i(t)}\right), \quad \omega_i(t) = \frac{d\phi_i(t)}{dt} \quad (6)$$

进而 Hilbert 谱可表示为

$$H(\omega, t) = \text{Re}\left(\sum_{i=1}^n a_i(t)\exp(j\int \omega_i(t)dt)\right) \quad (7)$$

对于特征提取, 首先对信号进行 HHT 变换, 得到 HHT 系数矩阵, 然后做出系数矩阵的三维图像, 最后将其时间域投影到频域(YZ 平面), 得到二维投影特征图, 淡化时间维度的影响, 突出频率与系数的关系。投影方向及投影后的二维图如图 3 所示。

2.3 基于双谱变换的特征图提取

通过双谱变换, 能够有效地抑制一定数量的高斯噪声, 使泄漏源噪声充分反映在双谱信息中。双谱变换的定义为

$$B(\omega_1, \omega_2) = \sum_{\tau_1=-\infty}^{\infty} \sum_{\tau_2=-\infty}^{\infty} c_{3x}(\tau_1, \tau_2) \exp[-j2\pi(\omega_1\tau_1 + \omega_2\tau_2)] \quad (8)$$

式中: $c_{3x}(\tau_1, \tau_2) = E\{x^*(t)x(t+\tau_1)x(t+\tau_2)\}$ 表示信号的三阶累积量。

首先对信号进行双谱变换, 然后得到双谱系数矩阵, 最后做出系数矩阵的三维图像。由于双谱的特殊对称性, 在两个频率主轴形成的平面上其第一、三象限包含的内容较多, 将其投影到视角 $(-45, 0, 0)$, 得到的三维双谱图像的包含轮廓、纹理特征最多, 且完全对称, 是对两个频率主轴形成的平面上第一、三象限内容的完全体现, 因此选用投影视角 $(-45, 0, 0)$ 表征的双谱特征最完备。投影方向及投影后的二维图如图 4 所示。

