第58卷 第1期
2022年1月

南京大学学报(自然科学)
JOURNAL OF NANJING UNIVERSITY
(NATURAL SCIENCE)

Vol. 58, No. 1
Jan., 2022

DOI:10.13232/j.cnki.jnju.2022.01.012

开放集识别研究综述

高 菲,杨 柳*,李 晖
(天津大学智能与计算学部,天津,300350)

摘 要:传统机器学习方法和深度神经网络在训练模型的过程中都需要大量标记样本作为支撑,然而标记大量样本是一个耗费巨大的过程,并且真实场景变化莫测,获得所有类别的标记样本是不现实的.因此,研究者开始突破标记样本的限制,提出一种更符合现实的场景——开放集识别(Open Set Recognition,OSR).OSR要求建立的模型不仅能分类训练过程中出现的类别,还可以有效地处理未见过的类别.近年来,OSR迅速发展成为热点领域,大量的工作围绕OSR展开.对现有的OSR工作进行总结:首先,从定义上将OSR与其他相关工作进行区分;其次,按照模型建立、度量选择、增量特点对OSR算法进行总结,并介绍了OSR的两种理论;最后展望了OSR未来的发展方向.

关键词:机器学习,深度神经网络,标记样本,开放集识别,度量选择,增量
中图分类号:TP181 **文献标志码:**A

A survey on open set recognition

Gao Fei, Yang Liu*, Li Hui
(College of Intelligence and Computing, Tianjin University, Tianjin, 300350, China)

Abstract: Traditional machine learning methods and deep neural networks need a large-scale of labeled samples as support in the process of training model. However, labeling a large-scale dataset is a time-consuming process, and it is not realistic to obtain all kinds of labeled samples due to the dynamic real world. Therefore, researchers broke through the limitation of labeled samples and proposed open set recognition which is more suitable to real scenes. Open set recognition models can not only classify the categories appearing in the training process, but also deal with the unseen categories effectively. In recent years, open set recognition has developed rapidly and attracted many researchers to focus on open set problems. This paper summarizes the existing open set recognition works. First, open set recognition is defined to distinguish from other related works. Second, the open set recognition algorithms are summarized according to the model building, metric selection and property of incremental. Furthermore, two theories used in open set recognition are introduced. Finally, this paper looks forward to the future development issues of open set recognition.

Key words: machine learning, deep neural networks, labeled samples, open set recognition, metric selection, incremental

随着机器学习技术的飞速发展,机器学习在图像识别、自然语言处理等多个领域取得了巨大成就,尤其在图像识别领域,机器学习技术被广泛应用于无人驾驶[1]、人脸识别[2-4]等应用性研究.同时,随着深度神经网络的成熟,卷积神经网络[5]和递归神经网络[6]也越来越多地用于解决实际问题,但无论是传统的机器学习方法还是深度神经网络算法,在训练过程中都需要大量的标记样本,这给研究工作带来了很大的局限性.首先,通常情况下这些标记样本都需要进行人工标注,而人

基金项目:国家自然基金(62076179),北京市自然科学基金重点研究专题(Z180006)
收稿日期:2021-09-05
*通讯联系人,E-mail:yangliuyl@tju.edu.cn

工标注样本需要付出高额的成本;其次,真实场景中新类是不断增加的,在训练过程中得到所有类别样本不现实.

鉴于现实情况,研究者希望识别算法能与人一样具备应对新类的能力.例如,人类在只见过马和熊猫但没有见过斑马的情况下仍能通过"有黑白条纹的马"这样的描述来准确识别斑马.基于这种人类根据属性描述识别物体的能力,研究者提出零样本学习[7].但是,人类即使在没有任何描述作为辅助的情况下,仍然可以应对新类的出现,由此研究者开始探索开放集识别问题.

开放集识别(Open Set Recognition,OSR)是依据真实场景提出的研究方向,要求模型在没有任何辅助信息时,不仅能分类见过的类别,还能准确识别新出现的类别.这一要求打破了传统封闭环境下识别的限制,建立模型的过程中人们不需要花费大量的时间和金钱收集标记样本甚至辅助信息.而且,OSR问题更贴近真实场景中新类不断出现的现实.

近年来,OSR问题受到越来越多研究者的关注,成为机器学习领域中的热点.为了OSR问题的进一步研究,本文对OSR进行了系统性总结.

1 开放集识别概述

1.1 OSR的形成与发展 OSR的概念最早可以追溯到21世纪初.随着机器学习和深度学习的发展,图像识别、文本分类、自然语言处理等领域也有了长足的发展.但是,人们逐渐发现,机器学习或者深度学习在处理问题的过程中都需要有大量的标记数据作为支撑,要求训练数据集必须是完备的,可这一点往往会受到现实情况的限制.因此,研究者开始研究在没有标记样本情况下的识别问题,提出了小样本数据学习、零样本学习以及开放集识别.然而,零样本学习虽然解决了样本稀缺的问题,但是它需要大量的辅助信息作为支撑,辅助信息的获得也是一个消耗巨大的过程.而开放集识别则是更具有挑战的不需要任何辅助信息的无标记样本问题.

很多应用问题本身就具有开放集识别特性,例如在人脸识别[2-4]中,测试序列出现人脸库中没有的人脸图像是经常发生的.在开放集识别的定义正式提出之前,Phillips et al[8]已经通过设置阈值的评估方法解决了人脸识别中出现新类的情况,这是一个典型的开放集身份识别问题.同样地,Li and Wechsler[9]再次从评估的角度看待开放集人脸识别,将其当作早期人脸识别测试中观察列表公式的变体.2012年Scheirer et al[10]首次提出OSR的概念以及相关的定义,并从约束开放空间的角度建立了1-vs-set模型.

1.2 开放集识别的定义

1.2.1 样本集类别的定义 封闭环境下,训练集样本和测试集样本的类别相同,即测试集中不会出现训练集中没有的类别,样本类别比较简单.但是,当大量工作不满足于封闭环境下的研究时,样本类别变得相对复杂.因此,为更好地解决开放环境问题,需要重新定义样本的类别.Geng et al[11]在研究OSR问题时,对Scheirer et al[12]的基本识别类别的划分进行扩展,最终将OSR问题中的样本分为四类:

(1)已知辅助信息的已知类(Known Known Classes,KKCs):KKCs包含在训练过程中被标记的正样本(某一KKC中的正样本对其他KKCs是负样本),同时,这些样本的辅助信息(语义信息和属性信息等)可以获得.

(2)无关信息的已知类(Known Unknown Classes,KUCs):KUCs包含被标记的负样本,即样本虽被标记但不属于问题期待的类别,如一些背景类别[13]等.

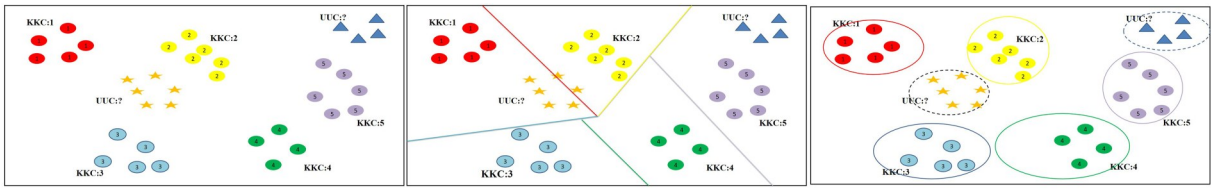
(3)已知辅助信息的未知类(Unknown Known Classes,UKCs):UKCs包含在训练过程中没有标记的样本,但是,在训练过程中样本的辅助信息(语义信息和属性信息等)可以获得.

(4)未知辅助信息的未知类(Unknown Unknown Classes,UUCs):UUCs包含在训练过程中没有标记的样本,同时,在训练过程中无法获得样本的辅助信息(语义信息和属性信息等).

有了上述四种样本类别的定义,可以对分类识别问题有更好的认识.下面根据四种样本类别给出OSR的定义,并对一些与OSR相关的工作进行简单介绍.

1.2.2 开放集识别的相关定义 下面从图像识别角度出发讨论OSR问题.图像识别本质上就

是通过对属于KKCs的图像进行训练得到一个模型$f: x_{tr} \to y_{tr}$,f的参数在训练中不断更新,以获得更好的分类性能. 然后,利用训练好的模型f,就可以分配给测试集样本x_{te}对应的预测标签$\hat{y}_{te}$. 而OSR问题稍有不同,因为在测试过程中会出现训练过程中没有出现的图像类别(UUCs),所以必须对模型f进行调整,使f不仅能对属于KKCs的图像进行相应预测,还能拒绝UUCs. 传统分类器与开放集识别任务的对比如图1所示.



(a) 数据集分布　(b) 传统分类器分类　(c) 开放集识别

图1　传统分类器与开放集识别对比:(a)数据集的原始分布,包括五个KKCs和两个UUCs;(b)传统分类器的决策边界,其中UUCs会分到KKCs中;(c)开放集识别,能识别UUCs并单独分类

Fig.1　Comparison of traditional classification and open set recognition: (a) the distribution of original dataset including KKCs and UUCs, (b) the decision boundary of each KKC obtained by traditional classification methods with UUCs included in KKCs´ spaces, (c) open set recognition which can recognize UUCs as a class

定义1　开放集识别　由样本-标签对组成的训练集与测试集分别表示为:

$$D_{tr}=\left\{\left(x_i\in X_{tr}, y_i\in Y_{tr}\equiv\left\{1,\cdots,C_{TR}\right\}\right)\middle| i=1,2,\cdots,m\right\}$$

$$D_{te}=\left\{\left(\begin{matrix}x_i\in X_{te}, y_i\in\left(Y_t\cup Y_e\right)\equiv\\ Y_{te}\equiv\left\{1,\cdots,C_{TR},\cdots,C_{TE}\right\}\end{matrix}\right)\middle| i=1,2,\cdots,n\right\}$$

其中,$Y_t\equiv\left\{1,\cdots,C_{TR}\right\}$,$Y_e\equiv\left\{C_{TR}+1,\cdots,C_{TE}\right\}$. OSR是利用训练集$D_{tr}$训练一个模型$f$,$f$能对测试集$D_{te}$中的$\left\{\left(x_i\in X_{te}, y_i\in Y_t\equiv\left\{1,\cdots,C_{TR}\right\}\right)\right\}$进行正确分类,并且正确识别$\left\{\left(x_i\in X_{te}, y_i\in Y_t\equiv\left\{C_{TR}+1,\cdots,C_{TR}\right\}\right)\right\}$.

