Open-MUSIC:基于度量学习与特征子空间投影的电磁目标开集识别算法

杨 柳,利 强,邵怀宗
(电子科技大学信息与通信工程学院,四川成都 611731)

摘 要: 在越来越复杂的电磁频谱环境中,要想实现对频谱资源的管控,首先要判断发送信号的辐射源是否是己方已知的.针对此问题,本文提出了一种基于计算特征子空间投影比值的算法Open-MUSIC(MUltiple SIgnal Classification),通过神经网络获得已知类特征表示;进而得到已知类特征矩阵的两个正交子空间;以特征在两个子空间内的投影比值为指标,对辐射源信号样本是否为已知做判决.在3个数据集上的仿真表明,Open-MUSIC算法的性能在电磁数据集上较其他方法提升了3%以上.

关键词: 开集识别; 特征子空间分解; 中心损失; 投影
中图分类号: TN911.7;TP391 **文献标识码:** A **文章编号:** 0372-2112(2022)06-1310-09
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20210829

Open-MUSIC: An Open Set Recognition Algorithm of Electromagnetic Target Based on Metric Learning and Feature Subspace Projection

YANG Liu, LI Qiang, SHAO Huai-zong
(*School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan* 611731, *China*)

Abstract: In the increasingly complex electromagnetic spectrum environment, in order to realize the management and control of spectrum resources, it is necessary to determine whether the received signal is from the known or unknown radiation source. To tackle this problem, this paper proposes an algorithm named Open-MUSIC(MUltiple SIgnal Classification) to discriminate the known and unknown sources. The key idea of Open-MUSIC is to form the feature space from the known classes via a judiciously designed neural network, and then the feature space is decomposed into two orthogonal subspaces, namely the range subspace and the null subspace. Based on the projection ratio of the test signal's feature onto the two subspaces, we can accurately discriminate the known and the unknown radiation sources. Experiments on three datasets show that the performance of the Open-MUSIC is improved by more than 3% on electromagnetic data sets compared to other methods.

Key words: open set recognition; feature subspace decomposition; center loss; projection

1 引言

近年来,电磁频谱已成为不可或缺的国家战略资源,是继陆、海、空、天、网之后的第六维作战空间,对电磁频谱的智能认知是实现制电磁权的关键.然而,战场复杂、开放的电磁空间和不断出现的未知辐射源,给电磁频谱认知带来了巨大挑战.其中,从侦收信号中快速、准确地识别出辐射源是未知目标还是已知目标的未知工作模式,是电磁目标认知需要解决的首要问题.由于缺少未知目标训练样本,对于未知目标的识别本质上属于开集识别[1](open set recognition),也被称为开放世界识别[2](open world recognition)或开放类识别(open category learning),本文使用开集识别这一术语.在开集识别的测试中,测试样本可能来自训练集所包含的类别以外的数据,开集识别算法的目的是学习一种分类预测模型,将已知类的样本分类成正确的类,并识别出未知类的样本.

收稿日期:2021-07-01;修回日期:2022-01-02;责任编辑:冯珂
基金项目:国家自然科学基金(No.62171110,No.U19B2028,No.U20B2070)

与开集识别相对应的是闭集识别,即训练集中的类别和测试集中的类别是一致的,数据集中所有的样本的类别都是已知的,没有未知类别的样本. 所以闭集识别在训练集与测试集数据分布相同的假设下,只需要寻找各个类别之间的分界线,将各类别分开即可. 自从 2010 年 AlexNet[3] 在 ImageNet LSVRC-2010 (ImageNet Large-Scale Visual Recognition Challenge-2010)上夺冠,基于深度学习的分类识别技术在图像、语音和电磁等领域受到了极大的关注. 但是,将现有基于闭集的识别网络直接应用到开集识别中,仍然面临许多问题.

2　相关工作与背景

2.1　电磁信号识别

近年来,基于深度学习的电磁信号识别取得了不错的成绩. O'Shea 等人[4]使用残差神经网络[5]在考虑了载波频偏、多径衰落和信道损伤等的情况下解决了信号分类识别问题,并讨论了设计此类模型的注意事项. Peng 等人[6]使用 AlexNet 和 GoogLeNet 来处理调制分类问题,体现了深度学习在电磁领域的显著优势. Duan 等人[7]提出了一种多载波波形自动分类方法,并利用主成分分析抑制加性高斯白噪声,降低神经网络的输入维数. 此外,Wong 等人[8]使用卷积神经网络来估计每个发射器的同向/正交(I/Q)不平衡参数. Huang 等人[9]提出了一种用于自动调制分类的压缩卷积神经网络,并提出了使用压缩损失来训练该网络. Zhang 等人[10]通过使用频带选择、信噪比选择和样本选择来减少模型训练所需的时间,并证明了深度学习在无线干扰识别的可行性. Liang 等人[11]提出了一种基于深度学习的功率控制方法,旨在解决最大化衰落多用户干扰信道总和率的非凸优化问题.

2.2　开集识别

本文主要研究开集识别问题,即在训练阶段没有未知类的信息:既没有这些类的实例信息,也没有属性信息. 训练完成后,在测试和使用阶段,算法需要对未知类的实例样本进行分辨. 对于开集识别问题,如今已经有了一些研究,这些研究大体可以分为两类:基于判别模型和基于生成模型.

