计算机科学
COMPUTER SCIENCE

基于元增量学习的开放集识别方法

孙晋永, 王雪纯, 蔡国永, 尚之量

引用本文

孙晋永, 王雪纯, 蔡国永, 尚之量. 基于元增量学习的开放集识别方法[J]. 计算机科学, 2025, 52(5): 187-198.

SUN Jinyong, WANG Xuechun, CAI Guoyong, SHANG Zhiliang. Open Set Recognition Based on Meta Class Incremental Learning [J]. Computer Science, 2025, 52(5): 187-198.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240600162

基于元增量学习的开放集识别方法

孙晋永　王雪纯　蔡国永　尚之量
桂林电子科技大学广西可信软件重点实验室　广西 桂林 541004
(sunjy@guet.edu.cn)

摘　要　传统图像分类算法假定世界是静态、封闭的,而大数据时代的真实世界却是动态、开放的,新类别及其样本不断出现,导致传统图像分类算法的准确率降低。针对这种情况,研究者提出了适用于真实世界的开放集识别问题,目标是从样本集中识别出未知类样本,同时保持对已知类样本的分类准确性。但现有的开放集识别方法都忽略了对识别出的未知类样本的进一步利用,且未知类样本通常数量较少,这些情况导致开放集识别模型无法增量地学习到已识别出的未知类样本蕴含的知识,影响了开放集识别模型的准确性和泛化性。为此,提出一种基于元增量学习的开放集识别方法,来提高开放集识别模型的准确性和泛化性。该方法使用双层优化机制构建开放集识别模型,对未知类样本进行深度聚类,使模型能够对聚类后的未知类样本进行增量学习。具体来说,首先,构建基于双层优化机制的开放集识别模型,并对其进行训练,使其具备对少量未知类样本进行增量学习的能力。然后,使用权重激励注意力机制来获取开放集识别模型参数的重要性,对模型的非关键参数进行更新,减少增量学习对模型的已知类分类能力的影响。其次,设计深度DBSCAN方法对未知类样本进行聚类,将每簇样本标记为一类,并使模型对其增量学习,丢弃离散样本,减少离散样本对增量学习效果的影响。最后,在4个公开数据集上进行实验,结果表明,相较于主流的开放集识别方法,所提方法在AUROC和F1分数上均具有更好的效果,可以充分地学习识别出的未知类样本的知识。

关键词:开放集识别;图像分类;增量学习;元学习;聚类
中图分类号　TP181

Open Set Recognition Based on Meta Class Incremental Learning

SUN Jinyong,WANG Xuechun,CAI Guoyong and SHANG Zhiliang
Guangxi Key Laboratory of Trusted Software,Guilin University of Electronic Technology,Guilin,Guangxi 541004,China

Abstract　Traditional image classification algorithms assume that the world is static and closed,whereas the real world is dynamic and open,and new categories and their samples are continually emerging,leading to a decrease in the accuracies of traditional image classification algorithms. To address this problem,researchers proposed open set recognition(OSR) problem for the real world which aims at identifying unknown-class samples while maintaining the classification accuracy for known-class samples. However,existing OSR methods generally neglect the further exploitation of identified unknown-class samples and the unknown class samples are scarce in number,so that the classification model is unable to incrementally learn the knowledge of identified unknown class samples,thereby impairing the accuracy and generalization capability of OSR models. Therefore,this paper proposes an OSR method based on meta-incremental learning to improve the accuracy and generalization of OSR models. This method employs a bi-level optimization mechanism to build an OSR model,and then cluster unknown class samples based on deep learning so that the built OSR model can incrementally learn the knowledge of unknown class samples. Specifically,an OSR model based on bi-level optimization mechanism is constructed and trained with few-shot unknown class samples,in order to enable the OSR model to incrementally learn the knowledge of few-shot unknown class samples. Then,a weight excitation attention method is used to obtain the importance of the OSR model's parameters and update non-critical parameters,thereby reducing the impact of incremental learning on the model's ability to classify known-classes. Additionally,a deep learning-based DBSCAN method is designed to extract features and cluster the identified unknown-class samples. Clustered samples are labeled as the same class and performed incremental learning. While samples that are difficult to cluster are rejected,to avoid the impact of too few unknown-

到稿日期:2024-06-27　返修日期:2024-08-21
基金项目:国家自然科学基金(62366010,61862016,62006058,62066010);广西可信软件重点实验室(KX202205);"认知无线电与信息处理"省部共建教育部重点实验室主任基金项目(CRKL210107)
This work was supported by the National Natural Science Foundation of China(62366010,61862016,62006058, 62066010), Guangxi Key Laboratory of Trusted Software Project(KX202205) and Fund of the Key Laboratory of Cognitive Radio and Information Processing,Ministry of Education(CRKL210107).
通信作者:王雪纯(islandwy@126.com)

class samples on the model's incremental learning effectiveness. Finally, experimental results on four public datasets show that the proposed method outperforms the mainstream open-set recognition methods on AUROC and F1 scores, and adequately learns the knowledge of identified unknown class samples.

Keywords Open set recognition, Image classification, Incremental learning, Meta learning, Clustering

1 引言

近年来，深度学习模型在样本分类方面取得了显著的进展[1]。但这些模型通常是基于静态样本集训练的，即样本集的类别是固定的，模型不能随着时间的推移进行动态调整。然而，在大数据时代，数据规模迅速增长，且数据来源逐渐多样化，新样本及其类别不断出现，导致分类模型的工作环境不断变化[2]。传统的分类模型通常只适用于已知类别的样本分类，无法应对开放环境中新类别样本的识别需求。Scheirer 等[3]提出基于开放世界假设的开放集识别问题(Open Set Recognition，OSR)。OSR 要求分类模型不仅能对已知类(Known Class)的新样本进行分类，而且能够识别未知类(Unknown Class)的样本，并拒绝将其分类为已知类。近年来，开放集识别问题受到越来越多研究者的关注，已成为分类模型研究的热点之一。

传统的开放集识别方法大多能够识别出未知类样本，但通常只能将其简单地标记为未知类别，而无法对其进一步利用。每当需要对新类样本进行分类时，就需要重新训练分类模型，会耗费大量资源。与机器学习模型不同，人类的学习能力是持续终身的。当人类认识新事物时，不需要忘记已学知识或是从零开始学习，而是逐步获取、完善和转化新事物的相关知识。人类尽管会逐渐遗忘旧知识，但不会完全丢失先前的知识。借鉴人类的学习方式，研究者们提出了增量学习(Incremental Learning)概念[4]。增量学习是指机器学习模型通过对新类样本或任务的学习来更新该模型，改进模型性能，而无需重新训练该模型。简言之，进行增量学习的模型能够持续处理现实世界的连续数据流，吸收其中的新知识，保留、整合和优化旧知识。