定义2　开放性[10]　OSR可以从定量角度定义问题的开放程度——开放性,表达式为:

$$O=1-\sqrt{\frac{2\times\left|C_{TR}\right|}{\left|C_{TA}\right|+\left|C_{TE}\right|}} \tag{1}$$

其中,$\left|C_{TA}\right|$,$\left|C_{TR}\right|$,$\left|C_{TE}\right|$分别表示需要被识别的类别数(即该类样本经过分类器可以分到正确的类别中)、训练集中的类别数以及测试集中的类别数. 式(1)中,O的值越大表示问题的开放程度越高,$O=0$则是封闭环境下的问题. 但是Scheirer et al[10]没有给出$\left|C_{TA}\right|$,$\left|C_{TR}\right|$,$\left|C_{TE}\right|$之间的关系,而文献[12, 14−16]使用了一个假设$C_{TA}=C_{TR}\subseteq C_{TE}$. 在进一步的研究中,Cardoso et al[17]给出了更加接近真实情况的假设$C_{TA}\subseteq C_{TR}\subseteq C_{TE}$,但这样的假设中很容易出现$O<0$的情况,这显然是不合理的. 为解决这个问题,Geng et al[11]重新给出开放性的定义:

$$O^*=1-\sqrt{\frac{2\times\left|C_{TR}\right|}{\left|C_{TR}\right|+\left|C_{TE}\right|}} \tag{2}$$

因为$C_{TA}\subseteq C_{TR}$,所以可用式(2)替换式(1),从而有效避免$O<0$的情况出现,而且,在很多情况下C_{TA}的数量是不能确定的.

定义3　开放空间风险[10]　假设S_O是一个包含开放空间O(包括远离KKCs和KUCs的样本)以及所有正训练样本(包括KKCs和KUCs的样本)的大空间,将开放空间风险定义为:

$$R_O(f)=\frac{\int_O f(x)\mathrm{d}x}{\int_{S_O} f(x)\mathrm{d}x} \tag{3}$$

$f(x)=1$表示样本x分到KKCs中. 开放空间风险是开放空间样本被标记为正样本以及整个空间被标记为正样本的比例,可以得知,在开放空间中越多的样本被标记为KKCs,R_O越大.

定义4　开放集风险[10]　给定训练集T,开放集风险可以表示为:

$$R_o(f)+\lambda_r R_\varepsilon(f(T)) \tag{4}$$

$$\underset{f\in H}{\operatorname{argmin}}\left\{R_o(f)+\lambda_r R_\varepsilon(f(T))\right\} \tag{5}$$

式(4)中,R_O表示开放空间风险,R_ε表示经验风险,λ_r是正则化常数.如式(5)所示,为解决OSR问题,通常是找到一个合适的模型f来最小化开放集风险(即在减小开放空间风险的同时平衡经验风险).

1.3 开放集识别的相关领域研究

1.3.1 零样本学习(Zero-shot Learning,ZSL) 零样本学习是近些年来机器学习领域一直关注的热点,与OSR问题的设定有极大的关联.在一些特殊的环境下,某些类的训练样本很难获得,但可以通过某些途径获得这些类相关的辅助信息(语义信息和属性信息等)来帮助识别这些类.用1.2.1的样本类别可以对零样本学习进行重新描述.对于零样本学习,训练过程中的训练样本属于KKCs,测试集中的样本属于UKCs,零样本学习的目的是通过建立一定的模型实现对UKCs的分类,建立模型的过程中可以借助KKCs和UKCs的辅助信息.

2009年,Palatucci et al[7]正式提出零样本学习(ZSL)的概念,此后有大量的工作在语义空间[18−22]或嵌入空间[23−25]对零样本学习进行了研究.虽然零样本学习已经比以前的封闭环境下分类的设定更加现实,但是辅助信息的获取不是一个容易的过程,大量的属性都是通过人工标注的形式获取.并且零样本学习只考虑了测试集包含UKCs的状况,而在真实的情况下,无法提前知道测试样本是属于KKCs还是UKCs,这也进一步延伸出G-ZSL问题[26].

1.3.2 一类样本分类问题 一类样本分类问题[27−29]专门用来应对测试集中出现新类的情况.在测试过程中可以使用一类样本分类器识别样本是否属于KKCs,这也属于异常值检测问题,其最终的目的是拒绝不属于KKCs的类.但是,可以发现一类样本分类问题在分类的过程中将所有的KKCs都当成一类,也就是说,分类器虽然可以识别UUCs,但不能把KKCs中的类别分开(图1中的数字类“1”“2”“3”“4”“5”看作一类)[27−28].针对无法分类KKCs的情况,Tax and Duin[29]提出对每个KKC都建立一个一类分类器,但是最终效果并不理想.一类分类问题的出现,一定程度上为OSR问题的提出奠定了基础.

1.3.3 开放世界识别 开放世界识别是OSR的一个扩展.通常情况下,OSR是个静态的集合概念,但是,为了更加接近现实情况中环境的不断变化,数据集应该是动态的,系统必须不断检测并添加新的类别.因此,Bendale and Boult[30]提出开放世界识别的概念,希望解决开放世界识别的系统一共能完成三个过程:首先,该系统能够检测新类(UUCs),即OSR的问题;其次,对识别的新类(UUCs)进行标记并选择合适的新类(UUCs)将其加入到已知类(KKCs)中;最后是一个增量学习的阶段,根据更新的已知类(KKCs)数据集对之前的模型进行一个更新.当然,这些过程应该是自动完成的.虽然这里将开放世界识别问题当作一个单独的问题进行描述,但是因为它相当于给OSR问题提供了一个更好的研究方向,并且其本身解决了OSR的问题,因此,针对开放世界问题的算法也会总结到下一节OSR算法中.

2 开放集识别算法研究进展

本节按照模型建立、度量选择、增量特点的角度对开放集识别算法进行总结,同时介绍开放集算法关于极值理论(Extreme Value Theory,EVT)和PAC(Probably Approximately Correct)的理论研究(如图2所示).

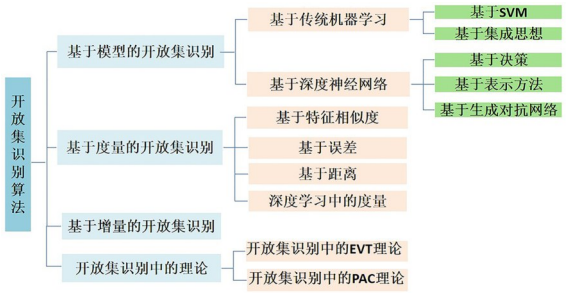


图2 开放集识别算法的分类

Fig. 2 The classification of Open Set Recognition

2.1 基于模型的开放集识别 从建立模型的角度出发介绍基于传统机器学习的和基于深度神经网络的OSR算法.现实生活中,图像识别、自然语言处理等领域的快速进步都离不开机器学习和深度神经网络的发展,因此,研究者在考虑OSR

问题时,大多从现有的机器学习算法和深度神经网络入手,改进算法使其适应开放环境.

2.1.1　基于传统机器学习的开放集识别　传统机器学习方法在封闭环境下的识别问题上取得了巨大成就.封闭环境下的识别问题通常假设训练集数据和测试集数据的类别一致,不存在UUCs的情况.然而,OSR的设定是测试集存在训练集中没有的类别,即存在UUCs.因此,适应封闭环境下的传统机器学习方法不能直接应用于OSR问题.近年来,大量研究者将开放空间风险应用于传统机器学习方法,使其拥有了处理UUCs的能力.这里主要介绍两种基于传统机器学习的OSR算法:一种是基于支持向量机机制(Support Vector Machine,SVM)[31]的OSR,另一种是融合了多种传统机器学习的基于集成思想的OSR.

2.1.1.1　基于SVM的开放集识别　SVM是一种通过构造超平面实现正负样本分类的算法,被广泛地应用于分类识别任务中.传统的SVM算法是在训练集类别和测试集类别相同的情况下设计的,所以在训练过程中构造的超平面可以有效地对测试集样本进行分类.然而,针对OSR问题,由于构造的超平面忽略了UUCs,导致UUCs在决策过程中会分到KKCs的决策空间(如图1b所示,UUCs分类错误),SVM算法的分类效果明显下降.为解决这个问题,研究者通过约束KKCs所占空间,提出了大量针对OSR的SVM算法.

Scheirer et al[10]在定义开放集风险的基础上提出了一种新的机制"1-vs-set".该算法基于带有线性核函数SVM算法,通过约束KKCs占据的空间减小开放空间风险.具体地,算法在核空间中构造另一个超平面,该超平面与SVM形成的超平面平行,两个超平面之间会形成一定距离的空间(如图3所示),此距离空间重新划定了KKCs的决策空间.具体的开放空间风险为:

$$R_O=\frac{\delta_\Omega-\delta_A}{\delta^+}+\frac{\delta^+}{\delta_\Omega-\delta_A}+p_A\omega_A+p_\Omega\omega_\Omega \tag{6}$$

式(6)包括了过度泛化风险$\frac{\delta_\Omega-\delta_A}{\delta^+}$以及过度专业化风险$\frac{\delta^+}{\delta_\Omega-\delta_A}$,这充分保障出现新类时模型会减小开放空间风险以及平衡经验风险.

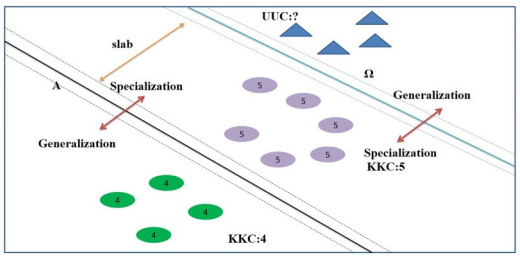


图3　线性1-vs-set机制

Fig. 3　Linear 1-vs-set machine

δ_A,δ_Ω表示各自对应平面的边缘距离,δ^+表示两个超平面之间的距离(这个距离可以包含所有的正样本数据),ω_A,ω_Ω对应两个边缘空间,p_A,p_Ω是人为定义的两个权重参数.使用新加的超平面可以有效限制KKCs占有的空间,测试样本如果在两个超平面之间就可以被分到正确的类别中,否则将根据样本靠近的超平面界限去划分到其他KKCs或者UUCs中.该算法本质上是针对开放集特性利用超平面限制KKCs空间过度占用.与此想法相似,Cevikalp[32]提出使用最佳拟合平面算法来使每个超平面接近某一类样本,远离其他类样本.Cevikalp and Triggs[33]提出一组准线性多面体二次曲线判别算子,它的正样本区域是$L1$球型.这类线性算子可以通过非对称分类器为某类正样本生成更加紧凑、约束良好的决策边界.