从基于判别模型的方面看,主要有基于传统机器学习的方法和基于深度神经网络的方法. 传统的机器学习方法通常是基于训练数据与测试数据分布相同的假设的,为了使这些方法能够运用在开集识别问题里,学者们进行了许多研究. Cevikalp[12,13]在 SVM(Support Vector Machine)的基础上,对已知类样本增加约束,提出了最佳拟合超平面分类器(best-fit hyperplane classifier). Bendale 等人[2]通过扩展最近类均值(nearest class mean)分类器,开发了最近邻非离群点(Nearest Neighbor non-Outlier,NNO)算法来解决开集识别问题. NNO 算法根据样本与各个已知类中心的距离进行分类,如果所有已知类的分类器都判断该样本不属于已知类,则将该样本判定为未知类. 对于深度神经网络来说,其本身就具有强大的学习表示能力,分类时通常使用 SoftMax 层与交叉熵损失,使得其本质上具有封闭性. 对于此问题,Bendale 等人[1]提出了 OpenMax 模型,首先用 SoftMax 层通过最小化交叉熵损失来训练网络,然后计算训练样本的特征到其对应类的平均特征向量的距离,并用于拟合每个已知类单独的威布尔分布,根据韦布尔分布拟合分数对特征向量进行重新分布,最后再利用 SoftMax 计算已知类和未知类的概率. Dhamija 等人[14]将 SoftMax 与新的熵开集损失和 Objectosphere 损失. Shu[15]提出了 DOC(Deep Open Classifier)模型,采用了 1-vs-rest 的 Sigmoid 层将 SoftMax 替代. Liu 等人[16]采用动态元嵌入结合了直接图像特征和相关的记忆特征,其特征范数表明对已知类的熟悉程度,以此来实现对未知类的识别. Hassen 等人[17]提出了 ii-loss 与交叉熵损失共同训练网络,使得其产生的特征更适合开集识别场景. 几乎所有的基于判别模型的开集识别算法都需要指定阈值,阈值在算法中起到了非常关键的作用,后面会对阈值的选定过程进行讨论说明.

从基于生成模型的方面看,Ge 等人[18]采用条件生成网络来生成未知类的样本,并与 OpenMax 结合,提出了 G-OpenMax 算法,可以对生成的未知类样本进行概率估计. Yu 等人[19]提出了对抗样本生成框架(adversarial sample generation framework),可以用它生成与已知类样本相近的未知类样本,必要时也可以生成已知类样本来扩充已知类数据集. Chen 等人[20]提出了一种称为对抗互易点学习(Adversarial Reciprocal Point Learning,ARPL)的方法,以在不损失已知分类精度的情况下最小化已知分布与未知分布的重叠部分. 这些方法已经取得了一些成果,但如何生成更有效的未知类样本仍需探索.

2.3　度量学习

在机器学习中,对高维数据进行各种形式的降维,主要是为了学习数据表示,即寻找一个可以更好地表示数据特征的低维空间,这个数据特征可以直接用于解决任务. 度量学习是传统机器学习的一种,就是在空间中寻找合适的空间或合适的距离度量函数,并用距离来度量样本之间的相似度. 通过训练,相似样本之间的距离小,不同样本之间的距离大.

传统的度量学习主要是学习一个距离度量函数. 例如马氏距离[21]需要学习一个(半)正定对称矩阵. 在深度度量学习中,主要是利用一定的损失函数作为距离度量,让网络学习一个低维的特征空间(通常称为

Embedding),达到同类聚合和异类分离的效果. 这个距离度量可以固定,不需要学习,比如欧式距离和余弦距离. 度量学习大致可以分为基于样本对和基于代理[22]两种. 许多度量学习算法都是基于样本对的,主要有Contrastive Loss和Triplet Loss等. 基于代理的方法则使用全局信息进行优化,例如Center Loss和Proxy-NCA等.

3 问题描述

开集识别的问题可以用以下数学语言来描述:给定一个训练集$T=\{(x_i,y_i)\,|\,i=1,2,\cdots,N\}$,其中$x_i\in\mathbb{R}^{\text{sample}}$,训练集中样本的类别集$S=\{1,2,\cdots,K\}$,其中$y_i\in S$. 在训练阶段,只能访问和使用训练集中的样本及其标签,而没有任何其他未知类的信息;而在测试阶段,有测试集$T_O=\{(x_i,y_i)\,|\,i=1,2,\cdots,M\}$,测试集的样本类别集合$S_O=\{1,2,\cdots,K,K+1,\cdots,P\}$,其中$K+1,\cdots,P$表示训练阶段未出现的类别. 鉴于上述定义,开集识别算法需要将以下风险最小化,即

$$\min_f C_O(f)+\lambda C_\varepsilon(f(V)) \tag{1}$$

其中,f是需要训练的开放集识别模型;C_O和C_ε分别代表开放空间风险和经验风险;V是训练数据,且只包含已知类;λ为常数. 这个风险旨在平衡经验风险和开放空间风险,在已知样本识别率高的情况下,将未知样本分辨出来.

4 算法描述

针对以上问题,本文提出基于特征子空间分解与投影的开集识别Open-MUSIC算法. 该算法主要包括3个步骤.

步骤1 通过结合交叉熵损失与中心损失来训练一个分类网络,训练完成后,该分类网络输出层的前一层输出结果用作数据特征提取,得到从数据到特征的映射模型,如图1所示.

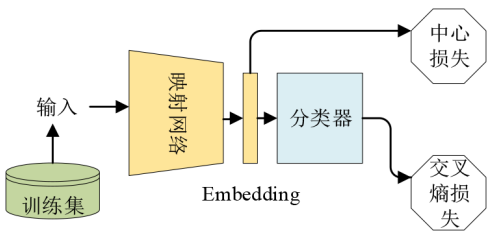


图1 基于神经网络的映射特征模型训练算法

步骤2 将所有训练样本输入模型中,得到各个已知类的中心特征向量,将各个向量组合形成已知类中心特征矩阵,对该矩阵进行正交子空间分解,得到其值域子空间与零域子空间,用于步骤3中评估指标的计算,具体如图2所示.