为了使开放集识别模型能够学习已识别的未知类样本蕴含的知识，提高模型的分类能力，同时避免重复训练造成的资源浪费，本文提出一种基于元增量学习的开放集识别方法。针对现实分类场景中未知类样本的数量可能有限的问题，结合元学习思想和增量学习方法来构建开放集识别模型。使用双层优化机制对开放集识别模型进行增量训练，在外层训练中通过采样训练集获得小样本增量学习任务训练集，在内层训练中通过小样本增量学习任务进行训练来更新开放集识别模型参数，使其获得对少量未知类样本进行增量学习的能力。为进一步提高分类模型的增量学习能力，还引入注意力机制，使用权重激励注意力机制与门控机制获取开放集识别模型参数的重要性，在增量学习中对非关键参数进行更新。设计深度 DBSCAN 方法，对未知类样本进行聚类，并增量地学习到开放集识别模型中。实验结果表明，与主流的开放集识别方法相比，本文提出的方法在 4 个经典图像数据集上的 F1 分数和 AUROC 更优。

2 相关工作

目前开放集识别问题一般以开放集的图像分类为研究对象，具体是指在图像分类任务中，对在训练集中未见过的类别样本进行有效识别。现有 OSR 方法主要分为 3 类：基于判别模型的方法、基于生成模型的方法、基于增量学习的方法。

1)基于判别模型的 OSR 方法

此方法通过建模已知类与未知类之间的边界来区分它们的样本。Scheirer 等[3]提出了基于支持向量机(Support Vector Machine，SVM)的 1-vs-Set 方法，通过添加与 SVM 超平面平行的另一个超平面来解决已知类过度占用特征空间的问题。但该方法仅适用于单一类别环境。为了解决多分类的开放集识别问题，Scheirer 等[5]提出了精简的衰减概率(Compact Abating Probability，CAP)模型，通过对样本从已知样本空间向开放空间移动的类概率进行衰减，研究了开放空间风险，以改善多类别条件下线性分类器的性能。Scheirer 等[5]将 CAP 模型与 EVT(Extreme Value Theory)[6]极值理论结合，提出了新的 Weibull 校准 SVM(W-SVM)方法，进一步限制开放空间的风险。该方法使用 SVM 条件阈值判断样本是否属于已知类，但前提是所有已知类的阈值都相同，这是不可能的。针对 W-SVM 阈值设置存在的问题，Scherreik 等[6]提出 POS-SVM 方法，为每个已知类分配一个固定的阈值。

近年来，深度神经网络(Deep Neural Network，DNN)被广泛应用于图像分类任务中。DNN 具有强大的特征提取能力，但在开放集识别任务中倾向于赋予未知类样本偏高的概率，因此无法有效地识别未知类样本。Bendale 等[7]提出使用 OpenMax 层代替 DNN 的 SoftMax 层，通过计算样本与其所属类的平均激活向量之间的距离来适配每个类的 Weibull 分布，以此计算已知类和未知类样本的概率估计。Shu 等[8]提出深度开放分类模型，使用 1-vs-Rest 层代替 SoftMax 层，为每一样本类生成一个合理的边界，并利用高斯拟合来收紧边界，以降低开放空间的风险。Zhou 等[9]提出了 PROSER 方法，通过设计虚拟的未知类作为已知类和未知类之间的边界，来提高模型区分已知类与未知类的能力。Yang 等[10]提出了基于卷积原型网络(Convolutional Prototype Network，CPN)的开放集识别方法，采用卷积神经网络(Convolutional Neural Networks，CNN)进行表示学习，并使用面向开放环境的原型网络代替面向封闭环境的 Softmax。这样的设计旨在提高 CNN 在 OSR 中的鲁棒性，同时保持其在封闭集环境中的高准确性。Lu 等[11]提出了一种新的原型挖掘与学习(PMAL)框架。该框架首先获取高质量和多样性的原型集特征，从训练样本中提取一组高质量的候选样本，避免噪声的干扰；然后根据多样性策略对原型集进行过滤，以在特征空间中有效区分已知类和未知类。

2）基于生成模型的 OSR 方法

此方法需要显式地建模和评估未知类。Ge 等[12]提出了生成 OpenMax（G-OpenMax）方法，利用条件生成对抗网络（cGAN）生成未知类样本，为分类器提供生成的未知类样本的概率估计。但这些生成的样本局限于已知类的子空间，影响了对未知类的模拟效果。Lawrence 等[13]提出了基于反事实图像样本的开放集识别方法（OSRCI）。该方法生成处于决策边界的图像样本作为未知类样本，这些样本接近但并不属于任何已知类。Pramuditha 等[14]进一步提出 GFROSR 方法，使用自监督的生成模型来学习更丰富的样本特征以增强类间差异，从而有效地区分已知类和未知类。Yang 等[15]提出了基于 GAN 的 OSR 模型，通过生成器自动生成与目标样本高度相似的伪目标样本作为负样本，并重新设计判别器以输出多个已知类别和一个“未知”类别的概率。该方法在人体活动数据集上取得了优于其他方法的效果。Feng 等[16]设计了双分支 GAN 网络，从语义分类对齐、语义对比映射两个方面学习开放集样本的语义信息，以实现已知类的良好可分离性，并将未知类别推离决策边界。Kong 等[17]提出 OpenGan 模型，使用真实的未知类样本与 GAN[18]生成的样本作为未知类训练该模型，并直接使用已训练的 GAN 判别器来评估样本属于已知类的概率。

3）基于增量学习的 OSR 方法

此方法利用识别出的未知类样本，将新样本的知识增量学习到模型中。Rosa 等[19]提出采用在线增量学习对开放集识别方法进行扩展，设计了在线度量学习和阈值增量更新方法。Venkataram 等[20]提出基于 CNN 的增量开放集方法，来处理未知类的文本文档。Shu 等[21]设计了原型学习深度网络。该网络在检测到未知类样本之后，手动地对样本进行标注，并利用这些标注好的未知类样本对网络进行更新。Dang 等[22]提出开放集增量学习（Open Set Model with Incremental Learning，OSmIL）方法，来持续识别和学习新的未知类别，并通过选择边缘样本以覆盖训练类别来简化模型。

基于判别模型和生成模型的 OSR 方法都缺乏对未知类样本知识的有效利用，不能对未知类样本进行分类。基于增量学习的 OSR 方法虽然能够利用未知类样本，但它直接将所有新样本类增量地学习到开放集识别模型中，没有考虑到未知类样本数量较少的情况。分类模型对样本数量极少的未知类进行增量学习，会造成已知类的分类准确率降低和不必要的资源浪费。

3 预备知识

3.1 开放集识别问题

传统的基于深度网络的分类模型基于封闭集假设，假定训练和测试样本来自相同的标签集。然而，在现实情况下，经常会出现训练集之外的新类别样本。因此，Scheirer 等[3]在 2012 年提出了开放集识别问题，目标是将未知类别的样本明确地识别出来，同时准确分类已知类别的样本，以提高分类模型对未知类别样本的识别准确性和鲁棒性。对于面向图像分类的 OSR 问题，封闭集分类和开放集识别的区别可以通过图 1 来形象地展示。