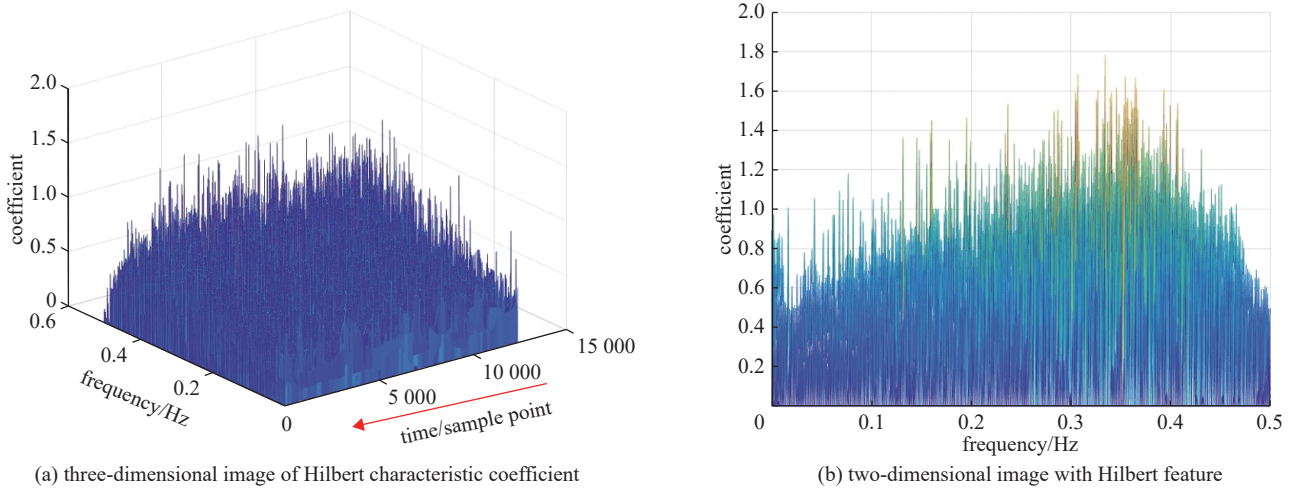


Fig. 3 Hilbert characteristic projection map
图 3 Hilbert 特征投影图

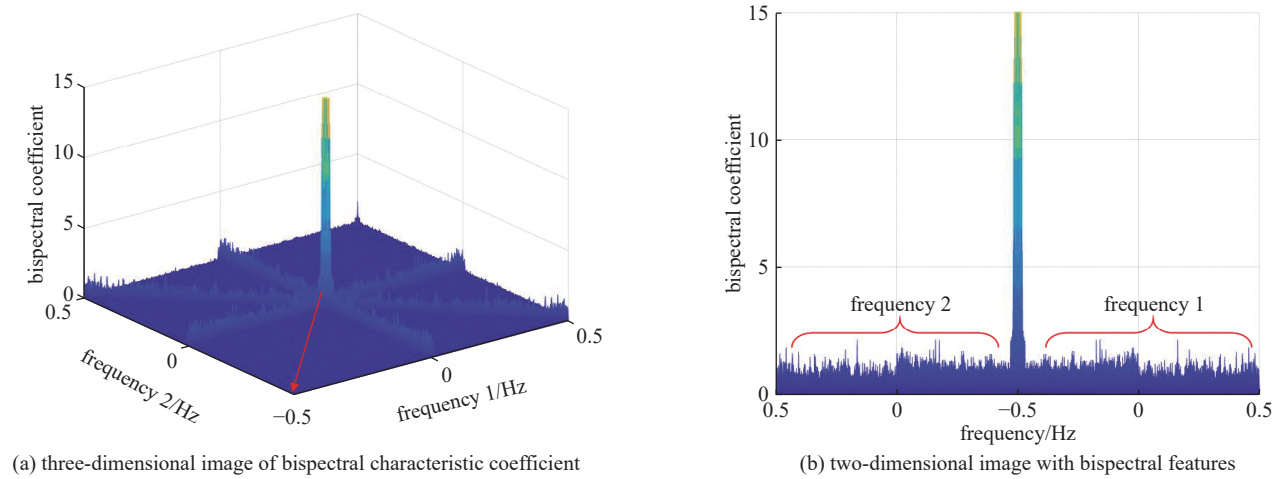


Fig. 4 Bispectral feature projection maps
图 4 双谱特征投影图

3 数据样本与特征提取结果

3.1 样本采集

测试所使用的数据集为自建的数据集,包含了五个不同的泄漏源,分别是时钟泄漏信号、笔记本触摸板泄漏信号、环境无线发射信号、屏幕显示信号以及未知辐射源信号。使用 RTL SDR 贴近联想 X230 笔记本或是监测无线环境来接收并存储到计算机中。每个泄漏源采集三到五条不等的 WAV 格式的 IQ 数据,每个 WAV 文件的采集时间为 10 s 到 20 s 不等。为了进行样本截取,采用了等距划分的方法,将每个 WAV 数据划分成 20 000 个采样点的小样本。根据这种方法,获得了每个泄漏源的一定数量的样本,如表 1 所示,其中五类泄漏源进行分别编号 1#~5#。