Scheirer et al[10]的算法虽然能减小KKCs占据的空间,但这只是相对减小,每一类KKC占据的空间仍然是无界的.Scheirer et al[12]尝试将非线性核函数引入算法,通过用有限测度对样本进行标记来进一步限制开放空间风险.之前的算法适用于解决开放环境中的单类识别问题,因此进一步在1-vs-set的基础上提出针对开放环境中的多类识别问题[12].具体地,针对OSR问题提出紧凑衰减概率(Compact Abating Probability,CAP)模型[12],在该模型中,越靠近开放空间的样本属于此KKC的概率越低.同时,利用CAP模型和EVT理论[34]进行概率估计,提出韦伯校准SVM(Weibull-calibrated SVM,W-SVM)[12].该方法由一元SVM和二元SVM组成.样本首先经过第一个结合CAP的一元SVM模型产生一个后验概率$P_O\left(y\middle|x\right)$,如果这个概率小于阈值$\delta_\tau$,样本就会被拒绝.否则,样本会经过第二个结合CAP的二元

SVM,产生一个对应KKC正样本的后验概率$P_\eta\left(y\middle|x\right)$(基于韦伯分布)和一个KKC负样本的后验概率$P_\psi\left(y\middle|x\right)$(基于逆韦伯分布).将问题进行形式定义一个指标变量:

$$l_y=\begin{cases}1, P_O\left(y\middle|x\right)>\delta_\tau\\0, \quad \text{otherwise}\end{cases} \tag{7}$$

对所有已知类别,多类W-SVM可以表示为:

$$y^*=\underset{y\in H}{\operatorname{argmax}}\, P_{\eta,y}(x)\times P_{\psi,y}(x)\times l_y \tag{8}$$

其中,$P_{\eta,y^*}(x)\times P_{\psi,y^*}(x)\geqslant\delta_R$,$\delta_R$是阈值,由具体问题的开放性定义为:

$$\delta_R=0.5\times openness \tag{9}$$

由于缺乏UUCs的先验知识,*openness*(开放性)在很多场景下无法确定.

如果算法可以准确地对任何KKCs的正样本建模而不出现过拟合的情况,那么即使存在UUCs,算法也可以有效拒绝UUCs. 基于这一思想,Jain et al[27]提出PI-SVM算法. PI-SVM是以多分类SVM为基础,并用EVT对决策边界上的正训练样本进行建模. PI-SVM与W-SVM一样是基于阈值的方法,但是基于阈值的方法有几点限制:首先,这种基于阈值的方法通常假设对于所有KKCs阈值都是一样的,这显然不合理;其次,阈值的设定与开放性相关,但在开放环境中UUCs的先验知识很难获得;最后,有些阈值的设定是根据经验确定的,缺乏理论支持. 因此,这种思想在开放集的效果上受到一定的局限.

为了突破现有的基于阈值方法的局限性,Scherreik and Rigling[35]引入POS-SVM分类器,该分类器根据定义2经验确定每个KKC的唯一拒绝阈值. Geng and Chen[16]提出基于HDP(Hierarchical Dirichlet Process)[36]的CD-OSR(Collective Decision-based OSR)模型,该算法不用设定分类KKCs和UUCs的阈值,而是引入了一些控制相应类中子类数量的阈值.

2.1.1.2 基于集成思想的开放集识别 许多OSR算法都是在某一种传统机器学习算法的基础上提出,因此,模型会受到单一算法的局限. 在封闭环境下,研究者已经通过将不同的方法进行融合实现了更加可靠的分类. 最近,从集成思想的角度出发,研究者们提出了一系列融合多种算法的OSR[37-39].

在某个特定任务中,KKCs和UUCs来自不同的数据分布,研究者采用集成思想针对KKCs和UUCs特征差异性做了大量研究. Vareto et al[37]在人脸识别任务上结合哈希函数和分类方法,并通过实验展示测试探测样本时响应值直方图对KKCs和UUCs的不同表现. Dong et al[38]提出一种将测试样本划分为已知、未知和不确定域的域划分算法,通过概率统计方法bootstrapping进行初始的域划分,然后引入Kolmogorov-Smirnov(K-S) Test进行微调得到最终的域划分. 另外,bootstrapping和K-S Test首次被引入挖掘和微调每个域的决策边界中.

同时,Neira et al[39]在考虑UUCs的前提下,将不同的分类器和特征结合起来. 具体做法是将一个新提出的基于开放集图的最优路径树分类器(Open-Set Graph-Based Optimum-Path Forest,OSOPF)、遗传算法(GP)和多数投票融合技术结合在一起. OSOPF学到更加富有弹性的未知类和离群点边界;GP结合不同问题的特征设置合适的相似度函数并在早期融合阶段提供一个更加鲁棒的分类器;多数投票法通过晚期融合技术结合不同分类器和特征的结果. 但该方法也存在不足:目前只致力于集成特定的类,而不致力于每个分类器的置信度,导致最终的分类效果不均衡.

2.1.2 基于深度神经网络的开放集识别 深度神经网络因其强大的学习表示能力被应用于许多分类识别任务. 但是,深度神经网络处理分类问题时存在一个巨大的挑战,即网络倾向于对与任务无关的数据产生高置信度的输出[40],因此,如果直接把深度神经网络引入OSR的问题,分类器的识别效果必然会受到影响,KKCs的识别准确率降低. 所以,调整深度神经网络使其适应开放环境也是研究者们关注的一个热点. 下面从基于决策、基于表示方法以及基于生成对抗网络三个角度介绍OSR的相关工作.

2.1.2.1 基于决策的开放集识别 深度神经网络一般利用SoftMax层输出各类别概率,预测样本类别. 然而,SoftMax层对输入向量进行标准化操作后,会使其预测的各类别概率之和为1,这在

本质上规定了它的封闭特性. 在现有实验设定中,与任务无关的数据一般分为“Fooling”样本和对抗样本,前者虽然在视觉上远离期望的类,但是分类器会产生很高的置信度;后者在视觉上与期望的类一致,分类器也会对其产生很高的置信度,但是这种高置信度是不正确的. 文献[41－43]证明这两种样本都会干扰深度神经网络. 因此,针对上述问题,研究者提出了不同的解决方案.

Bendale and Boult[44]通过引入OpenMax层估计未知类的概率,提出一种适用于OSR的深度神经网络方法. 具体地,首先,带有SoftMax层的深度神经网络通过最小化交叉熵损失函数进行训练,算法采用最近类平均的概念[45－46]将每个类表示为平均激活向量(MAV),激活向量的平均值(仅用正确分类的训练样本)位于该网络的倒数第二层. 然后,计算所有正确分类正训练样本与相应类别MAV的距离,并将其用于拟合每个类别的单独韦伯分布. 此外,根据韦伯分布拟合重新分配激活向量的值用于计算UUCs的伪激活,最后在这些新的重新分配的激活向量上再次使用SoftMax层计算KKCs和(伪)UUCs的类概率.

使用OpenMax可以自动拒绝许多开放环境下的UUCs样本及Fooling样本,但Rozsa et al[47]认为OpenMax与SoftMax一样容易受到比较复杂生成对抗技术的影响,因为这些技术直接作用于深层的表示. 因此,深层表示的改进也能促进OSR的发展. 基于深层表示的方法在下一小节进行详细的描述.

此外,Venkataram[48]将OpenMax引入文本分类的研究,解决了开放环境下的文本分类任务. 同样用于文本分类,Shu et al[49]认为OpenMax是通过减少每个已知类的开放空间达到拒绝未知类的目的,这种拒绝方式很薄弱,因此提出一个深度开放分类器(DOC)模型. DOC模型用1-vs-rest层(包含对应可见类的所有sigmod函数)代替OpenMax层,这给所有其他类(其余可见类和未见类)提供了一个合理的表示,使每一类形成一个合理的边界. 并且,算法用高斯拟合收紧决策边界,可以进一步降低被拒绝的开放空间风险.

Yang et al[50]提出卷积原型网络(Convolutional Prototype Network,CPN),其中,卷积神经网络继续用于表示学习,但在最终输出类别概率时,CPN用原型模型代替之前的SoftMax层,并设计了新的判别损失和生成损失,从而达到增大类间距离并减小类内距离.

OSR的方法大多是从KKCs的角度出发,在训练样本的嵌入空间上拟合一个概率分布,并根据这个概率分布检测异常值. 这种方式对KKCs的分类比较有效,但对UUCs的识别效果一般. Zhang et al[51]引入一个基于流的密度估计器来进一步检测样本是否属于UUCs.

2.1.2.2　基于表示方法的开放集识别　现有的基于深度神经网络的分类器都以监督学习的形式对KKCs进行训练,分类器能有效学习KKCs的样本表示,但这个表示对UUCs不适用. 为了能更合理地表示样本,研究者提出一系列有利于解决OSR问题的表示方法[17,52－53].

Cardoso et al[17]提出基于失重神经网络模型的精细距离计算的OSR方法,利用对未知数据和存储的知识之间的相似性进行分级的分类器,从训练样本中计算出对不属于任何KKCs的观测值的相似性的估计,此估计值用于定义属于KKCs的观测值和可能的异常值之间的边界. 这种相似性等级类似于后验概率,但不依赖于关于类的先验概率分布的假设. Yoshihashi et al[52]将有监督的分类网络和无监督的重构网络联合起来提出CROSR (Classification‐Reconstruction Learning for OSR)算法,利用重构过程中的潜在表示,补充在有监督分类过程中丢失的一些特征. 这些特征可能对KKCs的分类不重要,但可能是区别KKCs与UUCs的关键,补充重构特征可以更好地区分KKCs和UUCs样本. Hassen and Chan[53]也提出一种表示,在这个表示中,来自同一类的样本彼此靠近,来自不同类的样本相对疏远. 算法选择深度神经网络的最后一层线性层(将该层的输出作为SoftMax层的输入)的输出$\vec{z}_i$作为输入样本$\vec{x}_i$的投影表示,在此表示空间,利用基于距离的损失函数,增大不同类样本之间的距离,减小同一类样本之间的距离. 虽然有大量的算法寻找一个合适的表示方法去区分KKCs和UUCs,但是由于每个任务中KKCs与UUCs判别信息差异比较大,

这对研究者来说仍然是一项挑战.

变分自动编码器(Variational Auto-Encoder, AE)作为一种能够有效识别UUCs的手段被广泛应用,但它不能对KKCs提供有区别的表示. Sun et al[54]提出一种新方法:条件高斯分布学习(Conditional Gaussian Distribution Learning, CGDL),在VAE的基础上,除了有效检测UUCs,还通过强制不同的潜在特征来逼近不同的高斯模型,对已知样本进行分类. Perera et al[55]使用自监督方法捕获更高级的特征,如语义和结构属性,这给KKCs和UUCs的识别带来了更多的有用信息.