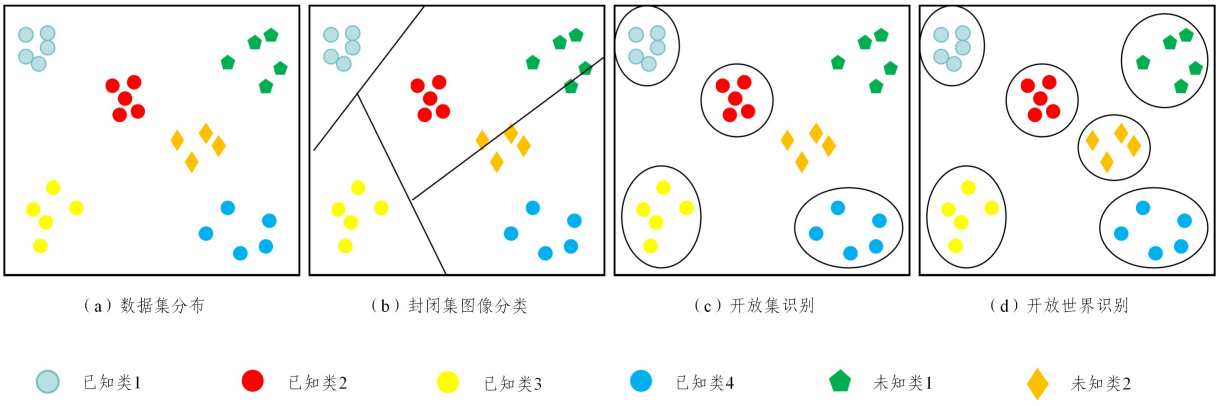


图 1 不同分类任务的对比

Fig. 1 Comparison of different classification tasks

定义 1（开放性） 开放性定量描述了开放集识别问题的开放程度，如式（1）所示[23]：

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

其中，$|C_{\mathrm{TR}}|$表示训练集中的类别数，$|C_{\mathrm{TE}}|$表示测试集中的类别数，$|C_{\mathrm{TA}}|$表示需要被识别的类别数。

定义 2（开放空间风险[23]） 开放空间风险指在开放集识别问题中，因存在未知类别导致分类模型对新样本进行分类时可能出现的误判风险。该风险的计算如式（2）所示：

$$R_O(f)=\frac{\int_O f(x)\mathrm{d}x}{\int_{S_O} f(x)\mathrm{d}x} \tag{2}$$

其中，$R_O(f)$即开放空间风险，表示未知类样本被分类模型误分类为已知类样本的可能性；$f(\boldsymbol{x})$是一个指示函数，值域为$\{0,1\}$。$f(\boldsymbol{x})=1$表示样本 $\boldsymbol{x}$ 被分到已知类中，$f(\boldsymbol{x})=0$表示样本 $\boldsymbol{x}$ 被识别为未知类。积分区间的开放空间 O 指由模型在训练阶段未见过的样本所构成的空间。S_O是由所有已知类样本组成的空间与 O 组成的大空间，即整个样本空间。可以通过先计算 O 空间样本被分类为已知类样本的积分、整个空间样本被分类为已知类样本的积分，再计算二者的比值，得到 $R_O(f)$。

定义 3（开放集风险[23]） 开放集风险由开放空间风险与经验风险组成，通过最小化开放集风险得到一个合适的开放集识别模型 f_{OSR}。开放集风险的计算如式（3）所示：

$$\arg\min_{f_{\mathrm{OSR}}\in H}\{R_O(f_{\mathrm{OSR}})+\lambda_r R_\varepsilon(f_{\mathrm{OSR}}(T))\} \tag{3}$$

其中，f_{OSR}表示开放集识别模型，R_O表示开放空间风险，T表示训练集，R_ε表示经验风险，λ_r为正则化系数。

在现实环境中，样本集的规模是动态增加的，开放集识别模型必须在检测中不断学习新类别的样本的知识。传统的开放集识别方法可以在分类时识别出未知类样本并拒绝，但其分类模型是静态的，不能随着样本集的变化而更新。Bendale等进一步扩展了开放集识别的定义，提出了开放世界识别(Open World Recognition)问题[24]。开放世界识别的方法应具有3个关键特征[25]：一是能够逐步更新已知类别的识别模型；二是具备学习新类别样本的能力，无需重新训练整个模型；三是能够区分输入的样本属于已知类别还是新类别。开放世界识别如图1(d)所示。

开放世界识别问题的形式化描述如下：在开放世界场景中，训练集包含已知类样本，而测试集包含已知类样本和未知类样本。设训练集 $D_{\mathrm{train}}=\{(\boldsymbol{x}_i,y_i)\mid \boldsymbol{x}_i\in X_{\mathrm{train}},y_i\in Y_{\mathrm{known}},i=1,2,\cdots,m\}$，测试集 $D_{\mathrm{test}}=\{(\boldsymbol{x}_i,y_i)\mid \boldsymbol{x}_i\in X_{\mathrm{test}},y_i\in(Y_{\mathrm{known}}\cup Y_{\mathrm{unknown}})\mid i=1,2,\cdots,n\}$，其中，$\boldsymbol{x}_i$为样本，$y_i$为样本的类别标签。已知类的标签集 $Y_{\mathrm{known}}=\{c_1,c_2,\cdots,c_k\}$，未知类的标签集 $Y_{\mathrm{unknown}}=\{c_{k+1},c_{k+2},\cdots,c_{k+u}\}$，其中 c_i为类别标签，$i=1,2,\cdots,k+u$。任务是：利用 D_{train}训练得到一个分类模型 f_{OW}，使用 f_{OW}对 D_{test}中的已知类样本(x_k,y_k)进行分类，同时识别出未知类样本(x_u,y_u)；且对该样本进行标记并增量学习，使 f_{OW}可以在下次测试时对未知类样本进行准确分类。因此，该问题的目标是设计一个模型 f_{OW}，使其能够对测试集的任意样本进行准确分类，无论该样本类别是否包含在训练集已知类中。

3.2 增量学习

人类的知识学习包括获取新知识、遗忘部分旧知识、整合新旧知识等过程。受此启发，研究者提出了增量学习的概念。增量学习[4]是指模型在接收新数据后，能够利用这些数据来更新和改进自身模型的过程。其能力主要表现在以下几个方面：处理连续的数据流、吸收新知识、保留旧知识、整合知识，以及优化旧知识。总的来说，增量学习的能力使得分类模型能够适应持续变化的工作环境，并不断提高性能和效率，从而更好地应对现实世界中不断变化的需求和挑战。

本质上，增量学习的目标是在缓解模型的灾难性遗忘的同时，尽可能地保持模型的稳定性和可塑性[26]。灾难性遗忘是指分类模型在学习新任务时，可能会导致模型在已经学习的旧任务上性能显著下降，这在基于误差反向传播的深度学习方法中比较突出。稳定性是指模型在接收新样本后可以保持性能稳定，而可塑性是指模型能够灵活调整参数以适应新样本。