表 1 五类泄漏源

Table 1 Five types of leakage sources

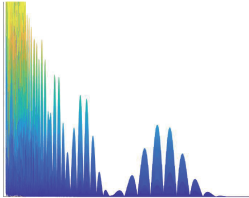
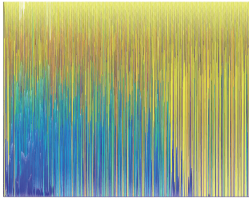
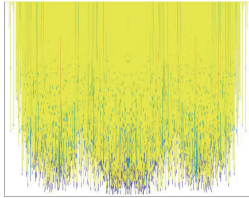
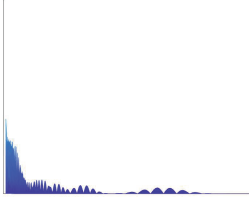
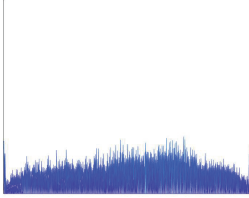
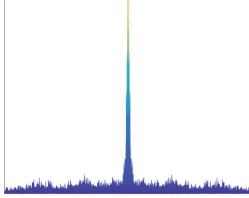
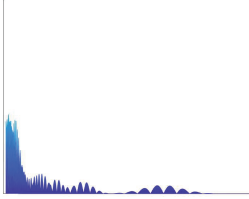
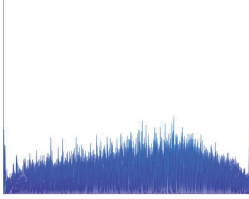
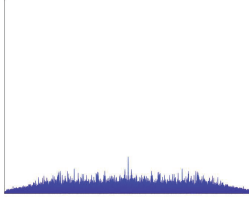
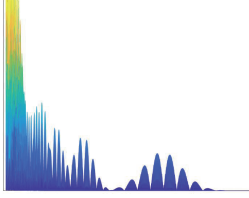
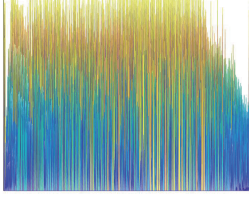
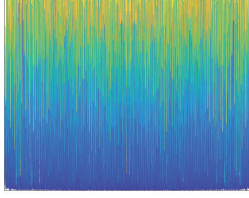
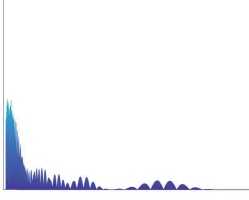
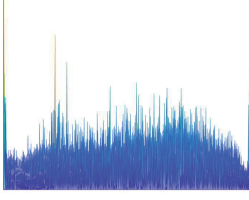
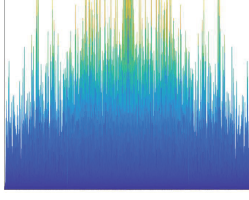
No.	signal type	total sampling points of each WAV file	number of samples intercepted by each WAV file	total number of samples taken
1	clock leak signal	11 264 000, 10 035 200, 7 168 000, 7 782 400	563, 501, 358, 389	1811
2	laptop touchpad leak signal	12 247 040, 15 589 376, 17 924 096, 21 274 624	612, 779, 896, 1 063	3 350
3	environmental radio emissions signal	17 981 440, 22 003 712, 25 976 832, 25 075 712, 15 302 656	899, 1 100, 1 298, 1 253, 765	5 315
4	screen display signal	21 553 152, 34 586 624, 26 722 304	1 077, 1 729, 1 336	4 142
5	unknown radiation source signal	15 728 640, 17 661 952, 26 402 816, 16 826 368	786, 883, 1 320, 841	3 830

3.2 特征提取结果

使用仿真软件中的 `cwt`、`hhspectrum`、`bispecd` 等函数, 对五类泄漏信号进行特征提取, 各类信号分别选择一个样本, 特征图如表 2 所示。可以直观地看出, 2#、3#、5# 的小波特征图和 HHT 特征图较为相似, 这是因为笔记本触摸板泄漏信号是一种耦合调制泄漏, 其与环境无线发射信号、未知辐射源信号相似, 三类信号都可看作是带宽、调制等特征近似的无线发射信号; 但是 1#~5# 五类泄漏信号提取出的高阶谱特征差异则较大, 基于高阶谱特征能够很好地区分五类信号。

表 2 五类泄漏源特征

Table 2 Five types of leak source characteristics

No.	signal type	wavelet feature map	HHT feature map	bispectral feature map
1	clock leak signal			
2	laptop touchpad leak signal			
3	environmental radio emissions signal			
4	screen display signal			
5	unknown radiation source signal			

4 识别验证

4.1 均衡数据集和非均衡数据集对比测试

由于提取的特征图均为彩色图像, 此处将 RGB 图像转为灰度图, 压缩至 224×224 后再送入网络进行分类识别。其中, 训练集和测试集的划分为 8:2; 优化器选用 Adagrad, 学习率为 0.001, L2 惩罚为 0.0005。

考虑到实际应用中每类的样本数量会不均衡, 所以采用了均衡数据集和非均衡数据集两种方案进行对比测

试。五个类别,均衡数据集每类选取相同数量的 1 800 条样本,共 9 000 条样本;非均衡数据集每类根据实际数量选择样本数。具体样本数量设置如表 3 所示。

表 3 五类泄漏源样本数据集数量

Table 3 Number of sample data sets of five types of leakage sources

No.	signal type	balanced dataset sample size		unbalanced dataset sample size	
		training set	test set	training set	test set
1	clock leak signal	1 440	360	1 449	362
2	laptop touchpad leak signal	1 440	360	2 680	670
3	environmental radio emissions signal	1 440	360	4 252	1 063
4	screen display signal	1 440	360	3 313	829
5	unknown radiation source signal	1 440	360	3 064	766