2.1.2.3 基于生成对抗网络的开放集识别 生成对抗网络(Generative Adversarial Networks, GANs)作为一个深度神经网络结构,在许多问题的解决上都取得了巨大的成就. 生成对抗网络通常包含一个生成器和一个判别器,生成器产生生成样本,试图使判别器无法识别出此样本是由生成器生成. 目前,大量的工作也基于生成对抗的思想对OSR问题做了进一步研究.

在以前的许多方法中,UUCs是根据特征或对KKCs的决策距离进行判断,没有对UUCs进行直接表示. 并且,OpenMax方法虽然根据KKCs的激活分数估计了UUCs的伪概率,达到拒绝效果,但实质上没有考虑UUCs的先验知识. 因此,为了能显式地对UUCs进行建模和决策得分,Ge et al[56]提出新的算法G-OpenMax,对OpenMax方法进行扩展,利用GANs合成新的类别图像直接估计UUCs概率,合成样本是由潜在空间中KKCs的混合分布生成. 这种方法不仅克服了伪概率估计的不足,还能可视化KKCs样本和UUCs样本. 但实验证明,G-OpenMax虽然可以在单色数据集上提高OSR的性能,却在自然图像上性能没有明显提升.

使用生成对抗思想可以很好地进行数据扩充,Neal et al[57]借助GANs对训练集样本进行扩充,提出了反事实图像生成(Open Set Learning with Counterfactual Images, OSRCI). OSRCI用一个编码-解码的生成对抗网络生成合成的开放集样本,这些样本很接近KKCs但不属于任何KKC. 采用这种数据扩充的方式,还进一步把OSR问题定义为多加了UUCs一类的分类器问题. 使用生成对抗网络不仅能生成负样本,还可以生成正样本进行数据扩充. Yu et al[58]提出对抗样本生成(Adversarial Sample Generation, ASG)框架,不仅可以生成KKCs的负样本作为UUCs样本,同时,如果KKCs样本比较少的话,也可以产生KKCs的正样本. 从上述工作可以看出,研究者付出了很多努力来构建一个负样本集或为目标集设置一个最优阈值. 在最近的工作中,Yang et al[15]基于GANs,用生成器生成与目标样本高度相似的样本并自动作为负的样本集,还重新设计了判别器以输出多个类别和一个UUCs. Ditria et al[59]提出一种开放集GAN体系结构(OpenGAN),为每个输入样本嵌入一个来自度量空间的特征. 使用类别等级和细粒度语义信息的最先进的度量学习模型,能够生成在语义上与给定的源图像相似的样本. 由度量学习模型提取的语义信息转移到分布之外的新类,允许生成模型生成不在训练分布之外的样本,通过这种方式,便可产生高质量的图像样本.

2.2 基于度量的开放集识别 为解决OSR问题,研究者从度量问题的角度出发,检测新样本与已有样本之间的统计特性,如特征相似度、误差、距离度量以及深度学习中的度量等.

2.2.1 基于特征相似度 Fei and Liu[60]将基于中心的相似度学习(Center-Based Similarity, CBS)[61]引入OSR模型,成功降低了模型的开放空间风险. 具体地,在CBS算法中,对一个二分类的文本分类问题,将文本的特征向量 $\vec{d}_i=\{x_1^i, x_2^i, \cdots, x_p^i\}$ 转化为基于中心的相似度空间特征向量 $\overrightarrow{v_i}=\left\{s_1^i, s_2^i, \cdots, s_p^i \middle| s_j^i=Sim\left(x_j^i, c_i\right)\right\}$,其中 Sim 是相似度函数,c_i 是第 j 类样本的中心点. 然后,OSR问题会进一步基于相似度特征解决. 在此计算中,文档的特征可以用不同的特征空间表示产生不同的样本中心点,也可以采用不同的相似度函数计算相似度. 本质上,基于CBS算法,模型以相似度为特征形成正样本和负样本的决策边界,投影到原始的文档空间中则相当于形成一个封闭的球形边界将正训练样本包围起来. 因此,该算法可以在SVM形成的决策边界的基础上进一步约束正样本的占有区域.

2.2.2　基于误差　近年来,大量基于稀疏表示的分类与恢复算法[62−63]被提出.特别地,研究者对基于稀疏表示的分类算法(SRC)[64]进行了大量研究.为了适应OSR问题,Zhang and Patel[14]提出一种基于广义稀疏表示的分类算法SROSR(Sparse Representation-based Open Set Recognition),利用类重构误差进行分类.由于OSR的判别信息都隐藏在匹配重建误差分布和非匹配重建误差分布之和的尾部,作者引入统计极值理论对两种误差的分布的尾部进行建模.具体做法分为两步:第一步,用EVT对两个分布进行建模,将OSR问题化简为假设检验问题;第二步,计算测试样本的重建误差并融合基于两个尾部分布的置信度分数来确定测试样本的类别.实验证明,SROSR具有很强的解决OSR问题的能力.

2.2.3　基于距离　距离是衡量相似度的一个重要指标,但是传统的基于距离的分类器在开放环境下的分类效果并不理想.因此,Bendale and Boult[30]通过扩展NCM(Nearest Class Mean)分类器[45−46],提出最近非离群点算法(Nearest Non-Outlier,NNO).NNO根据测试样本与KKCs均值之间的距离进行分类,并且只有当所有分类器都拒绝测试样本时,该测试样本才会被拒绝.为优化距离的计算,研究者也做出了许多努力.在人脸识别任务中,对于未知样本会提供一个图像集合(Query Set)用来识别结果;同样,每个已知类样本也形成一个图像集(Gallery Images Set).Cevikalp and Yavuz[65]提出一个快速和准确地计算Query Set与Gallery Set之间距离的方法Polyhedral Conic Classifier,可以通过简单的点乘高效地计算距离.

基于最近邻(NN)算法,Júnior et al[66]提出开放集最近邻(OSNN)方法,具体介绍了两种适应开放环境的NN分类器的扩展.第一种是OSNN类验证(OSNN Class Verification,OSNNcv),该方法的思想是在预测阶段选出测试样本s的两个最近邻.如果两个具有相同的标签t,则把标签t分给测试样本s,否则测试样本会被分到UUCs当中.在这个算法中,如果测试样本离训练样本很远,则无法被分到UUCs当中,为了解决这个问题,使用最近邻距离比率算法(Nearest Neighbor Distance Ratio,NNDR).该方法的特点在于不是直接对某一最相似类的相似性得分设置阈值,而是对两个最相似类的相似性得分比率设置阈值.测试样本s两个不同的最近邻u和t,计算$R=d(s,t)/d(s,u)$,如果R小于阈值τ,s被分为和t相同的标签,否则就会被分到UUCs.该方法也存在一个固有的缺点,因为只选择来自不同类的两个参考样本进行比较,所以当有异常值存在时,该方法的效果会受到很大的影响.

2.2.4　深度学习中的度量　上述方法都是基于传统机器学习的度量OSR方法,其实在深度学习方法中也有基于度量问题的OSR算法.在开放环境下,通常希望利用深度学习使样本的特征表示有两种特性:一是使来自同一类别的样本彼此靠近;二是使来自不同类别的样本相隔比较远.基于这个思想,Hassen and Chan[53]提出一种基于神经网络的表示方法和一种基于度量的损失函数解决OSR问题.该损失函数在训练过程中或者计算异常值得分时不用转换度量函数,都使用同一个距离函数进行度量.Mayer and Drummond[67]强调深度度量学习[68−74]在OSR的重要性.深度度量学习不同于传统的分类模型,利用带有SoftMax分类器的CNN,深度度量学习算法学习从图像空间到特征嵌入空间的转换,其中度量距离特指语义相似度.文献[68−74]的工作展示了深度度量学习强大的迁移能力并解释了样本特征是基于类的,即使这些类不在训练样本的分布中.此外,Shu et al[75]提出一种基于原型的开放式深度网络用于OSR任务,即通过使用原型模块和原型半径模块训练类别和原型半径的原型,将原型学习引入到OSR任务中,然后采用基于原型的距离度量方法检测未知类.基于样本与所有原型之间的统计信息,即样本与所有原型之间的距离,一定程度上打破了Júnior et al[66]的NNDR算法只选择不同两类的限制,不容易受到异常值的影响.基于原型的方法旨在寻找每个类的原型点,即所有属于这类的样本点与该原型点距离尽可能近.Chen et al[76]提出不同的想法,探索类以外的空间,并提出反向点(Reciprocal Points)的概念代表每个额外类空间,借助这些反向点,间接地将未知

信息引入只有KKCs的学习,从而学习更紧凑、更具区别性的表征. Chen et al[77]还进一步对上述方法进行改进,并进行了丰富的实验验证.

2.3 基于增量的开放集识别 在开放世界识别框架[30]中,为了使研究环境发生动态变化而更加接近现实世界,研究者递增地向系统增加新类和检测来自UUCs的样本,同时不断地更新KKCs的模型. 更新模型的过程中会出现一个非常现实的问题:每当有新的样本出现时模型就需要从头训练,这将是一个计算量巨大、消耗过度的过程,更严重的是,由于UUCs样本数量过少,重新训练的模型很大程度上会出现过拟合的现象. 在此基础上,研究者希望系统具有增量学习的特性,即每当检测出新类样本时,更新模型不需要重新训练,只需在原来的基础上进行调整,这样能降低整个模型的训练成本. De Rosa et al[78]提出采用在线增量学习的方式对三种非参算法进行扩展,并且制定了在线的度量学习和阈值增量更新算法. 其中,算法对NNO[30]进行扩展,进行置信度和阈值的更新:

$$C_y\left(x_t,\theta^t\right)=\exp\left(-\frac{1}{2\theta^t}dw^t\left(x_t,\mu_y^t\right)\right) \tag{10}$$

$$\theta^{t+1}=\left(1-\frac{1}{t}\right)^t+\frac{1}{t}\sum_{y\in H}dw^t\left(x_t,\mu_y^t\right) \tag{11}$$

式(10)中,$C_y\in[0,1]$表示在第t步样本x_t被分到类别y的置信度,w^t表示度量矩阵,θ表示参数. 式(11)用所有类平均值距离的期望值进行更新. 假设τ为阈值,当$C_{y^*}\leqslant\tau^t$时,即最大的置信度都小于阈值,则x_t为UUCs. 其中,阈值也要进行增量更新,阈值的更新方程为:

$$\tau^{t+1}=\begin{cases}0, & y_t\in\text{UUCs}\\ \left(1-\dfrac{1}{t^*}\right)\tau^t+\dfrac{1}{t^*}C_{y_t}\left(x_t,\theta^t\right), & \text{otherwise}\end{cases} \tag{12}$$

其中,t^*是添加了新样本之后的训练样本数. 但是由于算法在进行阈值设定时采用了类平均值,忽略了数据的分布,在进行理论推理的过程中会限制推理的质量.