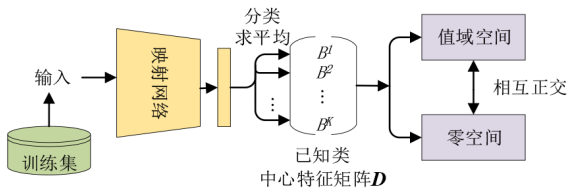


图2 特征子空间分解并计算投影比值

步骤3 将测试数据输入步骤1中的特征提取网络,并将提取到的特征分别投影到步骤2中的值域子空间和零域子空间,并计算投影长度比值. 若比值大于设定的阈值,则判定为属于已知类;否则,为未知类,具体如图3所示. 值得注意的是,阈值的设定对性能影响较大,后面本文会对阈值的设定进行详细讨论.

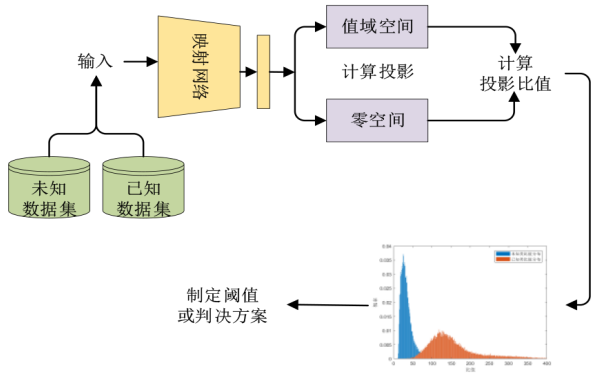


图3 确定阈值或判决方案

综上所述,算法主要包含:获得映射特征、特征子空间分解并计算投影比值、阈值确定. 下面对各步骤进行详细说明.

4.1 获得映射特征

获得映射特征就是只使用已知训练数据,学习一个模型,完成样本空间到特征空间的映射,即$F(x)$:$\mathbb{R}^{\text{sample}}\to\mathbb{R}^d$. 在开集识别环境下,映射的特征需要满足2个条件:缩小类内距离,扩大类间距离. 前者保证从已知目标数据中学习到目标特征最本质的表征,而后者保证已知和未知类边界划分更容易,使得式(1)中开放空间风险与经验风险都较小. 该想法与Fisher判别法类似,Fisher判别法目标是通过最大化2类质心距离与类内距离的比值,来得到一个映射矩阵,可以将2类样本映射到一维空间. 而本文可以使用神经网络来学习映射函数,将样本投影映射到高维空间.

一般情况下,映射网络为卷积神经网络,且采用交叉熵损失来监督训练网络,该损失函数由如下公式定义:

$$L_S=-\sum_{i=1}^{m}\log\frac{\mathrm{e}^{W_{y_i}^{T}F(x_i)+b_{y_i}}}{\sum_{j=1}^{K}\mathrm{e}^{W_j^{T}F(x_i)+b_j}} \tag{2}$$

其中,x_i为训练集中的第i个样本;y_i为该样本的分类标签;$F(x)$为该样本通过模型映射得到的映射特征,且$F(x)\in\mathbb{R}^d$;$W_j\in\mathbb{R}^d$为分类器的最后一个全连接层权重W第j行;b为该全连接层的偏置;m和K分别为训练批大小与已知类个数.

由其定义可知,最小化交叉熵损失只能保证通过映射网络得到的特征可分,即在一定程度上可以将各类之间的距离拉大,但并不能保证每类类内聚合. 为此,本文在交叉熵损失基础上,引入中心损失,即

$$L_C=\frac{1}{2}\sum_{i=1}^{m}\left\| x_i-c_{y_i}\right\|_2^2 \tag{3}$$

并使用交叉熵损失与中心损失联合监督训练网络[23],联合的损失由下式定义:

$$L=L_S+\lambda L_C \tag{4}$$

其中,c_i为第i类的中心特征向量;$\lambda\geqslant 0$为常数,用来平衡两种损失函数所占的比重,若λ为0,则该损失函数与交叉熵损失相同. 交叉熵损失主要对类间的分离做贡献,中心损失主要对类内的聚合做贡献. 其网络结构示意图如图1所示,其中Embedding向量为维度为d(>K)的特征. 映射网络参数的训练过程如算法1所示.

算法1　映射网络训练算法

输入:

T:训练数据集$\left(x_i,y_i\right)_{i=1}^{N}$

θ_C, W:映射网络与最后一层全连接层参数

$c_j\mid j=1,2,\cdots,K$:中心特征

λ,α,μ:超参数

输出:θ_C

1:**WHILE** NOT 网络收敛条件 **DO**

2:　$L^t=L_S^t+\lambda L_C^t$

3:　$\dfrac{\partial L^t}{\partial x_i}=\dfrac{\partial L_S^t}{\partial x_i}+\lambda\dfrac{\partial L_C^t}{\partial x_i}$

4:　$W^{t+1}=W^t-\mu\dfrac{\partial L^t}{\partial W^t}=W^t-\mu\dfrac{\partial L_S^t}{\partial W^t}$

5:　$\theta_C^{t+1}=\theta_C^t-\mu\sum_{i}^{N}\left(\dfrac{\partial L^t}{\partial x_i}\cdot\dfrac{\partial x_i}{\theta_C^t}\right)$

6:　$c_j^{t+1}=c_j^t-\alpha\dfrac{\sum_{i}^{N}\delta(y_i=j)(c_j-x_i)}{1+\sum_{i}^{N}\delta(y_i=j)}$

7:　$t\leftarrow t+1$

8:**END WHILE**

9:返回 θ_C

4.2　特征子空间分解

在完成数据特征提取后,已有多种方法对特征进行处理以适应开集识别场景. 比如,采用通过SoftMax层后的概率计算熵,并制定阈值,熵大于阈值,则为未知类;熵小于阈值,则为已知类. 或者采用离群值,计算实例到K个已知类中最近类平均值的距离作为决策量[24]. 受子空间MUSIC(MUltiple SIgnal Classification)算法启发,本文提出一种基于特征子空间分解投影的开集识别算法.