均衡数据集测试结果表明,均衡数据集在训练一轮后,训练集准确率 96.88%,测试集准确率 100%。这说明特征易于识别,所以能够快速收敛;但另一方面训练集和测试集样本不太均匀,测试集比训练集的准确率还要高。

非均衡数据集测试结果表明,在训练一轮后,训练集准确率 94.74%,测试集准确率 97.17%。在训练五轮后,训练集准确率 100%,测试集准确率 100%。这一方面说明非均衡数据集比均衡数据集收敛要慢,需要更多的迭代训练轮数。

4.2 加噪测试

因为对泄漏信号为贴近被测对象进行采集,信噪比(SNR)较高。为考察距离、电磁背景环境等对测试结果的影响,以及不同泄漏信号之间的相似性,对数据样本进行加噪对比测试。每类选取 500 条样本,用仿真软件中的 awgn 函数添加 SNR 为 0、3、5、7 dB 的噪声,各类信噪比分别进行训练,每类信噪比下五种信号的训练集样本数量为 400,测试集样本数量为 100。每种信噪比下的模型训练采用统一参数: max_epoch=50, lr=1×10⁻⁴, weight_decay=5×10⁻⁴。融合特征与单特征的结果进行对比如表 4 所示。从表中可以看出,融合特征在各种信噪比下具有较强的预测准确率,双谱特征对预测准确率具有较大的贡献,小波特征和 HHT 特征在低信噪比时有一定的误识别率。如果只是基于小波特征图来预测,噪声对预测准确率影响波动较大;如果只是基于 HHT 特征图来预测,则信噪比对预测准确率影响呈正相关;如果只是基于双谱特征图来预测,则预测准确率为 100%。

表 4 不同信噪比下的不同特征图预测准确率

Table 4 Prediction accuracy of different feature maps under different signal-to-noise ratios

No.	SNR/dB	fusion feature map/%	wavelet feature map/%	HHT feature map/%	bispectral feature map/%
1	0	99.8	95.8	95.2	100
2	3	100	98.4	97.8	100
3	5	100	93.6	98.8	100
4	7	100	93.0	99.8	100

采用融合特征时的预测结果混淆矩阵如图 5 所示。从图中可以看出,有一个 2#信号样本被预测成了 3#信号。

不同信噪比时,基于小波特征图的预测结果如图 6 所示。从图中可以看出,采用小波特征图来预测时,2#、3#、5#泄漏源样本互相之间区分难,有较多的误识别。

不同信噪比时,基于 HHT 特征图的预测结果如图 7 所示。从图中可以看出,采用 HHT 特征图来预测时,2#、3#、5#泄漏源样本互相比较难区分,有较多的误识别,信噪比越低越难预测。

测试进一步说明了,在不具备使用哪种特征能够更好地区分泄漏源等先验信息时,使用融合特征能够综合各种特征对预测准确率的贡献。

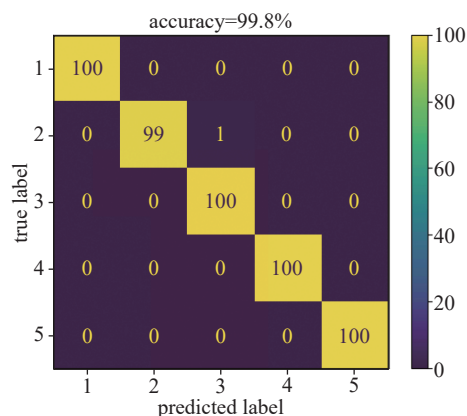


Fig. 5 Confusion matrix of prediction results based on fusion features when the signal-to-noise ratio is 0 dB