常见的增量学习方法有3种[4]：正则化(Regularization)、回放(Replay)、参数隔离(Parameter Isolation)。正则化方法通过向新任务的损失函数施加约束，来保护旧知识不被新知识覆盖，从而在学习新任务时保留先前学到的知识。回放方法则在训练新任务时保留一部分具有代表性的旧数据，并将其与新数据一起输入模型进行训练，以此“温故而知新”。参数隔离方法需要引入较多的参数和计算量，通常只适用于简单任务的场景。这3种方法各有优劣，需要根据具体情况选择最适合的策略。

目前的增量学习(Incremental Learning)研究通常使用大量带标签的新类别样本，然而在实际应用中，由于数据的偶发性和数据标记过程需要大量的人力投入，迅速积累大量的有标注训练数据通常是不切实际的。因此，在面对少量的训练样本时，分类模型还需要具备小样本增量学习的能力。小样本增量学习(Few-Shot Class-Incremental Learning，FSCIL)[27]是指模型在面对具有少量标记样本的新类别时，能够快速学习这些新类别的过程。这种方法的关键在于利用有限的样本进行模型更新，并确保分类模型能够在面对新类别样本时保持高准确性和泛化能力。其主要挑战是避免灾难性地忘记旧知识，同时防止模型过拟合到样本很少的新类。因此，FSCIL通常需要结合迁移学习、元学习等方法，使得模型可以充分利用已有的知识，加快对新类别的学习过程。

FSCIL[25]的形式化描述如下：通过一系列互不相交的样本类进行增量学习，其中每个类包含少量样本。具体来说，训练集由一系列带有标签的样本集合组成，即$\{D^0,D^1,\cdots\}$，其中 $D^t=\{(x_j^t,y_j^t)\}_{j=1}^{|D^t|}$，$t=1,2,3$。$D^t$对应的标签集 C^t互不相交，即对于任意 i和j，$C^i\cap C^j=\Phi$。C^0被称为基类。只有 D^0中包含大量的训练样本，而 D^t包含新类的少量样本。FSCIL模型可以先使用 C^0离线训练模型，一旦离线训练完成，FSCIL模型需要在 D^t训练集上执行在线增量学习以调整模型，在随后的每个增量训练会话(Training Session)中学习新类。在第 t个训练会话中只有 D^t可用，其中 D^t只包含 C^t中新类的少量训练样本。对于 D^t，每类具有 c个类别和 k个训练样本的设置被称为 c-way k-shot FSCIL。例如，在5-way 5-shot FSCIL的情况下，每个增量会话中 D^t包含5个新类，其中每个类有5个训练样本。在增量地学习了 D^t之后，FSCIL模型可以对目前所有类的测试样本即 $C^0\cup C^1\cup\cdots\cup C^t$中的样本进行分类。

3.3 元学习

元学习(Meta-Learning)[28]是一种旨在训练机器学习的模型学习如何学习的方法。换句话说，元学习关注的是机器学习的模型本身的学习过程，而不仅仅是单纯地利用样本对模型进行训练。其目标是使模型具备更好的泛化能力，更快地适应新任务，以更有效地利用少量的训练样本。

元学习的核心理念是从多个学习任务中提取通用模式、规律或策略，以便在面对新任务时做出有效的预测或决策。常见的元学习方法包括基于优化的方法、基于度量的方法和基于模型的方法[28]。基于优化的方法主要关注如何在训练阶段优化模型参数，以便模型在遇到新任务时可以快速适应。基于度量的方法侧重于优化度量函数以学习样本之间的相似度，使得模型能够更好地泛化到新类别或任务。基于模型的方法训练模型来模拟任务之间的关系，从而达到上述目的。目前，元学习已广泛应用于多个领域，如计算机视觉、自然语言处理、强化学习等，并在一些领域取得了显著进展。

模型无关的元学习(Model-Agnostic Meta-Learning，MAML)[29]是一种基于优化的元学习方法，也是目前最流行的元学习方法之一。它提供一种通用的框架，使得模型能够通过少量的训练样本快速适应新的任务或新的数据集。其核

心思想是在元学习阶段优化模型的参数，使模型根据当前任务的特性快速收敛到最优解。MAML 使用嵌套优化机制来学习模型，其中内部训练执行任务级优化，根据少量的训练样本进行模型参数更新，以应对特定的任务。而外部训练通过元方法的优化目标执行全局模型更新，以提高模型对新任务的泛化能力。

4 基于元增量学习的开放集识别方法

针对未知类样本未能得到充分利用以及未知类样本通常数量较少导致开放集识别模型的准确性不高和泛化性不好的情况，本文提出一种基于元增量学习的开放集识别方法（Meta Class Incremental Learning for Open Set Recognition，MILOSR）。该方法利用增量学习方法和元学习理论构建一个开放集识别模型，以实现 MILOSR 模型对未知类样本的增量学习，并通过深度聚类实现对未知类样本的分类，以提高分类模型的准确性和泛化性。目前开放集识别问题一般以图像样本为研究对象，因此本文同样使用图像数据集作为研究对象。MILOSR 模型的框架如图 2 所示。