MUSIC算法是对协方差矩阵进行分解,根据奇异值的大小将其划分为两个正交的子空间,即信号子空间和噪声子空间. 类似地,将已知类中心特征矩阵进行奇异值分解得到值域子空间和零域子空间,利用已知类和未知类在两个正交的子空间分布的不同来进行区分. 具体而言,首先通过下式得到训练集中每个样本的特征向量$\boldsymbol{A}_j^i\left(\boldsymbol{A}_j^i\in\mathbb{R}^d\right)$

$$\boldsymbol{A}_j^i=F\left(x_j\right),\left(y_j=i\right) \tag{5}$$

其中,$\boldsymbol{A}_j^i$表示第i个已知类的第j个样本通过模型后的特征. 然后,计算各个类的中心特征矩阵$\boldsymbol{D}$,即

$$B^i=\frac{\sum_{j=1}^{N_i}\boldsymbol{A}_j^i}{N_i} \tag{6}$$

$$\boldsymbol{D}=\left(B^1,B^2,\cdots,B^K\right)^{\mathrm{T}},\boldsymbol{D}\in\mathbb{R}^{K\times d} \tag{7}$$

其中,中心特征矩阵$\boldsymbol{D}$由所有已知类的中心特征向量组成. 对$\boldsymbol{D}$进行奇异值分解,得到它的值域子空间和零域子空间,两个空间相互正交. 容易看出,如果待分类样本来自某个已知类,其特征可以近似由$\boldsymbol{D}$的值域子空间刻画,因此,其在$\boldsymbol{D}$的零域子空间投影近似为零. 同样地,如果待分类样本为未知类,其特征无法由已知类的中心特征矩阵$\boldsymbol{D}$完全表征,即未知类特征在$\boldsymbol{D}$的零空间有(较大)投影. 因此,可以利用已知类和未知类在$\boldsymbol{D}$的两个正交子空间投影长度的差异来区分已知和未知. 基于此,定义如下比值:

$$\varsigma=\frac{\left\|\boldsymbol{A}\cdot v_1\right\|_2^2}{\left\|\boldsymbol{A}\cdot v_2\right\|_2^2} \tag{8}$$

其中,$\boldsymbol{A}$是通过映射模型得到的样本特征;$\|\cdot\|_2^2$是向量二范数的平方. $v_1\in\mathbb{R}^{d\times K}$和$v_2\in\mathbb{R}^{d\times(d-K)}$分别代表矩阵$\boldsymbol{D}$的值域子空间和零域子空间. 综上所述,已知类的样本比值较大,未知类的样本比值较小. 两个正交空间中样本特征的投影大小的比值可以将已知类与未知类区分开,具体步骤见算法2.

4.3　阈值确定

如式(9)所示,阈值直接用于判断是否是未知类的

算法2 子空间投影比算法

输入:

F:特征映射网络

T:训练数据集$\left(x_i,y_i\right)_{i=1}^{N}$

K:已知类个数

x:测试样例

输出:该测试样例的比值ς

1:$N_i\leftarrow 0,i=1,2,\cdots,K$

2:**FOR** (x_i,y_i) in T **DO**

3: $A_{N_i+1}^{y_i}\leftarrow F(x_i)$

4: $N_{y_i}\leftarrow N_{y_i}+1$

5:**END FOR**

6:**FOR** $k\in[1,2,\cdots,K]$ **DO**

7: **FOR** $n\in[1,2,\cdots,N_k]$ **DO**

8: $B_k\leftarrow B_k+A_n^k/N_k$

9: **END FOR**

10:**END FOR**

11:$\boldsymbol{D}\leftarrow[B_1,B_2,\cdots,B_K]^{\mathrm{T}}$

12:$v_1,v_2\leftarrow \mathrm{SVD}(\boldsymbol{D})=U\Sigma V^{\mathrm{T}}=[U]\Sigma[v_1,v_2]^{\mathrm{T}}$

13:对于测试样例x有$A\leftarrow F(x)$

14:$\varsigma=\dfrac{\left\|a\cdot v_1\right\|_2}{\left\|a\cdot v_2\right\|_2}$

15:返回ς

样本,且阈值的好坏直接影响算法的准确性. 下面主要介绍两种确定阈值的方法.

$$\mathrm{Relation}\left(y,S\right)=\begin{cases}y\in S, & \varsigma\geqslant\mathrm{threshold}\\ y\notin S, & \varsigma<\mathrm{threshold}\end{cases}\tag{9}$$

4.3.1 通过正确率确定阈值

第一种方法,阈值只使用已知类样本来确定. 将所有已知类样本经过映射模型,获得特征后,可由式(8)计算该样本比值,并按从大到小排序,其序列记为S. 然后固定已知类识别准确率Accuracy,如:90%,95%或99%,划分阈值门限为S中下标为round(length(S)·Accuracy)所对应的比值作为阈值. 实验发现,依据已知类准确率的划分方式,可避免门限划分过低,导致未知类误判为已知类.