图 5 信噪比为 0 dB 时基于融合特征的预测结果混淆矩阵

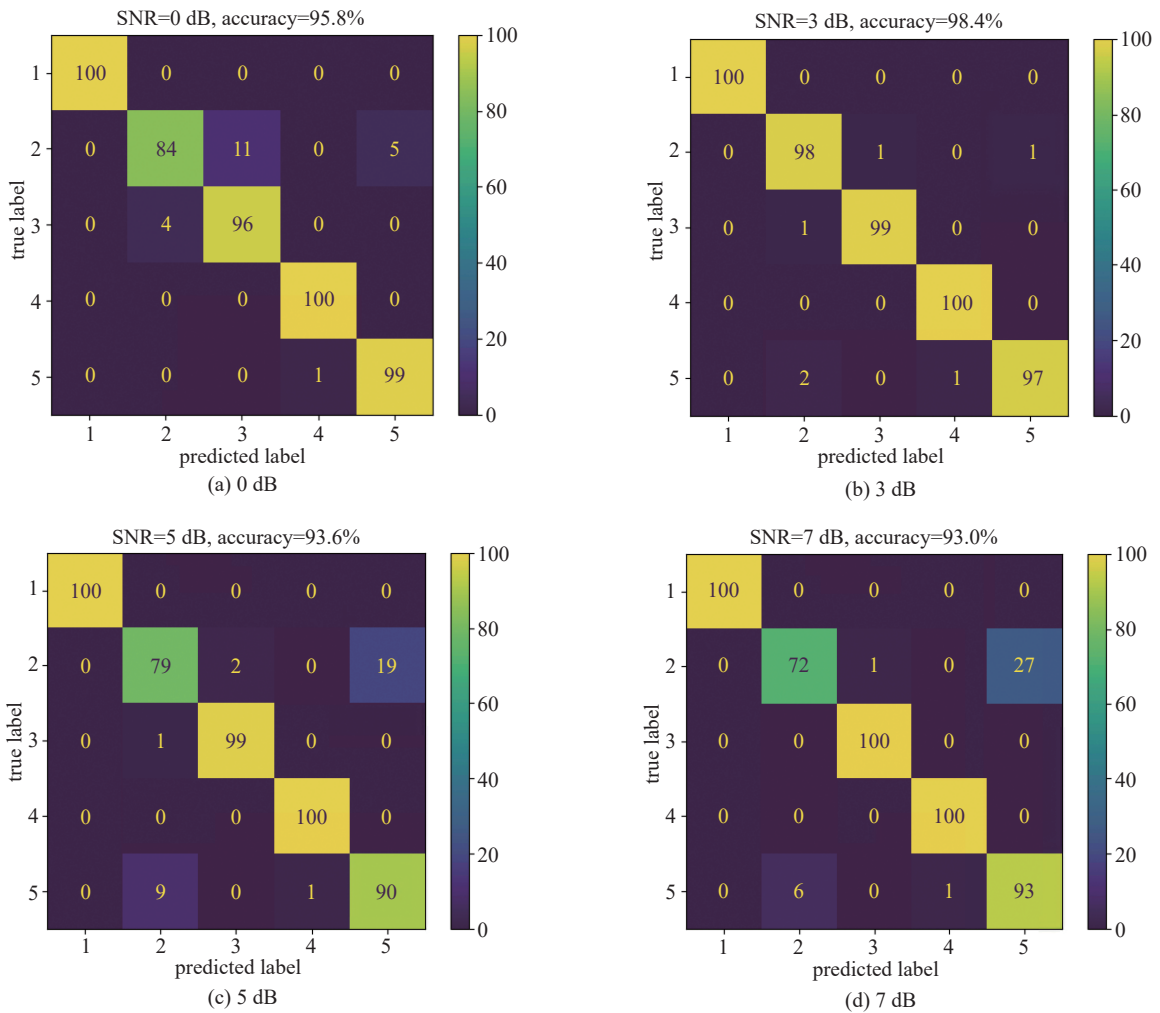
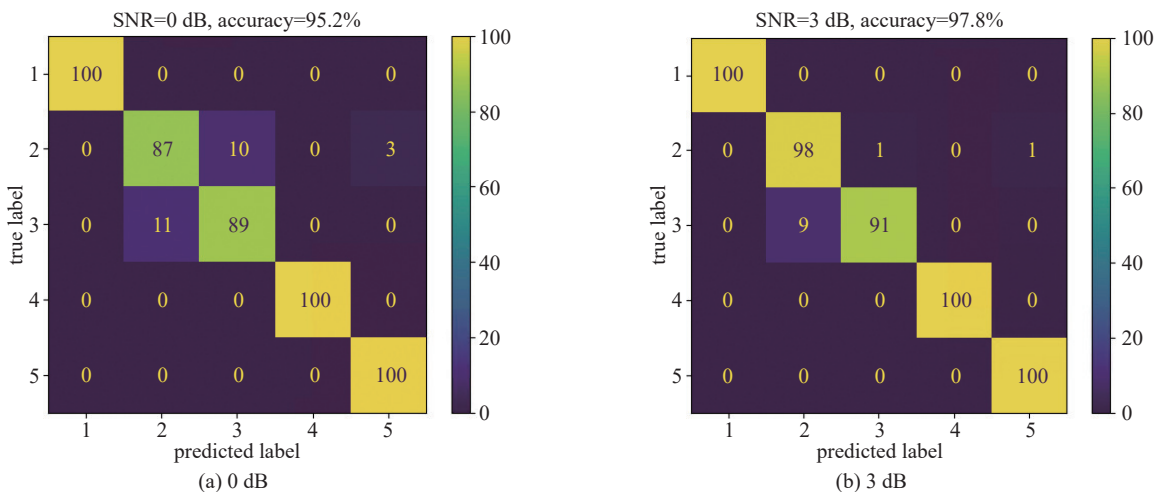