基于增量的OSR思想也用于深度神经网络中,Venkataram[48]提出基于卷积神经网络的增量开放集算法,实验证明该算法能够处理UUCs的文本文档. Shu et al[75]设计了原型学习深度网络,该网络在检测到UUCs样本之后,手动地对样本进行标注,并利用这些标注好的UUCs样本对网络进行更新. 网络的分类器会根据新样本和原型之间的距离分布进行初始化,具体的过程:首先,计算新样本和原型之间的距离分布,然后利用均值归一化得到一个权值分布,最后根据权值分布对新的预测器进行权重初始化. 每一类在网络中新的权重更新为:

$$w_{N+1}=\frac{1}{N}\sum_{n=1}^{N}\alpha_n\times w_n \tag{13}$$

其中,N为当前的类别数,$[\alpha_1,\alpha_2,\cdots,\alpha_N]$为归一化之后的权值分布,$\sum_{n=1}^{N}\alpha_n=1$.

2.4 开放集识别中的理论 现有的学习算法在学习识别函数时很少或根本不考虑分布信息,这样会使算法缺乏较强的理论基础,并且有些算法很难从理论的角度证明其识别未知类的能力.

2.4.1 开放集识别中的EVT理论 采用增量学习的方式解决OSR问题,避免新类出现时需要重新训练模型的费用,但采用什么方式来有效地形成各类的决策边界是研究者关注的重点.

EVT[34]规定一个点相对于另一类点的径向包含概率的函数形式,换句话说,是通过选择最能概括每一类的点和分布,即相对冗余度最小的点和分布,得到每一类决策边界的紧凑概率表示. 其特征是其极值向量(EV),它提供一个关于开放空间风险的递减界,新数据到达时可以有效地更新这些EV,从而进一步表示每一类决策边界.

基于这个重点,Rudd et al[79]提出EVM模型,该模型考虑分布信息,将EVT理论引入分类器的构造中以获得更加紧凑的统计模型. 作为间隔分布理论从每个类公式到逐样本公式的扩展,EVM是根据样本点相对于参考点的样本半距离分布来建模的,具体包含以下定理:

定理1 假设可以从一个合理定义的类分布中选择出一个正样本x_i和丰富的负样本x_j,产生成对的边缘估计m_{ij},并假设一个连续的非退化的边缘分布,然后用韦伯分布便可给出x_i边距最小值的分布.

利用定理1,每个点x_i都可以估计它自己到边缘的距离分布,从而产生:

推论1　Ψ密度函数　利用定理1给出的条件,可以推出x^*包含在x_i估计的边界中的概率:

$$\Psi\left(x_i,x^*,\kappa_i,\lambda_i\right)=\exp^{-\left(\frac{\left\|x_i-x^*\right\|}{\lambda_i}\right)^{\kappa_i}} \tag{14}$$

其中,$\left\|x_i-x^*\right\|$是x^*与x_i之间的距离,κ_i,λ_i是最小m_{ij}拟合得到的Weibull形状和尺度参数.

决策函数:一旦EVM的训练过程完成,一个新样本x^*属于类C_l的概率便可以由式(14)得到,因此会产生以下的决策函数:

$$y^*=\begin{cases}\text{argmax}_{l\in\{1,\cdots,M\}}\hat{P}\left(C_l\middle|x^*\right), & \text{if } \hat{P}\left(C_l\middle|x^*\right)\geqslant\delta\\ \text{UUCs}, & \text{otherwise}\end{cases} \tag{15}$$

基于边缘分布和极值理论,EVM有很好的解释能力,可以进行非线性无核变带宽增量学习,进一步用于探索开放集人脸识别[80]和入侵检测[81].

同时,EVT理论也用于其他算法中.由于OSR的判别信息都隐藏在匹配重建误差分布和非匹配重建误差分布之和的尾部,Zhang and Pater[14]的SROSR算法在基于广义稀疏表示上引入EVT理论对两种误差的分布的尾部进行建模.同样,Oza and Pater[82]提出一种新的基于深度卷积神经网络的OSR算法,该算法的解码器网络的重建误差被用于开放集的拒绝,为了提高整体性能也利用EVT对已知类的重建误差分布尾部进行建模.Mundt et al[83]还将EVT理论运用到分布外数据(OOD)检测,在能推出模型不确定性的深度神经网络的基础上,结合基于OSR的EVT算法,限制模型开放空间风险.

虽然EVT理论被许多研究者引入解决OSR问题,但是,如果KKCs和UUCs的几何结构不同,简单的识别任务也会失败.为了克服这一局限,Vignotto and Engelke[84]提出两种新的算法,这两种算法的思想是采用不基于已知类几何表示的EVT近似-GPD分类器和GEV分类器.

2.4.2　开放集识别中的PAC理论　在一般开放集问题的假设下,很少有算法能保证其检测UUCs的能力.因此,Liu et al[85]通过引入PAC理论,从概率的角度对模型从理论方面重新进行设计.该算法能实现具体的UUCs检测率,如能成功检测95%的UUCs.假设存在一个KKCs的分布D_0,可以从D_0中生成一个训练集S_0,同时还存在一个混合分布D_m,D_m是KKCs分布D_0和UUCs分布D_a的混合,可以从D_m中生成混合数据集S_m.注意,在D_m中,假设可以以α的概率从D_a中生成一个UUCs数据,以$1-\alpha$的概率从D_0中生成一个KKCs数据.基于以上假设,设计使用异常检测器的阈值去判断UUCs,如果异常得分大于阈值则标记样本为UUCs,否则将样本标记为KKCs.因此,问题的关键在于阈值的选择.考虑固定异常检测器异常分数的累积分布函数(CDFs),混合分布D_m的异常值得分可以表示为:

$$F_m(x)=(1-\alpha)F_0(x)+\alpha F_a(x) \tag{16}$$

由式(16)可以推出F_a的异常值得分:

$$F_a(x)=\frac{F_m(x)-(1-\alpha)F_0(x)}{\alpha} \tag{17}$$

考虑F_a的推导,通过选择异常分数阈值τ_q(F_a的q分位数)并对异常分数大于τ_q的所有测试查询发出警报,可以直接获得$1-q$(例如95%)的UUCs检测率.但在真实情况下,很难得到F_m和F_0,因此,可以通过S_m和S_0推出:

$$\hat{F}_a(x)=\frac{\hat{F}_m(x)-(1-\alpha)\hat{F}_0(x)}{\alpha} \tag{18}$$

但是,从实验结果上去看,该算法对于小数据集或者未知类占比比较小(即α比较小)的数据集存在一定的局限性.

3　实验分析

3.1　实验数据集介绍　大部分的OSR模型是针对图像识别问题设计的,因此图像数据集是OSR实验数据集的主体.目前经常用于OSR的基准数据集如表1所示.

由表可见,大部分设置将同一个数据集的类别划分为KKCs和UUCs,但是也有一部分实验,为了丰富训练集和测试集,从不同的数据集进行KKCs和UUCs的划分.OSR早期算法1-vs-set和W-SVM联合Caltech 256[94]和Image-Net[95]设置实验并用方向梯度直方图(Histogram of Oriented Gradient,HOG)[96]以及LBP-Like[97]对图像特征进行描述.Neal et al[57]提出CIFAR+10和CIFAR+50,即从CIFAR10中选择四类作为KKCs,从CIFAR100中分别选择10类和50类作为UUCs.

表 1 开放集识别的相关数据集

Table 1 Related datasets of OSR

Dataset	Abstract	Number of Instances	feature dimension	Number of classes	Number of KKCs	Number of UUCs
MNIST[86]	Handwritten Digits Images	60000	28×28	10	6	4
SVHN[87]	Color House-Number Images	630420	32×32	10	6	4
PENDIGITS[88]	Processed image features	10992	17	10	5	5
LETTER[89]	letters of an alphabet	20000	16	26	10	16
CIFAR10[90]	Color Images	60000	32×32	10	6	4
COIL20[91]	Grayscale Images	1440	16×16	20	10	10
YALEB[92]	Face Images	2414	32×32	38	10	28
Tiny-ImageNet[93]	Subset of Imagenet	100000	32×32	200	20	180

3.2 评价标准 本节介绍OSR的评价标准. 和以前封闭环境下的识别问题相比,测试集中出现了UUCs的样本,因此需要对以前的评价标准进行调整,并定义一些新的合理的评价标准.

首先,给出一些变量的定义,对于第i类KKC来说($i\in\{1,2,\cdots,C\}$,C是KKCs的类别总数),TP_i,TN_i,FP_i,FN_i分别代表分类正确的正样本数、分类正确的负样本数、分类错误的正样本数以及分类错误的负样本数.同时TU,FU分别代表识别正确的UUCs样本数和识别错误的UUCs样本数.下面给出评价指标的定义:

(1)OSR的准确率:对于一般的封闭环境下的分类器来说,准确率是一个常用的分类指标,一般可以表示为:

$$A=\frac{\sum_{i=1}^{C}\left(TP_i+TN_i\right)}{\sum_{i=1}^{C}\left(TP_i+TN_i+FP_i+FN_i\right)} \tag{19}$$

考虑OSR问题会出现UUCs,因此将UUCs分类情况考虑进去,调整之后准确率的表达式[11]为:

$$A_O=\frac{\sum_{i=1}^{C}\left(TP_i+TN_i\right)+TU}{\sum_{i=1}^{C}\left(TP_i+TN_i+FP_i+FN_i\right)+TU+FU} \tag{20}$$

上面在计算OSR准确率时是根据样本数量进行判断的,这样的评价指标无法显示分类器对于KKCs和UUCs的分类效果. 训练一个分类器时,分类器会倾向于样本数量最多的类. 在OSR中,如果UUCs的数量比较多,则分类器对UUCs的拒绝能力比较强(这种情况是成立的,随着环境开放性增大UUCs是未知的),上述的准确率也较高. 但这种情况下,分类器对KKCs的分类判断显然是不合理的,因为KKCs的准确率可能很低. 因此,Júnior et al[66]同时考虑KKCs的准确率和UUCs的准确率,给对应权重提出了标准化的准确率:

$$NA=\lambda_r AKS+\left(1-\lambda_r\right)AUS \tag{21}$$

$$AKS=\frac{\sum_{i=1}^{C}\left(TP_i+TN_i\right)}{\sum_{i=1}^{C}\left(TP_i+TN_i+FP_i+FN_i\right)} \tag{22}$$

$$AUS=\frac{TU}{TU+FU} \tag{23}$$

式(21)中,$0<\lambda_r<1$是正则化系数.