4.3.2 通过似然比确定阈值

第二种方法,利用生成对抗模型生成一些与训练样本相近的负样本,与训练样本或生成的正样本一起,经过步骤1和步骤2后,得到各个样本的比值,画出统计直方图(图4). 由图可以看出,假定正样本的比值与负样本的比值遵循某个分布,如正态分布或威布尔分布等,则可以用似然比对测试集做分类预测. 以威布尔分布为例,有

$$p\left(x|H_0\right)=\begin{cases}\dfrac{k_0}{\lambda_0}\left(\dfrac{x}{\lambda_0}\right)^{k_0-1}\mathrm{e}^{-(x/\lambda_0)^{k_0}}, & x\geqslant 0\\ 0, & x<0\end{cases}\tag{10}$$

$$p\left(x|H_1\right)=\begin{cases}\dfrac{k_1}{\lambda_1}\left(\dfrac{x}{\lambda_1}\right)^{k_1-1}\mathrm{e}^{-(x/\lambda_1)^{k_1}}, & x\geqslant 0\\ 0, & x<0\end{cases}\tag{11}$$

其中,H_0为未知类;H_1为已知类;$k_0,\lambda_0,k_1,\lambda_1$可以通过正负样本的比值计算出来.

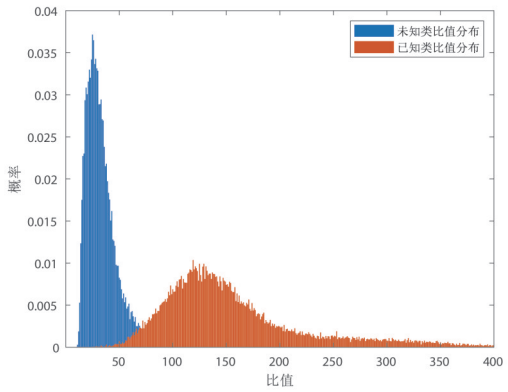


图4 已知类与未知类比值分布直方图

当$p(H_0|x)>p(H_1|x)$时,表示该样本属于未知类;否则该样本属于已知类. 而由贝叶斯公式可知,$p(H_0|x)>p(H_1|x)$与$p(x,H_0)>p(x,H_1)$等价,而$p(x,H)=p(x|H)\cdot p(H)$,故设

$$\begin{aligned}L(x)&=\frac{p\left(x|H_0\right)}{p\left(x|H_1\right)}\\&=\frac{k_0}{k_1}\left(\frac{\lambda_1}{\lambda_0}\right)^{k_0-k_1+1}\exp\left[\left(\frac{x}{\lambda_1}\right)^{k_1}-\left(\frac{x}{\lambda_0}\right)^{k_0}\right]\end{aligned}\tag{12}$$

假设样本属于已知类与未知类的先验概率相等,即$p(H_0)=p(H_1)=0.5$,则有

$$\tau=\frac{p(H_0)}{p(H_1)}=1\tag{13}$$

所以,有判决准则:

$$\delta(x)=\begin{cases}0, & L(x)\leqslant\tau\\ 1, & L(x)>\tau\end{cases}\tag{14}$$

即$L(x)\leqslant\tau$时,该样本属于未知类;否则,该样本属于已知类.

5 实验与结果分析

在本节中,我们将在3个数据集上进行算法有效性验证. 3个数据集分别为MNIST手写数字数据集、雷达PDW数据集、无人机信号数据集.

本文主要使用识别精度(Accuracy)、F值(F-measure)与ROC曲线(Receiver Operating Characteristic Curve)下的面积AUC-ROC来衡量各种算法在开放集上的效果,F-measure由下式定义:

$$\text{F-measure}=\frac{2\cdot\text{Precision}\cdot\text{Recall}}{\text{Precision}+\text{Recall}} \tag{15}$$

其中,Precision为准确率,Recall为召回率,F-measure为准确率与召回率的调和平均值. Precision与Recall定义为

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{16}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{17}$$

其中,TP为将正类预测为正类的数量;FP为负类预测为正类的数量,即误报率;FN为将正类预测为负类数,即漏报率.

第二个指标为准确率,计算式为

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{TN}+\text{FP}+\text{FN}} \tag{18}$$

其中,TP、FP、FN与上述相同;TN为将负类预测为负类的数量.

由于F-measure与Accuracy受阈值影响较大,故引入ROC曲线下的面积AUC-ROC来衡量算法的性能. ROC曲线又称接受者操作特征曲线. 该曲线最早应用于雷达信号检测领域,用于区分信号与噪声. 后来人们将其用于评价模型的预测能力. 对于一个二分类模型,其阈值可能设定或高或低,每种阈值的设定会得出不同的FP和TP,将同一模型每个阈值的(FP,TP)坐标都画在ROC空间里,就成为特定模型的ROC曲线. 而ROC曲线与FP轴所包围的面积越大,表示该模型性能越强.

5.1　数据集描述

5.1.1　MNIST手写数字数据集

MNIST数据集是手写数字的灰度图像数据集,数据集中共包括6万多张训练图像样本与1万多张测试图像样本,共分为10类,且每个样本大小为28×28. 因为该数据集中的灰度图像样本已经可以直接在模型中使用,所以不需要对数据集做任何预处理操作.

在MNIST数据集中,样本分为10类. 为适应开集识别场景,我们选取0,1,2,3,4,5为已知类进行训练;设定6,7,8,9为未知类,在训练阶段不可见.