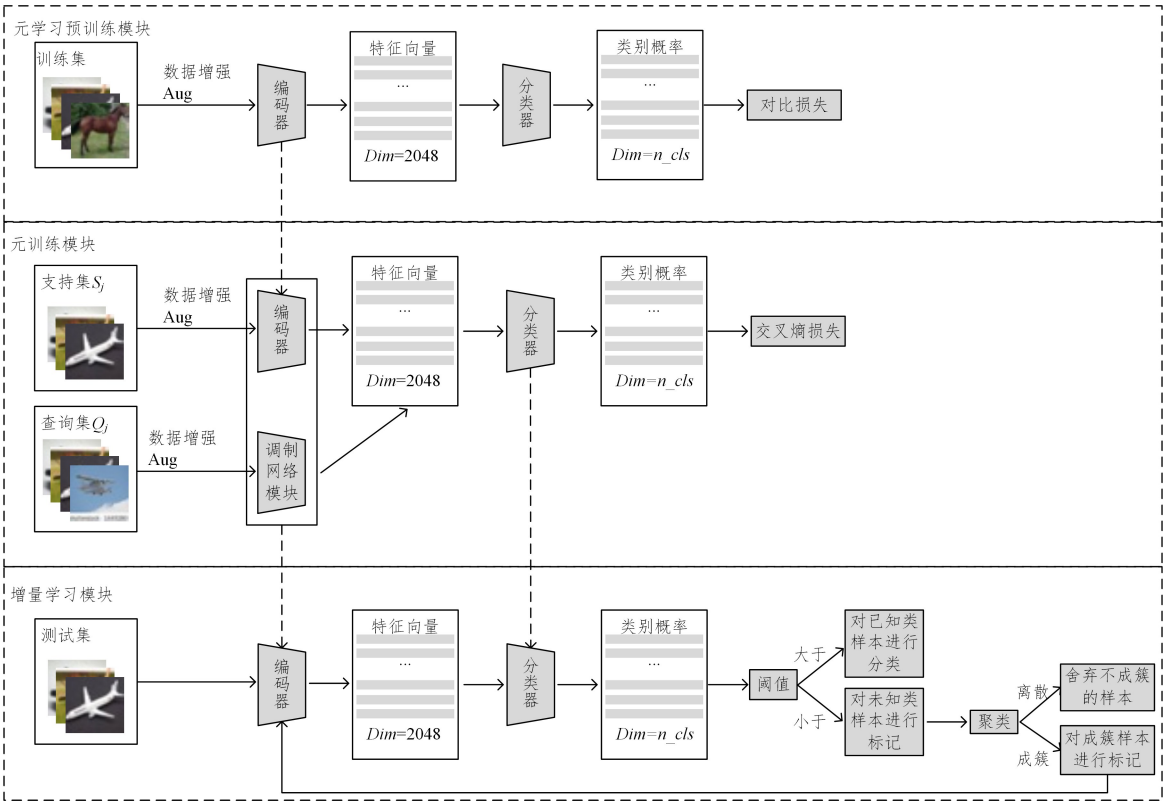


图 2 MILOSR 模型框架

Fig. 2 Framework of MILOSR

MILOSR 模型由 3 个部分组成，从上到下依次为：元学习预训练模块、元训练模块和增量学习模块。这 3 个模块分别对应 MILOSR 模型的 3 个阶段：元学习预训练阶段、元训练阶段和增量学习阶段。其中，编码器均使用 ResNet50，用于从样本中提取特征；分类器均由带有非线性激活函数的全连接层组成。在模型的预训练阶段，首先从训练集中划分已知类样本集和未知类样本集。然后，将已知类样本输入 MILOSR 模型进行预训练。此阶段使用 PCLOSR 方法[30]训练模型。在模型的元训练阶段，在每个训练轮次开始前，将训练集中的已知类样本进一步划分为多个小样本增量学习任务，并对这些样本进行数据增强。每个任务包括支持集和查询集。其中，支持集是元学习任务中用于模型训练和参数更新的样本集；而查询集则用于模型评估和测试，反映其在新任务上的泛化能力。首先使用支持集样本对预训练模型的编码器进行训练，然后通过查询集样本对编码器和调制网络模块进行微调。在模型的增量学习阶段，使用训练好的分类器对测试集样本进行测试，对已知类样本进行分类，对识别出的未知类样本则拒绝分类。对识别出的未知类样本进行聚类，标注汇聚成簇的样本，使用这些样本对 MILOSR 模型进行增量学习。不在任何簇内的样本被视为离散样本，直接舍弃。图 2 中带箭头的虚线表示将编码器或分类器的参数迁移到下一阶段。

本文使用 $\boldsymbol{\theta}=\{\boldsymbol{\theta}_{\mathrm{E}},\boldsymbol{\theta}_{\mathrm{M}},\boldsymbol{\theta}_{\mathrm{FC}}\}$ 表示整个 MILOSR 模型的参数，其中 $\boldsymbol{\theta}_{\mathrm{E}},\boldsymbol{\theta}_{\mathrm{M}},\boldsymbol{\theta}_{\mathrm{FC}}$ 分别表示编码器、调制网络模块和分类器的参数。

4.1 数据预处理

元学习的核心思想是使模型在面对新任务时能够利用以前学到的知识和经验进行快速学习，因而适用于增量学习。MAML[29]是一种流行的元学习方法，本文将其引入 MILOSR 模型中。在结合 MAML 的开放集识别任务中，需要对样本集进行预处理，即划分样本集。首先，将样本类按一定比例划分为已知类和未知类，训练集中仅包含已知类样本，而测试集中同时包含已知类和未知类样本。使用训练集对模型进行预训练。其次，在元训练阶段，在每个训练轮次开始前，将训练集中的样本划分为互不相交的多个小样本增量学习任务，每个任务都包括一个支持集和一个查询集，即 $D_j=$

$\{(S_j, Q_j)\}_{j=0}^{n}$。其中，S_j 和 Q_j 是第 j 个任务的支持集和查询集，它们含有相同的类别，但样本数量不同，样本也互不相同；而同一个训练轮次的不同任务间的类别彼此不同。

4.2 调制网络模块

Yann 等[31]提出，在特定任务上训练的深度网络模型中，参数的重要性通常是不均衡的。因此，Kirkpatrick 等[32]提出在面对新任务或知识时，通过调整参数的学习率或更新策略，可以让以前任务中的关键参数保持稳定，而非关键参数则可以根据新的知识进行调整，从而使得深度网络模型在吸收新知识的同时避免灾难性遗忘。Chi 等[33]遵循这一思想，提出一种选择性激活机制，通过训练另一个并行的调制网络来调整深度网络模型的参数可塑性。Quader 等[34]提出了一种新的注意力机制，即权重激励机制，用于在训练阶段获取卷积神经网络权重的重要性向量，并将更多的注意力集中在重要的权重上。

为了进一步提高 MILOSR 模型的增量学习能力，在模型的元训练阶段引入权重激励机制，使用该机制对分类网络（Classification Network，CN）和调制网络（Modulation Network，MN）进行双向引导调制。基于双向引导调制的注意力机制的结构如图 3 所示。

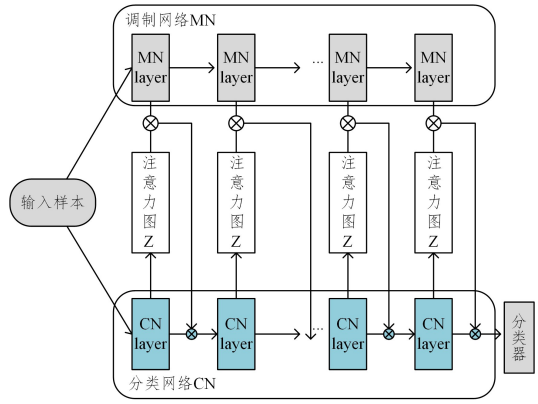


图 3 基于双向引导调制的注意力机制的结构

Fig. 3 Attention mechanism based on bi-directional guided modulation

在 MILOSR 模型训练过程中，CN 获取已知类样本知识并将其编码在权重中，通过双向引导调制利用这些知识，使 MN 可以更有效地区分模型参数的重要性。

注意力机制的结构如图 4 所示。在这个结构中，通过每层 CN 输出的特征图生成注意力图 $\boldsymbol{Z}$，该图展示了当前分类网络层中权重的重要性。