(2)F-measure:大多数的OSR算法都用F-measure作为评价标准,它结合了精度P和召回率R,具体的计算式为:

$$F=2\times\frac{P\times R}{P+R} \tag{24}$$

F-measure对OSR的一个小扩展是将所有UUCs当作一个简单的类并以与封闭环境相同的方式获得其值,这种做法对于OSR测试的评价显然不正确. 考虑下面的情况,所有UUCs的正确分类都被认为是正确的KKCs正样本分类,但这种分类结果没有任何意义,因为在训练过程中UUCs没有用于训练分类器. Júnior et al[66]在只考虑KKCs的基础上对精度和召回率的计算进行改进,从宏平均和微平均的角度进行计算:

$$P_{ma}=\frac{1}{C}\sum_{i=1}^{C}\frac{TP_i}{TP_i+FP_i} \tag{25}$$

$$R_{ma}=\frac{1}{C}\sum_{i=1}^{C}\frac{TP_i}{TP_i+FN_i} \tag{26}$$

$$P_{mi}=\frac{\sum_{i=1}^{C}TP_i}{\sum_{i=1}^{C}\left(TP_i+FP_i\right)} \tag{27}$$

$$R_{mi}=\frac{\sum_{i=1}^{C}TP_i}{\sum_{i=1}^{C}\left(TP_i+FN_i\right)} \tag{28}$$

此外,Sokolova and Lapalme[98]提出对于F-measure来说,无论TN怎么改变其值都不会变化,但在OSR下TN是一个非常重要的变量.因此,Scherreik and Rigling[35]引入约登指数J来表示一个算法避免失败的能力[99],J越高代表这个算法越能避免失败.

(3)AUROC (Area Under the ROC Curve):开放环境的开放性是不确定的,因此需要选择直接表示分类器性能好坏的指标AUROC[57],它提供检测算法性能的无校准测量,能表示从UUCs类别很少到UUCs类别占大多数的所有情况.目前,AUROC是OSR工作中最常用的评价指标.

3.3　模型以及实验结果分析　本节对OSR算法以及实验结果进行比较分析,分为基于非深度特征的OSR算法(如表2所示)和基于深度特征的OSR算法两部分(如表3所示).引用Geng et al[11]的实验结果,表2数据代表微平均F-measure(%),表3数据为AUROC.

表2　基于非深度特征的开放集识别算法结果

Table 2　Results of OSR based the non-depth feature

Method	LETTER(O^*=0%)	LETTER (O^*=25.46%)	YALEB (O*=0%)	YALEB (O^*=23.30%)	EVT (y/n)
1-vs-set[10]	81.51±3.94	42.08±2.63	87.99±2.42	49.36±1.96	n
W-SVM[34]	95.64±0.25	85.72±0.85	86.01±2.42	84.56±2.19	y
PI-SVM[27]	96.92±0.36	84.16±1.01	93.47±2.74	88.96±1.16	y
SROSR[14]	84.21±2.49	66.50±8.22	88.09±3.41	83.99±4.19	y
OSNN[66]	83.12±17.41	64.97±13.75	81.81±8.40	72.90±9.41	y
EVM[79]	96.59±0.50	82.81±2.42	68.94±6.47	54.40±5.77	y
CD-OSR[36]	96.94±1.36	86.21±1.46	89.75±1.15	88.00±2.19	n

表3　基于深度特征的开放集识别算法结果

Table 3　Results of OSR based the depth feature

Method	MNIST (O^*=13.40%)	SVHN (O^*=13.40%)	CIFAR10 (O^*=24.41%)	Tiny-ImageNet (O^*=57.36%)	EVT (y/n)	GAN (y/n)
OpenMax[44]	98.1	89.4	81.7	57.6	n	n
CROSR[52]	99.8	95.5	—	67.0	y	n
G-OpenMax[56]	98.4	89.6	82.7	58.0	n	y
OSRCI[57]	98.8	91.0	83.8	58.6	n	y

3.3.1　基于非深度特征的开放集识别算法　基于非深度特征的OSR算法采用传统机器学习方法,依据样本进行类别判断.选择1-vs-set,W-SVM,PI-SVM,SROSR,OSNN,EVM,CD-OSR进行比较.这些算法除了基于非深度特征的算法,在建模的过程中还需要为置信度、距离比率等进行设定阈值.通过实验结果分析可以发现,CD-OSR算法的效果最好,不仅在LETTER数据集和YALEB数据集上的得分高,而且随着开放程度的增大它的效果相对来说也最稳定.原因可能是除了CD-OSR的其余算法都是基于KKCs和UUCs的决策阈值设定,在实验设置的过程中很难获得UUCs的先验知识,只能利用KKCs设置阈值,而CD-OSR算法基于HDP (Hierarchical Dirichlet Process)过程摆脱了这种限制,算法中的阈值只是用来控制过程中子类的数目.但由于HDP不适用于高维度数据,CD-OSR的效果有些许下降.同时观察到,除了1-vs-set和CD-OSR之

外的算法都引入了EVT,通过对比这些算法和1-vs-set的结果,可见引入EVT确实可以利用边缘信息解决开放识别问题;但与CD-OSR对比还可以意识到,在OSR中阈值是比较重要的因素.

3.3.2 基于深度特征的开放集识别算法 基于深度特征的OSR算法是通过深度神经网络提取样本特征做出判别. 选择OpenMax,CROSR,G-OpenMax,OSRCI进行对比,可以发现CROSR效果最好,其次是OSRCI. 并且,很明显在深度神经网络中引入生成对抗网络估计未知类达到了比较理想的效果. 虽然CROSR没有引入生成对抗网络,但是它用重构过程中的潜在表示保留了与未知类密切相关的知识.

4 开放集识别未来的研究方向与展望

作为机器学习领域新兴的热点,近几年,OSR迅速发展,在图像识别、文本分类、人脸识别等领域取得了巨大的成就. OSR是对传统封闭环境下识别问题的突破,同时,OSR算法衍生于封闭集识别算法,与传统机器学习算法和深度神经网络等方法紧密相关. 对于某些测试集出现新类的场景,可以通过OSR算法或者开放世界识别算法对新类做出拒绝反应,甚至可以通过人工标注等过程完成对新类样本的学习. 但是,因为OSR是一个新兴领域,现有的OSR算法还存在一些限制,所以本节将根据OSR算法现有的不足,讨论OSR未来的研究方向.

4.1 建立有效开放集识别模型 在最开始的OSR工作中[10],传统封闭环境下分类器所面临的最大挑战是KKCs过度占据空间. 因此在出现UUCs时,UUCs样本会被划分到KKCs的空间中,显然这并不能达到将UUCs当成单独一类处理的目的. 从这个角度出发,可以从以下三个方面解决OSR问题:

第一,通过一系列策略使KKCs形成更加紧凑的空间,在封闭环境的分类任务中,已经有工作借助聚类学习强大的约束能力为目标类形成紧密的分布区域[100−101],达到决策空间的紧凑化. 但是这项工作还没有用于OSR中,因此将聚类学习与OSR工作结合起来也是一个值得研究的方向. 第二,通过类似生成技术加强UUCs知识形成UUCs的空间,OSR在训练过程中缺少UUCs的数据,因此,文献[56−58]借助生成对抗技术生成UUCs的实例为UUCs提供先验知识,但是如何生成质量更好更接近真实数据的实例还需要结合具体实际进行研究. 第三,通过注意力机制[102]或者嵌入子空间[103]等技术增大KKCs与UUCs之间的差异性. 使用注意力机制让模型关注样本或者类别之间的不同点,选择合适的嵌入子空间,使得KKCs的样本与UUCs的样本相距比较远.

4.2 UUCs类别的处理 在现有的OSR模型中,UUCs通常会作为一类数据进行拒绝. 但是,在很多现实场景中,对UUCs进行分类也有很大的意义. 例如在故障诊断领域,故障A和故障B都属于以前系统没有出现过的情况,考虑故障A的解决需要切断系统电源,而故障B只需要切断部分电路电源,如果此时把故障A与故障B当成一类,采用切断系统电源的方式,这种做法就会造成很大的系统损失. CD-OSR使用HDP的层次过程探索UUCs类之间的关系. 因此,在这方面的研究可以结合数据的层次结构[95]或者模型的层次结构[104]通过层次搜索的方式将UUCs进行进一步的处理,以适应具体问题.

4.3 开放集识别与其他领域研究 OSR是更加接近于现实场景的一个假设,因此可以将OSR与涉及分类或者识别的领域相结合. 例如,领域自适应、增量学习、强化学习、对抗防御以及联邦学习等. 下面结合具体的领域,对OSR的研究方向进行进一步探讨.

领域自适应是迁移学习[105]的一个重要研究方向,传统领域自适应问题是训练集与测试集样本类别相同可是数据分布不同(如手写数字集与合成图像数字集),领域自适应能将在训练集中训练的模型应用于测试集中. Busto and Gall[106]通过在训练集中加入无关类,提出开放集领域自适应(OSDA)的概念. Saito et al[107]探讨了更具挑战的开放性场景,即在训练集没有无关类的情况下实现测试集中UUCs识别. 算法具体采用了生成对抗网络,不仅使两个领域的KKCs差异缩小还有效识别了UUCs. 刘晓龙和王士同[108]提出一种开放集模糊领域自适应算法,该方法通过计算目标域样本的模糊隶属度表示源域到目标域的映射,

从而逐步在同一空间下实现对目标域的分类. 为了进一步分离KKCs和UUCs,刘晓龙和王士同还在前文[107]的基础上,仅将从目标域分离出的KKCs与源域样本进行对齐[109].

开放世界识别就是将增量学习引入OSR中,开放世界识别模型不仅要求将UUCs识别出来,还要求根据人工标注等手段将UUCs加入KKCs中,将UUCs在下次模型的训练中当成KKCs进行模型的更新. 强化学习[110]是在没有任何监督的标签的情况下,通过尝试性地做出一些行为得到反馈,不断地调整之前的行为,系统就可以知道什么样子的行为是最好的结果. 在强化学习中,开放性是其特征,因此将强化学习与OSR结合起来具有很强的理论依据. 对抗防御的目的是减少网络对图像的攻击,开放环境下这种攻击会变得更加复杂. Shao et al[111]考虑开放环境下的对抗防御问题,提出开放对抗防御机制(Open-Set Adversarial Defense,OSAD). 本文已表明OSR系统容易受到对抗性攻击. 联邦学习[112]是从用户隐私的角度出发形成的新的学习领域,传统学习中不管是KKCs还是UUCs,都假设模型可以直接获得这些数据进行处理,但在实际情况中,用户不希望模型能够获得自己的数据,因此将OSR与联邦学习结合起来是未来应用领域发展的潜在要求.