5.1.2　多功能雷达工作模式数据集

多功能雷达数据集是通过仿真生成的多功能雷达不同工作模式的脉冲描述字(PDW)数据,一共包含55个已知工作模式和6个未知工作模式,每条PDW数据主要包括:脉冲到达时间(TOA)、载波频率(RF)、脉冲宽度(PW)、脉冲幅度(PA)、脉冲到达角度(DOA)等参数. 由于在侦收中,PA和DOA受环境影响较大,不作为工作模式识别的特征. 已知和未知模式分别包含757个和120个样本,每个样本包含100个脉冲记录.

在使用雷达数据集之前需要对数据做预处理. 将TOA转为脉冲重复间隔(PRI)后,每条PDW样本的PRI,RF和PW作为3个通道,形成3×100的类图片样本. 为了更适合CNN提取特征,将样本延展为3×100×100的图片,并将每个通道按下式进行归一化,得到预处理后的数据集.

$$x'=\frac{x-\min\{x\}}{\max\{x\}-\min\{x\}} \tag{19}$$

在训练阶段,随机将757个已知类样本划分为训练集(637个样本)与测试集(120个样本),训练集主要用于模型训练,测试集可与未知类数据(120个样本)共同用于开集识别测试.

5.1.3　无人机个体识别信号数据集

无人机个体识别信号数据集由实际采集的9款无人机时域信号数据组成,用于对无人机个体指纹的识别. 部分时域信号如图5所示.

对无人机采集信号需要进行预处理. 预处理主要包含提取有效信号部分和将时域信号处理为类图片形式,方便CNN提取特征. 采用能量检测方法对有效信号部分进行提取切片,即计算窗内数据的能量,大于阈值则为信号部分,小于阈值则为噪声部分. 之后对提取出的有效信号进行短时傅里叶变换(Short-Time Fourier Transform,STFT)形成时频图片. 图6给出了图5有效信号在STFT变换后的时频图.

通过上述预处理过程,为每架无人机提取了600张时频图样本,共5 400个样本,并将9架无人机中的5架作为已知类,其余4架作为未知类,已知类和未知类样本大小分别为3 000和2 400.

5.2　实验设计

本实验将Open-MUSIC与OpenMax[1]、OLTR[16]、ii-loss[17]和ARPL[20]在MNIST手写数字识别、雷达工作模式识别和无人机个体指纹识别上进行实验对比,通过F-measure、Accuracy与AUC-ROC等指标对各个模型进行评估. Open-MUSIC在3个数据集上映射网络模型分别如表1~表3所示.

5.3　实验结果及分析

表4~表6分别给出了各个算法在MNIST数据集、雷达数据集与无人机信号数据集上的结果.

在MNIST数据集上,ARPL算法在3个指标上都表现最佳. Open-MUSIC算法虽然AUC-ROC略低于其他算法,但是F-measure与Accuracy等指标都仅次于ARPL算法,优于其他方法. OpenMax、OLTR和ii-loss等方法虽然AUC-ROC较高,但其余两个指标较低,这表