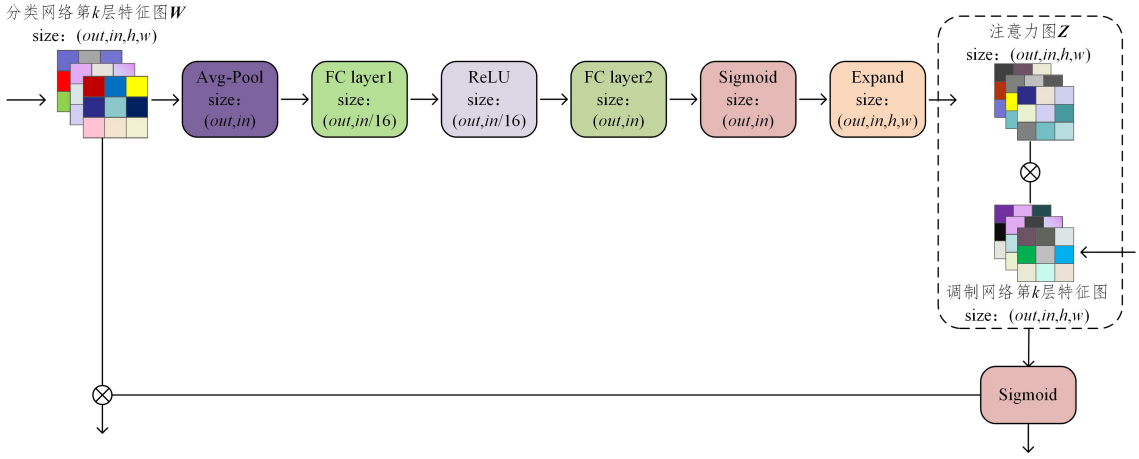


图 4 注意力机制的结构

Fig. 4 Structure of attention mechanism

在神经网络中，特征图通常被表示为一个四维张量，其中的维度通常包括批次大小（batchsize）、通道数（channels）、高度（height）、宽度（width）。在一个卷积层中，特征图的格式通常是（batch size，channels，height，width）。为方便描述，在图 4 中，将特征图的格式简记为（out，in，h，w）。注意力图 $\boldsymbol{Z}$ 如式(4)所示：

$$\boldsymbol{Z}_{i,j}=\mathrm{Sigmoid}(FC_2(\mathrm{ReLU}(FC_1(Avg(\boldsymbol{W}_{i,j}))))) \tag{4}$$

其中，$\boldsymbol{Z}_{i,j}$ 是由 $\boldsymbol{W}_{i,j}$ 生成的注意力图，$\boldsymbol{W}_{i,j}$ 是第 i 个输入样本和第 j 个通道的分类网络特征图。Avg 表示平均池化操作，将特征图 $\boldsymbol{W}_{i,j}$ 沿着（h，w）维度平均。平均池化是一种常见的池化操作，通常用于降低图像或特征图的空间维度，同时保留重要信息。FC_1 和 FC_2 是完全连接层，用于将池化后的特征图进行线性变换。通过这个变换，从输入特征中学习到一个适当的调制参数，以便调制分类网络中的权重。ReLU 是一种激活函数，可以引入非线性特性，从而使神经网络能够学习复杂的非线性模式和特征。Sigmoid 函数对输出向量进行压缩，将其转换为一个在(0，1)范围内的值。最后，将权重表示重塑为与输入特征相同的形状，得到注意力图 $\boldsymbol{Z}$。

通过向量点乘运算将 $\boldsymbol{Z}$ 应用于 MN 的特征图，生成新的门控掩码，再将掩码应用到 CN 的特征图上。为了匹配权重的大小，对 CN 和 MN 使用相同的网络架构。本文使用权重激励机制设计 MN，在元训练阶段对 MILOSR 模型的 MN 参数 $\boldsymbol{\theta}_M$ 进行训练，以在处理新类别时保持先前学到的重要信息，从而提高 MILOSR 模型的泛化能力和效果。

4.3 模型的元学习预训练阶段

本阶段首先对经过数据预处理的训练集样本进行数据增强，以增加样本的多样性和丰富性。常见的增强方式有随机裁剪、随机旋转、缩放等操作，这些操作可以提高模型的泛化能力。将增强后的样本输入编码器，提取样本的特征，并进行分类。本阶段使用 PCLOSR 方法[30]进行训练。在

训练完成后，冻结经过预训练的编码器的参数 $\boldsymbol{\theta}_E$，供元训练阶段使用。经过预训练，编码器可以学习到更有用和抽象的特征表示，从而提高 MILOSR 模型在后续任务上的性能和泛化能力。

4.4 模型的元训练阶段

借鉴 MAML[29] 的嵌套优化机制，本方法使用了双层优化机制的训练模式。其中，外层训练控制整体训练流程，内层训练负责实际的元训练过程。具体来说，对于外层训练，简单地循环遍历指定的轮次，从训练集中采样获得一系列小样本增量学习任务的支持集和查询集，并对 MILOSR 模型进行元训练。对于内层训练，在每个训练轮次，模型会依次经过热身模块、快速适应模块、元更新模块。内层训练过程如图 5 所示，图中带箭头的虚线表示将编码器、分类器的参数迁移到下一阶段。