5　总结

开放集识别是近几年来机器学习领域新兴的热点,它摆脱了封闭环境下训练集与测试集样本类别一致的限制,更加接近于现实环境情况. OSR假设在开放环境进行,即测试集中会出现训练集中没有的样本类别,这给传统的分类识别算法带来了巨大的挑战.

基于开放环境,OSR的任务可以包含两大部分:准确识别KKCs和拒绝UUCs,或者也可以描述为同时减少经验风险和开放集风险. 本文首先指出开放集学习的发展历程以及相关定义,并对与开放集相关的零样本学习、一类分类问题和开放世界识别问题进行了简单介绍. 然后,重点分析了近年来关于OSR领域的相关工作,并从建立模型、度量选择、增量特点进行分类,同时指出了在OSR中的两个理论:EVT和PAC. OSR作为一个新兴的领域,有许多研究方向可以继续探索. 本文指出研究者不仅可以只专注于OSR问题,还可以将OSR与现在多个领域的工作进行结合,如强化学习、联邦学习等.

随着OSR原理和模型的深入研究,解决OSR问题的算法一定会更加成熟,并可以应用于大量真实场景中,为机器学习的发展和现实场景应用做出更大的贡献.

参考文献

[1] Shaout A, Kaja N, Awad S. A smart traffic sign recognition system//2015 11th International Computer Engineering Conference. Cairo, Egypt: IEEE, 2015: 157－162.

[2] Chellappa R, Wilson C L, Sirohey S. Human and machine recognition of faces: A survey. Proceedings of the IEEE, 1995, 83(5): 705－741.

[3] Daugman J. Face and gesture recognition: Overview. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1997, 19(7): 675－676.

[4] Zhao W, Chellappa R, Phillips P J, et al. Face recognition: A literature survey. ACM Computing Surveys, 2003, 35(4): 399－458.

[5] Krizhevsky A, Sutskever I, Hinton G E. ImageNet classification with deep convolutional neural networks//Proceedings of the 25th International Conference on Neural Information Processing Systems. Lake Tahoe, Nevada: Curran Associates Inc., 2012: 1097－1105.

[6] Gregor K, Danihelka I, Graves A, et al. DRAW: A recurrent neural network for image generation// Proceedings of the 32nd International Conference on International Conference on Machine Learning. Lille, France: JMLR.org, 2015: 1462－1471.

[7] Palatucci M, Pomerleau D, Hinton G, et al. Zero-shot learning with semantic output codes//Proceedings of the 22nd International Conference on Neural Information Processing Systems. Vancouver, Canada: Curran Associates Inc., 2009: 1410－1418.

[8] Phillips P J, Grother P, Micheals R. Evaluation methods in face recognition//Li S Z, Jain A K. Handbook of face recognition. Springer London, 2011: 551－574.

[9] Li F Y, Wechsler H. Open set face recognition using transduction. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2005, 27(11): 1686－1697.

[10] Scheirer W J, de Rezende Rocha A, Sapkota A, et al. Toward open set recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2013, 35(7): 1757－1772.

[11] Geng C X, Huang S J, Chen S C. Recent advances in open set recognition: A survey. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 43(10): 3614－3631.

[12] Scheirer W J, Jain L P, Boult T E. Probability models for open set recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2014, 36(11): 2317－2324.

[13] Dhamija A R, Günther M, Boult T E. Reducing network agnostophobia//Proceedings of the 32nd International Conference on Neural Information Processing Systems. Montréal, Canada: Curran Associates Inc., 2018: 9157－9168.

[14] Zhang H, Patel V M. Sparse representation-based open set recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2017, 39(8): 1690－1696.

[15] Yang Y, Hou C P, Lang Y, et al. Open-set human activity recognition based on micro-Doppler signatures. Pattern Recognition, 2019(85): 60－69.

[16] Geng C X, Chen S C. Collective decision for open set recognition. 2020, arXiv:1806.11258.

[17] Cardoso D O, Gama J, França F M G. Weightless neural networks for open set recognition. Machine Learning, 2017, 106(9－10): 1547－1567.

[18] Romera-Paredes B, Torr P H S. An embarrassingly simple approach to zero-shot learning//Proceedings of the 32nd International Conference on International Conference on Machine Learning. Lille, France: JMLR.org, 2015: 2152－2161.

[19] Kodirov E, Xiang T, Gong S G. Semantic autoencoder for zero-shot learning//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, HI, USA: IEEE, 2017: 4447－4456.

[20] Bucher M, Herbin S, Jurie F. Improving semantic embedding consistency by metric learning for zero-shot classiffication//Proceedings of the 14th European Conference on Computer Vision. Amsterdam, The Netherlands: Springer, 2016: 730－746.

[21] Norouzi M, Mikolov T, Bengio S, et al. Zero-shot learning by convex combination of semantic embeddings. 2014, arXiv:1312.5650.

[22] Zhang Z M, Saligrama V. Zero-shot learning via semantic similarity embedding//Proceedings of 2015 IEEE International Conference on Computer Vision. Santiago, Chile: IEEE, 2015: 4166－4174.

[23] Zhang L, Xiang T, Gong S G. Learning a deep embedding model for zero-shot learning//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu, HI, USA: IEEE, 2017: 3010－3019.

[24] Frome A, Corrado G S, Shlens J, et al. DeViSE: A deep visual-semantic embedding model//Proceedings of the 26th International Conference on Neural Information Processing Systems. Lake Tahoe, Nevada: Curran Associates Inc., 2013: 2121－2129.

[25] Akata Z, Perronnin F, Harchaoui Z, et al. Label-embedding for attribute-based classification//Proceedings of 2013 IEEE Conference on Computer Vision and Pattern Recognition. Portland, OR, USA: IEEE, 2013: 819－826.

[26] Chao W L, Changpinyo S, Gong B Q, et al. An empirical study and analysis of generalized zero-shot learning for object recognition in the wild//Proceedings of the 14th European Conference on Computer Vision. Amsterdam, The Netherlands: Springer, 2016: 52－68.

[27] Jain L P, Scheirer W J, Boult T E. Multi-class open set recognition using probability of inclusion//Proceedings of the 13th European Conference on Computer Vision. Zurich, Switzerland: Springer, 2014: 393－409.

[28] Bodesheim P, Freytag A, Rodner E, et al. Kernel null space methods for novelty detection//Proceedings of 2013 IEEE Conference on Computer Vision and Pattern Recognition. Portland, OR, USA: IEEE, 2013: 3374－3381.

[29] Tax D M J, Duin R P W. Growing a multi-class classifier with a reject option. Pattern Recognition Letters, 2008, 29(10): 1565－1570.

[30] Bendale A, Boult T. Towards open world recognition//Proceedings of 2015 IEEE Conference

on Computer Vision and Pattern Recognition. Boston,MA,USA:IEEE,2015:1893－1902.

[31] Cortes C, Vapnik V. Support - vector networks. Machine Learning,1995,20(3):273－297.

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

[33] Cevikalp H, Triggs B. Polyhedral conic classifiers for visual object detection and classification// Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition. Honolulu,HI,USA: IEEE,2017:4114－4122.

[34] Kotz S, Nadarajah S. Extreme value distributions: Theory and applications. London: Impenial College Press,2000.

[35] Scherreik M D,Rigling B D. Open set recognition for automatic target classification with rejection. IEEE Transactions on Aerospace and Electronic Systems, 2016,52(2):632－642.

[36] Gershman S J, Blei D M. A tutorial on Bayesian nonparametric models. Journal of Mathematical Psychology,2012,56(1):1－12.

[37] Vareto R,Silva S,Costa F,et al. Towa rds open-set face recognition using hashing functions//2017 IEEE International Joint Conference on Biometrics. Denver,CO,USA:IEEE,2017:634－641.

[38] Dong H Z, Fu Y W, Sigal L, et al. Learning to separate domains in generalized zero-shot and open set learning:A probabilistic perspective. 2021,arXiv: 1810.07368.

[39] Neira M A C, Júnior P R M, Rocha A, et al. Data-fusion techniques for open-set recognition problems. IEEE Access,2018(6):21242－21265.

[40] Matan O, Kiang R K, Stenard C E, et al. Handwritten character recognition using neural network architectures//Proceedings of the 4th USPS Advanced Technology Conference. Washington DC, USA, 1990:1003－1011.

[41] Nguyen A, Yosinski J, Clune J. Deep neural networks are easily fooled: High confidence predictions for unrecognizable images//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Boston, MA, USA: IEEE, 2015:427－436.

[42] Goodfellow I J, Shlens J, Szegedy C. Explaining and harnessing adversarial examples. 2015, arXiv: 1412.6572.

[43] Szegedy C, Zaremba W, Sutskever I, et al. Intriguing properties of neural networks. 2014, arXiv: 1312.6199.

[44] Bendale A, Boult T E. Towards open set deep networks//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas,NV,USA:IEEE,2016:1563－1572.

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

[46] Ristin M, Guillaumin M, Gall J, et al. Incremental learning of NCM forests for large - scale image classification//Proceedings of 2014 IEEE Conference on Computer Vision and Pattern Recognition. Columbus,OH,USA:IEEE,2014:3654－3661.

[47] Rozsa A, Günther M, Boult T E. Adversarial robustness: Softmax versus openmax. 2017, arXiv: 1708.01697.

[48] Venkataram V M. Open set text classification using neural networks. Master Dissertation. Colorado Springs: University of Colorado Colorado Springs, 2018.

[49] Shu L, Xu H, Liu B. DOC: Deep open classification of text documents. 2017,arXiv:1709.08716.

[50] Yang H M, Zhang X Y, Yin F, et al. Convolutional prototype network for open set recognition. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2020, doi: 10.1109/TPAMI. 2020.3045079.

[51] Zhang H J, Li A, Guo J, et al. Hybrid models for open set recognition//European Conference on Computer Vision. Glasgow, UK: Springer, 2020: 102－117.

[52] Yoshihashi R, Shao W, Kawakami R, et al. Classification - reconstruction learning for open - set recognition//Proceedings of 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Long Beach, CA, USA: IEEE, 2019: 4011－4020.

[53] Hassen M, Chan P K. Learning a neural-network-

based representation for open set recognition. 2018, arXiv:1802.04365.

[54] Sun X, Yang Z N, Zhang C, et al. Conditional gaussian distribution learning for open set recognition//Proceedings of 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Seattle, WA, USA: IEEE, 2020: 13477－13486.

[55] Perera P, Morariu V I, Jain R, et al. Generative-discriminative feature representations for openset recognition//Proceedings of 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Seattle, WA, USA: IEEE, 2020: 11811－11820.

[56] Ge Z Y, Demyanov S, Chen Z T, et al. Generative OpenMax for multi-class open set classification. 2017, arXiv:1707.07418.