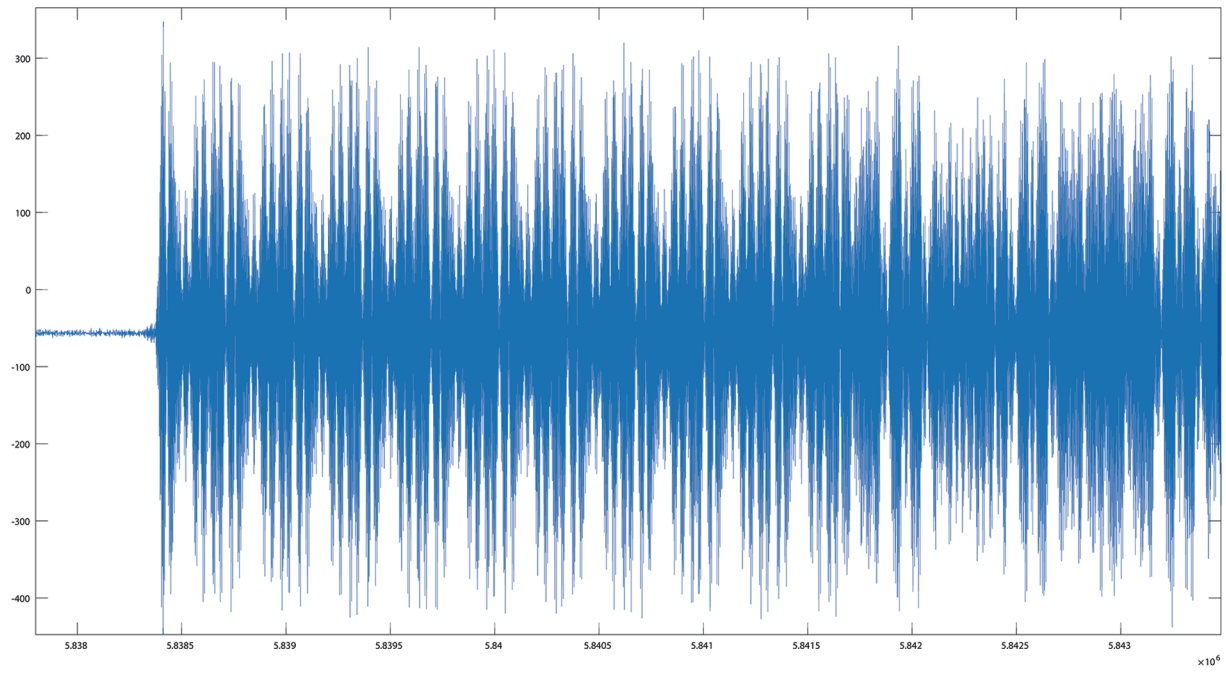


图5 无人机信号时域图

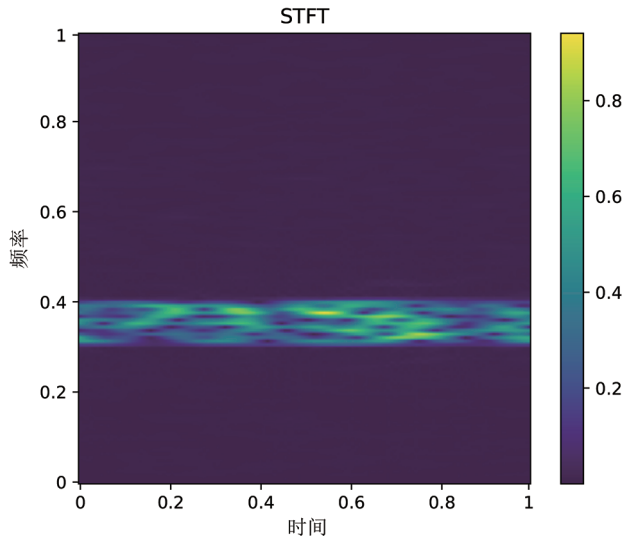


图6 无人机信号时频图

明这些算法的性能受阈值影响较大,也说明了Open-MUSIC设定的阈值效果较好.

在雷达数据集上,Open-MUSIC较其他方法性能提升了3%以上,较表现最差的OpenMax算法性能提升了近40%. 在无人机信号数据集上,Open-MUSIC的F-measure与Accuracy保持在90%以上,AUC-ROC在95%以上,性能显著高于其他算法.

综合以上结果来看,Open-MUSIC相对于其他方法更适合处理电磁数据,比如在无人机数据集上,其性能相较于其他方法至少提升了4%. 同时,Open-MUSIC更适合处理类数较多且每类样本数较少数据,如在雷达数据集中,每类所含样本最少只有4个样本. 此时OpenMax这种依赖每类训练数据的得分来拟合分布的

表1 MNIST数据集所使用特征映射网络参数表

层名称	卷积核大小/神经元个数	卷积核深度	激励函数
卷积层	5*5	32	PReLU
卷积层	5*5	32	PReLU
池化层	2*2	—	—
卷积层	5*5	64	PReLU
卷积层	5*5	64	PReLU
池化层	2*2	—	—
卷积层	5*5	128	PReLU
卷积层	5*5	128	PReLU
池化层	2*2	—	—
全连接层	32	—	PReLU
全连接层	6	—	—

表2 雷达PDW数据集所使用特征映射网络参数表

层名称	卷积核大小/神经元个数	卷积核深度	激励函数
卷积层	3*3	32	ReLU
池化层	2*2	—	—
卷积层	3*3	64	ReLU
池化层	2*2	—	—
卷积层	5*5	128	ReLU
池化层	2*2	—	—
全连接层	512	—	ReLU
全连接层	256	—	ReLU
全连接层	128	—	ReLU
全连接层	55	—	—

表3　无人机数据集所使用特征映射网络参数表

层名称	卷积核大小/神经元个数	卷积核深度	激励函数
卷积层	3*3	32	ReLU
卷积层	3*3	32	ReLU
池化层	2*2	—	—
卷积层	3*3	64	ReLU
卷积层	3*3	64	ReLU
池化层	2*2	—	—
卷积层	3*3	128	ReLU
卷积层	3*3	128	ReLU
池化层	2*2	—	—
卷积层	3*3	256	ReLU
卷积层	3*3	256	ReLU
池化层	2*2	—	—
全连接层	512	—	ReLU
全连接层	256	—	ReLU
全连接层	128	—	ReLU
全连接层	5	—	—

表4　MNIST数据集实验结果

算法	评估指标		
	F-measure	Accuracy	AUC-ROC
OpenMax	0.791	0.800	0.981
OLTR	0.653	0.703	0.986
ii-loss	0.861	0.842	0.983
ARPL	0.966	0.966	0.996
Open-MUSIC	0.937	0.938	0.984

表5　雷达数据集实验结果

算法	评估指标		
	F-measure	Accuracy	AUC-ROC
OpenMax	0.415	0.470	0.577
OLTR	0.727	0.639	0.833
ii-loss	0.911	0.906	0.935
ARPL	0.713	0.621	0.747
Open-MUSIC	**0.941**	**0.937**	**0.969**

表6　无人机信号数据集实验结果

算法	评估指标		
	F-measure	Accuracy	AUCROC
OpenMax	0.700	0.623	0.915
OLTR	0.653	0.703	0.881
ii-loss	0.813	0.815	0.907
ARPL	0.680	0.626	0.803
Open-MUSIC	**0.916**	**0.911**	**0.956**

算法效果较差,而Open-MUSIC使用中心损失训练映射网络,为每个类单独维护一个中心,且子空间分解时每类中心都有相同的权重,在一定程度上可以减小样本数少所带来的影响. Open-MUSIC在3个数据上的AUC-ROC均超过了95%,表明本文算法较其他算法鲁棒性较强,且更适合于电磁数据.

6　结论

本文针对电磁频谱认知领域内的电磁目标开集识别问题,借鉴MUSIC算法,提出了基于正交子空间分解的开集识别方法Open-MUSIC. 该方法通过使用映射网络得到的已知类特征,组成已知类中心特征矩阵,进而对该矩阵进行正交子空间分解,得到其值域子空间与零域子空间,通过计算测试样本特征在两个子空间内的投影比值来对未知类进行识别,以提升识别效果. 实验表明Open-MUSIC算法在电磁数据集上效果较其他开集识别算法更好.