Fig. 6 Confusion matrix of prediction results based on wavelet features at different signal-to-noise ratios

图 6 不同信噪比时基于小波特征的预测结果混淆矩阵

5 结论

本文提出的基于融合特征的泄漏信号分类识别方法,综合运用了多种高维度特征提取方法和深度学习技术,测试结果表明,该方法能够更综合地区分多类电磁泄漏信号,特征抗噪声鲁棒性高,能适应复杂的电磁环境场景,且基于图形化方式表征的特征可解释性强,具有较高的工程应用价值。后续将进一步开展验证,丰富信号类型的多样性,并推动泄漏信号类型的实时检测。



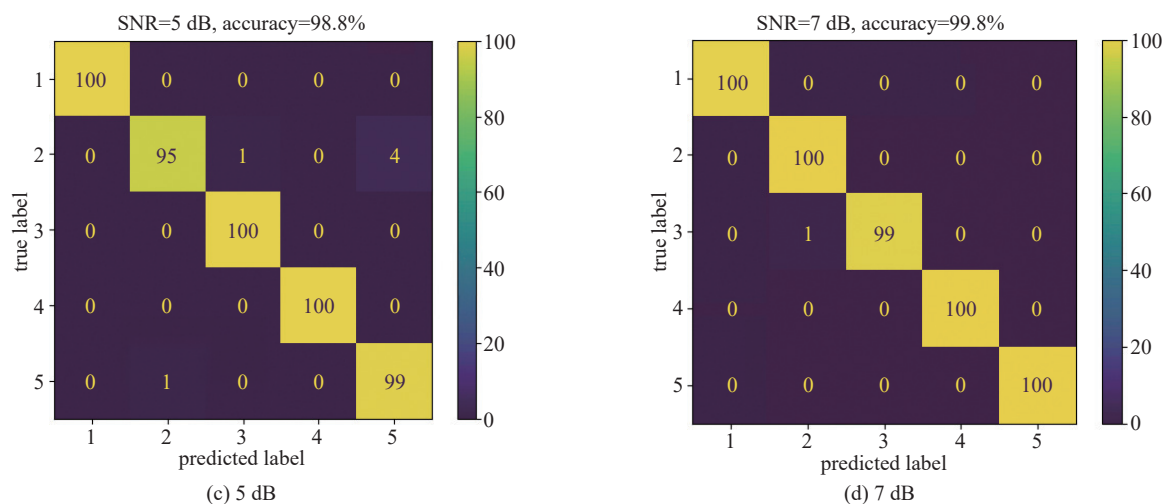


Fig. 7 Confusion matrix of prediction results based on HHT features at different signal-to-noise ratios

图 7 不同信噪比时基于 HHT 特征的预测结果混淆矩阵

参考文献:

- [1] 刘文斌, 丁建锋, 寇云峰, 等. 物理隔离网络电磁漏洞研究[J]. *强激光与粒子束*, 2019, 31: 103215. (Liu Wenbin, Ding Jianfeng, Kou Yunfeng, et al. Research on electromagnetic vulnerability of air-gapped network[J]. *High Power Laser and Particle Beams*, 2019, 31: 103215)
- [2] 刘文斌, 王梦寒, 寇云峰, 等. 基于电磁泄漏信号的设备行为识别与安全应用[J]. *通信技术*, 2019, 52(7): 1761-1765. (Liu Wenbin, Wang Menghan, Kou Yunfeng, et al. Behavior recognition and security application of electronic equipment based on electromagnetic leakage signal[J]. *Communications Technology*, 2019, 52(7): 1761-1765)
- [3] 刘文斌, 丁建锋, 寇云峰, 等. 软件定义电磁泄漏技术与应用分析[J]. *通信技术*, 2017, 50(9): 2094-2099. (Liu Wenbin, Ding Jianfeng, Kou Yunfeng, et al. Software-defined electromagnetic leakage technology and its application[J]. *Communications Technology*, 2017, 50(9): 2094-2099)
- [4] 王梦寒, 寇云峰, 刘文斌, 等. 计算机网络电磁泄漏信号的实时监测与智能识别[J]. *通信技术*, 2019, 52(7): 1755-1760. (Wang Menghan, Kou Yunfeng, Liu Wenbin, et al. Real-time monitoring and intelligent recognition of electromagnetic leakage signals in computer networks[J]. *Communications Technology*, 2019, 52(7): 1755-1760)
- [5] 关天敏, 韩振中, 茅剑. 显示器电磁信息泄漏的机器学习检测方法研究[J]. *信息安全学报*, 2021, 6(2): 101-109. (Guan Tianmin, Han Zhenzhong, Mao Jian. Research on the detection method of electromagnetic information leakage from display by machine learning[J]. *Journal of Cyber Security*, 2021, 6(2): 101-109)
- [6] 徐艳云, 张萌, 黄伟庆. 信息设备电磁辐射信息泄漏的可检测距离估计方法研究[J]. *信息安全学报*, 2020, 5(1): 44-56. (Xu Yanyun, Zhang Meng, Huang Weiqing. Study on detectable distance for electromagnetic information leakage of information equipment[J]. *Journal of Cyber Security*, 2020, 5(1): 44-56)
- [7] Sehatbakhsh N, Nazari A, Alam M, et al. REMOTE: robust external malware detection framework by using electromagnetic signals[J]. *IEEE Transactions on Computers*, 2020, 69(3): 312-326.
- [8] Werner F T, Yilmaz B B, Prvulovic M, et al. Leveraging EM side-channels for recognizing components on a motherboard[J]. *IEEE Transactions on Electromagnetic Compatibility*, 2021, 63(2): 502-515.
- [9] Jorgensen E J, Werner F T, Prvulovic M, et al. Deep learning classification of motherboard components by leveraging EM side-channel signals[J]. *Journal of Hardware and Systems Security*, 2021, 5(2): 114-126.
- [10] 丁建锋, 刘文斌, 丁磊, 等. 基于主动检测的电子设备电磁信息泄漏新型威胁分析[J]. *通信技术*, 2018, 51(4): 936-940. (Ding Jianfeng, Liu Wenbin, Ding Lei, et al. New threat analysis of electromagnetic information leakage in electronic equipment based on active detection[J]. *Communications Technology*, 2018, 51(4): 936-940)
- [11] 丁建锋, 刘文斌, 王梦寒, 等. 计算机声光电磁信号互调泄漏威胁分析[J]. *通信技术*, 2019, 52(4): 967-970. (Ding Jianfeng, Liu Wenbin, Wang Menghan, et al. Threat analysis of computer information leakage in intermodulation of acoustic, optical and electromagnetic signals[J]. *Communications Technology*, 2019, 52(4): 967-970)
- [12] 程磊, 罗儒俊, 寇云峰, 等. 基于电源线的传导电磁信息泄漏模型与验证[J]. *通信技术*, 2018, 51(4): 941-946. (Cheng Lei, Luo Rujun, Kou Yunfeng, et al. Verification of conductive electromagnetic information leakage model based on power line[J]. *Communications Technology*, 2018, 51(4): 941-946)
- [13] 齐国雷, 寇云峰, 胡浩, 等. 基于隐蔽声通道的物理隔离计算机信息泄漏研究[J]. *通信技术*, 2018, 51(3): 700-704. (Qi Guolei, Kou Yunfeng, Hu Hao, et al. Information leakage based on acoustic convert channel for air-gapped computers[J]. *Communications Technology*, 2018, 51(3): 700-704)
- [14] 胡浩, 罗儒俊, 齐国雷, 等. 基于LED显示屏的隐蔽光传输通道[J]. *通信技术*, 2018, 51(7): 1689-1693. (Hu Hao, Luo Rujun, Qi Guolei, et al. Covert-optical transmission channel based on LED display[J]. *Communications Technology*, 2018, 51(7): 1689-1693)
- [15] Guri M, Zadov B, Bykhovsky D, et al. PowerHammer: Exfiltrating data from air-gapped computers through power lines[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 1879-1890.