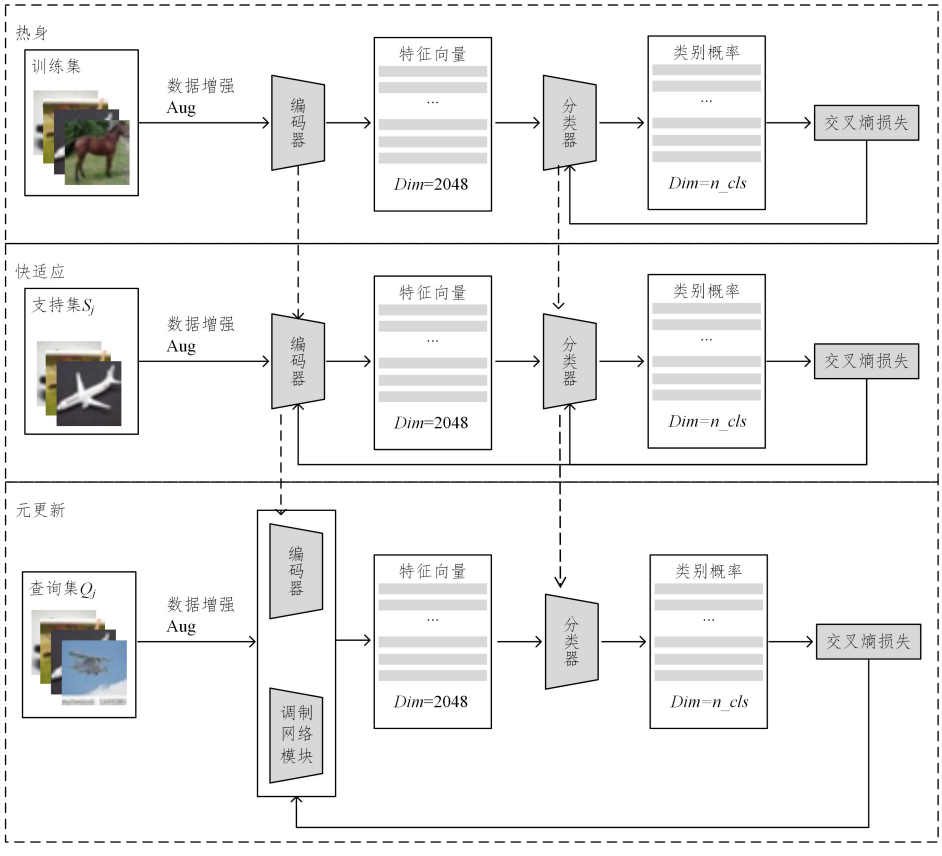


图 5 元训练的内层训练过程

Fig. 5 Inner training process of meta-training

1）热身模块。在每个训练轮次的内层训练开始时对 MILOSR 模型进行预热，利用少量样本进行梯度下降，以减少随机性的影响。具体过程如下：在每个训练轮次开始时，定义一个空的累积查询集 Q_c，用于存储各任务的查询集；将预训练得到的编码器参数 $\boldsymbol{\theta}_E$ 加载至 MILOSR 模型中，丢弃预训练阶段的分类器参数 $\boldsymbol{\theta}_{\mathrm{FC}}$；在每个训练任务开始前，为新类增加新的分类器，并将新的分类器随机初始化，记为 $\boldsymbol{\theta}_{\mathrm{FC_{new}}}$；为了减少随机性的影响，冻结编码器参数，训练模型并对 $\boldsymbol{\theta}_{\mathrm{FC_{new}}}$ 进行微调，以使其更接近局部最优解。

2）快速适应模块。快速适应（Fast Adaptation）是元学习中常用的技术，使用少量样本进行快速调整，以适应新任务或新领域。具体操作包括：将 $\boldsymbol{\theta}_{\mathrm{FC_{new}}}$ 与来自之前训练任务的 $\boldsymbol{\theta}_{\mathrm{FC_{old}}}$ 并联拼接起来，即 $\boldsymbol{\theta}_{\mathrm{FC}}=[\boldsymbol{\theta}_{\mathrm{FC_{old}}};\boldsymbol{\theta}_{\mathrm{FC_{new}}}]$；然后，模型对新类进行快速自适应，使用梯度下降法更新 $\boldsymbol{\theta}_{\mathrm{E}}$ 和 $\boldsymbol{\theta}_{\mathrm{FC}}$，如式(5)所示：

$$\begin{aligned}\widetilde{\boldsymbol{\theta}}_{\mathrm{E}}&=\boldsymbol{\theta}_{\mathrm{E}}-\alpha\nabla_{\boldsymbol{\theta}_{\mathrm{E}}}L_{\mathrm{CE}}(\boldsymbol{X}_j^s,Y_j^s;\boldsymbol{\theta})\\ \widetilde{\boldsymbol{\theta}}_{\mathrm{FC}}&=\boldsymbol{\theta}_{\mathrm{FC}}-\alpha\nabla_{\boldsymbol{\theta}_{\mathrm{FC}}}L_{\mathrm{CE}}(\boldsymbol{X}_j^s,Y_j^s;\boldsymbol{\theta})\end{aligned}\tag{5}$$

其中，$\boldsymbol{X}_j^s$ 和 Y_j^s 分别是第 j 个任务中支持集的样本和标签；$L_{\mathrm{CE}}(\boldsymbol{X},Y;\boldsymbol{\theta})$ 用于计算模型在给定输入样本 $\boldsymbol{X}$ 的预测概率与目标标签 Y 之间的交叉熵损失。将更新后的编码器网络参数和分类器网络参数分别记为 $\widetilde{\boldsymbol{\theta}}_{\mathrm{E}}$，$\widetilde{\boldsymbol{\theta}}_{\mathrm{FC}}$。

3）元更新模块。此模块用于在查询集上评估模型在当前任务上的分类效果并更新参数。快速适应模块模拟了开放集识别模型在线学习新类的过程。理想情况下，模型调整后的参数在旧任务中的类别和在当前任务中的新类别上均表现良好。来自旧任务的查询集反映了更新后的模型如何克服灾难性遗忘，而当前任务的查询集验证了模型对新类别的适应性。因此，在元更新阶段，将当前任务的查询集 Q_j 附加到累积查询集 Q_c 中，同时使用新旧类样本进行评估。此阶段中，模型优化目标定义为：

$$\min_{\boldsymbol{\theta}_{\mathrm{E}},\boldsymbol{\theta}_{\mathrm{M}}}\sum_{(X^q,Y^q)\in Q^C}L_{\mathrm{CE}}(X^q,Y^q;\widetilde{\boldsymbol{\theta}}_{\mathrm{E}},\widetilde{\boldsymbol{\theta}}_{\mathrm{FC}},\boldsymbol{\theta}_{\mathrm{M}})\tag{6}$$

其中，$\boldsymbol{\theta}_{\mathrm{M}}$ 指调制网络参数；$L(\cdot)$ 使用 $\widetilde{\boldsymbol{\theta}}_{\mathrm{E}}$ 和 $\widetilde{\boldsymbol{\theta}}_{\mathrm{FC}}$ 计算损失，并在 $\boldsymbol{\theta}_{\mathrm{E}}$ 和 $\boldsymbol{\theta}_{\mathrm{M}}$ 上进行优化更新。通过梯度下降法求解式(6)：

$$\begin{aligned}\boldsymbol{\theta}_{\mathrm{E}}&=\boldsymbol{\theta}_{\mathrm{E}}-\beta\nabla_{\boldsymbol{\theta}_{\mathrm{E}}}\sum_{(X^q,Y^q)\in Q^C}L_{\mathrm{CE}}(X^q,Y^q;\widetilde{\boldsymbol{\theta}}_{\mathrm{E}},\widetilde{\boldsymbol{\theta}}_{\mathrm{FC}},\boldsymbol{\theta}_{\mathrm{M}})\\ \boldsymbol{\theta}_{\mathrm{M}}&=\boldsymbol{\theta}_{\mathrm{M}}-\beta\nabla_{\boldsymbol{\theta}_{\mathrm{M}}}\sum_{(X^q,Y^q)\in Q^C}L_{\mathrm{CE}}(X^q,Y^q;\widetilde{\boldsymbol{\theta}}_{\mathrm{E}},\widetilde{\boldsymbol{\theta}}_{\mathrm{FC}},\boldsymbol{\theta}_{\mathrm{M}})\end{aligned}\tag{7}$$

当一个训练轮次中的所有任务都完成后，Q_c 将被重置为空。对于每个新的轮次，都需要重复进行热身阶段、快适应阶段和元更新阶段，直到元训练结束。

在元训练过程中，MILOSR 模型参照小样本增量学习的过程，对 $\boldsymbol{\theta}_E$ 进行微调，以适应增量学习环境，从而在增量学习阶段中保持模型稳定性，提升分类性能。同时，对 $\boldsymbol{\theta}_M$ 进行训练，使关键参数不参与增量学习过程，从而缓解模型在增量学习时的遗忘，提高模型的稳定性，促进增量学习过程的顺利进行。在元训练结束后，$\boldsymbol{\theta}_M$ 被冻结，不再参与训练过程。元训练算法的伪代码如算法 1 所示。