参考文献

[1] BENDALE A, BOULT T E. Towards open set deep networks[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas: IEEE, 2016: 1563-1572.

[2] BENDALE A, BOULT T. Towards open world recognition [C]//2015 IEEE Conference on Computer Vision and Pattern Recognition. Boston: IEEE, 2015: 1893-1902.

[3] KRIZHEVSKY A, SUTSKEVER I, HINTON G E. ImageNet classification with deep convolutional neural networks[J]. Communications of the ACM, 2017, 60(6): 84-90.

[4] O´SHEA T J, ROY T, CLANCY T C. Over-the-air deep learning based radio signal classification[J]. IEEE Journal of Selected Topics in Signal Processing, 2018, 12(1): 168-179.

[5] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas: IEEE, 2016: 770-778.

[6] PENG S L, JIANG H Y, WANG H X, et al. Modulation classification based on signal constellation diagrams and deep learning[J]. IEEE Transactions on Neural Networks and Learning Systems, 2019, 30(3): 718-727.

[7] DUAN S R, CHEN K, YU X, et al. Automatic multicarrier waveform classification via PCA and convolutional neural networks[J]. IEEE Access, 2018, 6: 51365-51373.

[8] WONG L J, HEADLEY W C, MICHAELS A J. Specific emitter identification using convolutional neural network-based IQ imbalance estimators[J]. IEEE Access, 2019, 7: 33544-33555.

[9] HUANG S, CHAI L, LI Z N, et al. Automatic modulation

classification using compressive convolutional neural network[J]. IEEE Access, 2019, 7: 79636-79643.

[10] ZHANG X W, SEYFI T, JU S T, et al. Deep learning for interference identification: Band, training SNR, and sample selection[C]//2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications. Cannes: IEEE, 2019: 1-5.

[11] LIANG F, SHEN C, YU W, et al. Towards optimal power control via ensembling deep neural networks[J]. IEEE Transactions on Communications, 2020, 68(3): 1760-1776.

[12] CEVIKALP H, TRIGGS B, FRANC V. Face and landmark detection by using cascade of classifiers[C]//2013 10th IEEE International Conference and Workshops on Automatic Face and Gesture Recognition. Shanghai: IEEE, 2013: 1-7.

[13] CEVIKALP H. Best fitting hyperplanes for classification [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 39(6): 1076-1088.

[14] DHAMIJA A R, GÜNTHER M, BOULT T E. Reducing Network Agnostophobia[EB/OL]. (2018) [2021]. https://arxiv.org/abs/1811.04110.

[15] SHU L, XU H, LIU B. DOC: Deep Open Classification of Text Documents[EB/OL]. (2017) [2021]. https://arxiv.org/abs/1709.08716.

[16] LIU Z W, MIAO Z Q, ZHAN X H, et al. Large-scale long-tailed recognition in an open world[C]//2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). Long Beach: IEEE, 2019: 2532-2541.

[17] HASSEN M, CHAN P K. Learning a neural-network-based representation for open set recognition[C]//Proceedings of the 2020 SIAM International Conference on Data Mining. Philadelphia, PA: Society for Industrial and Applied Mathematics, 2020: 154-162.

[18] GE Z Y, DEMYANOV S, GARNAVI R. Generative OpenMax for multi-class open set classification[C]//Proceedings of the British Machine Vision Conference 2017. London: British Machine Vision Association, 2017: 42.1-42.12.

[19] YU Y, QU W Y, LI N, et al. Open category classification by adversarial sample generation[C]//Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence. California: International Joint Conferences on Artificial Intelligence Organization, 2017: 469.

[20] CHEN G Y, PENG P X, WANG X Q, et al. Adversarial reciprocal points learning for open set recognition[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, DOI:10.1109/TPAMI.2021.3106743.

[21] DE MAESSCHALCK R, JOUAN-RIMBAUD D, MASSART D L. The mahalanobis distance[J]. Chemometrics and Intelligent Laboratory Systems, 2000, 50(1): 1-18.

[22] WANG X, HAN X T, HUANG W L, et al. Multi-similarity loss with general pair weighting for deep metric learning[C]//2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). Long Beach: IEEE, 2019: 5017-5025.

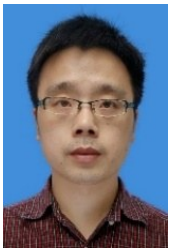
[23] WEN Y D, ZHANG K P, LI Z F, et al. A discriminative feature learning approach for deep face recognition[C]// European Conference On Computer Vision. Cham: Springer, 2016: 499-515..

[24] MENSINK T, VERBEEK J, PERRONNIN F, et al. Distance-based image classification: Generalizing to new classes at near-zero cost[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013, 35(11): 2624-2637.

作者简介

杨 柳 男，1999 年出生，安徽芜湖人. 2020年在电子科技大学获得学士学位，现为硕博连读生. 主要研究方向为知识引导的机器学习.

E-mail: 1070032777@qq.com



利 强（通讯作者） 男，1982年出生，四川成都人. 副教授、博士生导师. 分别于2005年、2008年在电子科技大学获得学士和硕士学位，于2012年在香港中文大学获得博士学位. 主要研究方向为无线通信优化算法、电磁频谱智能感知等.

E-mail: lq@uestc.edu.cn

邵怀宗 男，1967年出生，四川巴中人. 教授、博士生导师. 1992年在长春理工大学获得学士学位，1998年在四川大学获得硕士学位，2003年在电子科技大学获得博士学位. 主要研究方向为无线通信、电子对抗、新体制通信、人工智能等.

E-mail: hzshao@uestc.edu.cn