[57] Neal L, Olson M, Fern X, et al. Open set learning with counterfactual images//Proceedings of the European Conference on 15th European Conference on Computer Vision. Munich, Germany: Springer, 2018: 620－635.

[58] Yu Y, Qu W Y, Li N, et al. Open-category classification by adversarial sample generation. 2017, arXiv:1705.08722.

[59] Ditria L, Meyer B J, Drummond T. OpenGAN: Open set generative adversarial networks// Proceedings of the Asian Conference on Computer Vision. 2020.

[60] Fei G L, Liu B. Breaking the closed world assumption in text classification//Proceedings of 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies. San Diego, CA, USA: ACL, 2016: 506－514.

[61] Fei G L, Liu B. Social media text classification under negative covariate shift//Proceedings of 2015 Conference on Empirical Methods in Natural Language Processing. Lisbon, Portugal: ACL, 2015: 2347－2356.

[62] Wright J, Ma Y, Mairal J, et al. Sparse representation for computer vision and pattern recognition. Proceedings of the IEEE, 2010, 98(6): 1031－1044.

[63] Peng J T, Li L Q, Tang Y Y. Maximum likelihood estimation-based joint sparse representation for the classification of hyperspectral remote sensing images. IEEE Transactions on Neural Networks and Learning Systems, 2019, 30(6): 1790－1802.

[64] Wright J, Yang A Y, Ganesh A, et al. Robust face recognition via sparse representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2009, 31(2): 210－227.

[65] Cevikalp H, Yavuz H S. Fast and accurate face recognition with image sets//Proceedings of 2017 IEEE International Conference on Computer Vision Workshops. Venice, Italy: IEEE, 2017: 1564－1572.

[66] Júnior P R M, De Souza R M, de O Werneck R, et al. Nearest neighbors distance ratio open-set classifier. Machine Learning, 2017, 106(3): 359－386.

[67] Meyer B J, Drummond T. The importance of metric learning for robotic vision: Open set recognition and active learning//2019 International Conference on Robotics and Automation. Montreal, Canada: IEEE, 2019: 2924－2931.

[68] Schroff F, Kalenichenko D, Philbin J. FaceNet: A unified embedding for face recognition and clustering//Proceedings of 2015 IEEE Conference on Computer Vision and Pattern Recognition. Piscataway, NJ, USA: IEEE, 2015: 815－823.

[69] Song H O, Xiang Y, Jegelka S, et al. Deep metric learning via lifted structured feature embedding// Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, NV, USA: IEEE, 2016: 4004－4012.

[70] Sohn K. Improved deep metric learning with multi-class N-pair loss objective//Proceedings of the 30th International Conference on Neural Information Proceedings Systems. Barcelona, Spain: Curran Associates Inc., 2016: 1857－1865.

[71] Kumar B G V, Carneiro G, Reid I. Learning local image descriptors with deep siamese and triplet convolutional networks by minimizing global loss functions//Proceedings of 2016 IEEE Conference on Computer Vision and Pattern Recognition. Las Vegas, NV, USA: IEEE, 2016: 5385－5394.

[72] Song H O, Jegelka S, Rathod V, et al. Learnable structured clustering framework for deep metric learning. 2017, arXiv:1612.01213.

[73] Harwood B, Kumar B G V, Carneiro G, et al. Smart mining for deep metric learning//Proceedings of 2017

IEEE International Conference on Computer Vision. Venice, Italy: IEEE, 2017: 2840－2848.

[74] Meyer B J, Harwood B, Drummond T. Deep metric learning and image classification with nearest neighbour gaussian kernels//2018 25th IEEE International Conference on Image Processing. Athens, Greece: IEEE, 2018: 151－155.

[75] Shu Y, Shi Y M, Wang Y W, et al. P-ODN: Prototype based open deep network for open set recognition. 2020, arXiv:1905.01851.

[76] Chen G Y, Peng P X, Wang X Q, et al. Adversarial reciprocal points learning for open set recognition. 2021, arXiv:2103.00953.

[77] Chen G Y, Qiao L M, Shi Y M, et al. Learning open set network with discriminative reciprocal points. 2020, arXiv:2011.00178.

[78] De Rosa R, Mensink T, Caputo B. Online open world recognition. 2016, arXiv:1604.02275.

[79] Rudd E M, Jain L P, Scheirer W J, et al. The extreme value machine. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2018, 40(3): 762－768.

[80] Günther M, Cruz S, Rudd E M, et al. Toward open-set face recognition//Proceedings of 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops. Honolulu, HI, USA: IEEE, 2017: 573－582.

[81] Henrydoss J, Cruz S, Rudd E M, et al. Incremental open set intrusion recognition using extreme value machine//2017 16th IEEE International Conference on Machine Learning and Applications. Cancun, Mexico: IEEE, 2017: 1089－1093.

[82] Oza P, Patel V M. Deep cnn-based multi-task learning for open-set recognition. 2019, arXiv: 1903.03161.

[83] Mundt M, Pliushch I, Majumder S, et al. Open set recognition through deep neural network uncertainty: Does out-of-distribution detection require generative classifiers? //Proceedings of 2019 IEEE/CVF International Conference on Computer Vision Workshop. Seoul, Korea (South): IEEE, 2019: 753－757.

[84] Vignotto E, Engelke S. Extreme value theory for open set classification: GPD and GEV classifiers. 2019, arXiv:1808.09902.

[85] Liu S, Garrepalli R, Dietterich T G, et al. Open category detection with PAC guarantees//Proceedings of the 35th International Conference on Machine Learning. Stockholm, Sweden, 2018: 3169－3178.

[86] LeCun Y, Bottou L, Bengio Y, et al. Gradient-based learning applied to document recognition. Proceedings of the IEEE, 1998, 86(11): 2278－2324.

[87] Netzer Y, Wang T, Coates A, et al. Reading digits in natural images with unsupervised feature learning. http: //citeseerx. ist. psu. edu/showciting? doi=10.1.1.231.6173, 2020－03－20.

[88] Bilenko M, Basu S, Mooney R J. Integrating constraints and metric learning in semi-supervised clustering//Proceedings of the 21st International Conference on Machine Learning. Banff, Canada: ACM, 2004: 81－88.

[89] Frey P W, Slate D J. Letter recognition using Holland-style adaptive classifiers. Machine Learning, 1991, 6(2): 161－182.

[90] Krizhevsky A. Learning multiple layers of features from tiny images. Technical Report. Toronto: University of Toronto, 2009.

[91] Nene S A, Nayar S K, Murase H. Columbia object image library (COIL-20). Technical Report CUCS-005-96. Columbia University, 1996.

[92] Georghiades A S, Belhumeur P N, Kriegman D J. From few to many: Illumination cone models for face recognition under variable lighting and pose. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2001, 23(6): 643－660.

[93] Le Y, Yang X. Tiny ImageNet visual recognition challenge//CS 231N. 2015.

[94] Griffin G, Holub A, Perona P. Caltech-256 object category dataset. Technical Report 7694. California Institute of Technology, 2007.

[95] Deng J, Dong W, Socher R, et al. ImageNet: A large-scale hierarchical image database//Proceedings of 2009 IEEE Conference on Computer Vision and Pattern Recognition. Miami, FL, USA: IEEE, 2009: 248－255.

[96] Dalal N, Triggs B. Histograms of oriented gradients for human detection//2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. San Diego, CA, USA: IEEE, 2005, 1: 886－893.

[97] Sapkota A, Parks B, Scheirer W, et al. FACE-GRAB: Face recognition with general region assigned to binary operator//2010 IEEE Computer Society Conference on Computer Vision and Pattern Recognition-Workshops. San Francisco, CA, USA: IEEE, 2010: 82－89.

[98] Sokolova M, Lapalme G. A systematic analysis of performance measures for classification tasks. Information Processing & Management, 2009, 45(4): 427－437.

[99] Sokolova M, Japkowicz N, Szpakowicz S. Beyond accuracy, F-score and ROC: A family of discriminant measures for performance evaluation//Australasian Joint Conference on Artificial Intelligence. Hobart, Australia: Springer, 2006: 1015－1021.

[100] Cai W L, Chen S C, Zhang D Q. A multiobjective simultaneous learning framework for clustering and classification. IEEE Transactions on Neural Networks, 2010, 21(2): 185－200.

[101] Qian Q, Chen S C, Cai W L. Simultaneous clustering and classification over cluster structure representation. Pattern Recognition, 2012, 45(6): 2227－2236.

[102] Zhao B, Wu X, Feng J S, et al. Diversified visual attention networks for fine-grained object classification. IEEE Transactions on Multimedia, 2017, 19(6): 1245－1256.

[103] Qin S J. An overview of subspace identification. Computers & Chemical Engineering, 2006, 30(10－12): 1502－1513.

[104] Qu Y Y, Lin L, Shen F M, et al. Joint hierarchical category structure learning and large-scale image classification. IEEE Transactions on Image Processing, 2017, 26(9): 4331－4346.

[105] Pan S J, Yang Q. A survey on transfer learning. IEEE Transactions on Knowledge and Data Engineering, 2010, 22(10): 1345－1359.

[106] Busto P P, Gall J. Open set domain adaptation// Proceedings of 2017 IEEE International Conference on Computer Vision. Venice, Italy: IEEE, 2017: 754－763.

[107] Saito K, Yamamoto S, Ushiku Y, et al. Open set domain adaptation by backpropagation//Proceedings of the 15th European Conference on Computer Vision. Munich, Germany: Springer, 2018: 156－171.

[108] 刘晓龙, 王士同. 面向开放集图像分类的模糊域自适应方法. 计算机科学与探索, 2021, 15(3): 515－523. (Liu X L, Wang S T. Fuzzy domain adaptation algorithm for open set image classification. Journal of Frontiers of Computer Science and Technology, 2021, 15(3): 515－523.)

[109] 刘晓龙, 王士同. 渐进式分离的开放集模糊域自适应方法. 计算机应用, 2021, 41(11): 3127－3131. (Liu X L, Wang S T. Open-set fuzzy domain adaptation algorithm via progressive separation. Journal of Computer Applications, 2021, 41(11): 3127－3131.)

[110] Szepesvári C. Algorithms for reinforcement learning. Synthesis lectures on artificial intelligence and machine learning. San Franscisco, CA, USA: Morgan & Claypool, 2010.

[111] Shao R, Perera P, Yuen P C, et al. Open-set adversarial defense//16th European Conference on Computer Vision. Glasgow, UK, USA, 2020: 682－698.

[112] Yang Q, Liu Y, Chen T J, et al. Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 2019, 10(2): Article No. 12.

(责任编辑 杨可盛)