算法 1 元训练算法

Input: Meta-Learning Pretrained Encoder

Output: Meta-Training Model

1. Initialize the models with pre-trained weights
2. WHILE i<maxepoch DO
3. sample a sequence
4. $Q_c=\emptyset$
5. WHILE k < maxsession DO
6. Warm-up $\boldsymbol{\theta}_{FC_{new}}$
7. IF k>0 THEN
8. $\boldsymbol{\theta}_{FC}=\text{Concatenate}(\boldsymbol{\theta}_{FC_{old}},\boldsymbol{\theta}_{FC_{new}})$
9. ENDIF
10. fast_adapt

$$\widetilde{\boldsymbol{\theta}}_E=\boldsymbol{\theta}_E-\alpha\nabla_{\boldsymbol{\theta}_E}L_{CE}(X_j^s,Y_j^s;\boldsymbol{\theta})$$

$$\widetilde{\boldsymbol{\theta}}_{FC}=\boldsymbol{\theta}_{FC}-\alpha\nabla_{\boldsymbol{\theta}_{FC}}L_{CE}(X_j^s,Y_j^s;\boldsymbol{\theta})$$

11. $Q^c=Q^c\cup Q^j$
12. meta_update

$$\boldsymbol{\theta}_E=\boldsymbol{\theta}_E-\beta\nabla_{\boldsymbol{\theta}_E}\sum_{(X^q,Y^q)\in Q^C}L_{CE}(X^q,Y^q;\widetilde{\boldsymbol{\theta}}_E,\widetilde{\boldsymbol{\theta}}_{FC},\boldsymbol{\theta}_M)$$

$$\boldsymbol{\theta}_M=\boldsymbol{\theta}_M-\beta\nabla_{\boldsymbol{\theta}_M}\sum_{(X^q,Y^q)\in Q^C}L_{CE}(X^q,Y^q;\widetilde{\boldsymbol{\theta}}_E,\widetilde{\boldsymbol{\theta}}_{FC},\boldsymbol{\theta}_M)$$

13. END WHILE
14. END WHILE

算法 1 描述了元学习的双层循环训练过程，时间复杂度为 $O(maxepoch * maxsession)$，其中，$maxepoch$ 为模型最大训练轮数，$maxsession$ 为每轮训练中支持集的数量。

4.5 模型的增量学习阶段

在 MILOSR 模型完成元训练阶段后，进行以下步骤：首先，使用测试样本对模型进行测试，对已知类样本进行分类，同时识别未知类样本并拒绝为其分类；然后，针对在测试中被识别为未知类的样本进行聚类，舍弃离散样本，并对成簇的未知类样本进行标注；最后，将具有标签的未知类样本增量地学习到模型中，以进一步提高模型的分类性能和泛化能力。

1）测试

使用经过元训练的 MILOSR 模型对测试集样本进行测试，测试集包括已知类样本与未知类样本。将样本输入 MILOSR 模型中，以获取测试样本被分类到各类的概率。然后，将最大概率与阈值进行比较。如果概率高于阈值，则将该样本分类为已知类，并标记为相应的已知类；否则，将其标记为未知类。阈值的选取方法参考文献[35]。

2）深度聚类

在测试阶段，MILOSR 模型可识别并标注未知类样本，将其知识增量学习到模型中可提升模型的分类能力，使模型能识别和分类这些类别的图像样本。然而，对所有被识别出的未知类样本进行增量学习存在两个问题：一是人工标注费时费力；二是未知类样本数量不确定，且样本数量极少时难以有效学习。因此，本文提出在增量学习前先进行聚类，再分情况处理，即先对未标注未知类样本进行聚类，然后将成簇的样本标注为新类别进行增量学习，而游离在簇外的样本被视为离群样本，不值得进行增量学习，可以直接舍弃。

深度聚类(Deep Clustering)是一种将深度学习与传统聚类方法结合的方法，其利用神经网络的特征提取能力，将样本映射到高维特征空间，然后在该空间中执行聚类操作。DeepCluster[36]是一种深度聚类方法，其利用预训练的深度神经网络提取特征，并使用 k 均值算法对这些特征进行迭代分组。随后，将得到的分组结果作为监督信号来更新神经网络的参数。然而，k 均值聚类需要事先设置聚类个数 k，因此它并不适用于未知类别数量难以确定的开放集识别问题。密度聚类算法 DBSCAN 不需要事先确定簇的数量，能够根据样本点的密度自适应地发现簇，且能够识别并排除噪声点，不将其分配给任何簇，这使得它在处理包含噪声和异常值的样本集时表现更为优越。在处理未知类样本的问题中，可以将数量较少的未知类样本视作噪声点并排除在簇外。因此，本文提出了深度 DBSCAN(DeepDBSCAN)聚类方法，以更好地应对未知类样本的聚类和分类任务。对未知类样本进行深度聚类主要包括以下步骤。

(1)特征提取：首先将图像样本转换为适合聚类的表示形式，如特征向量。在本模型中，使用 MILOSR 模型中的编码器来提取图像的特征向量。

(2)特征降维：在实际应用中，高维特征数据难以存储且需要大量时间进行聚类。因此，本模型在聚类前进行 PCA 降维分析，以降低存储需求并减少运行时间。PCA 降维方法通过找到数据中最重要的特征方向(主成分)，将原始高维数据映射到一个新的低维空间，从而减少数据维度并保留尽可能多的信息，以便后续的聚类操作。

(3)聚类：首先将降维后的样本特征向量作为输入，然后使用 DBSCAN 算法进行密度聚类。参数设置包括 $epsilon(\varepsilon)$ 和 $MinPts$。其中，ε 是一个半径参数，用于确定邻域的大小；而 $MinPts$ 则定义了核心点的最小密度阈值。接着，对于每个样本特征向量，计算其在给定半径范围内的邻域中包含的样本数。若邻域中的样本数大于或等于 $MinPts$，则该样本被视为核心点。最后，通过合并核心点与在其邻域内的相互密度可达的点来构建聚类。对于不是核心点的样本，如果其在任何核心点的邻域内，则将其归入同一簇。聚类过程不断迭代，直到所有样本都被分配到簇或标记为噪声点。

3）增量学习

在对未知类样本进行聚类后，需要标注参与增量学习的未知类样本，并输入 MILOSR 模型进行学习。与元更新阶段类似，首先为新增的未知类增加新的分类器参数并进行热身

操作，然后将未知类样本输入 MILOSR 模型中。为了缓解灾难性遗忘问题，需要事先冻结调制网络参数，并通过交叉熵损失函数微调编码器和分类器参数。

在增量学习的训练结束后，MILOSR 模型可分类的已知类增加了。在测试中，MILOSR 模型可以对所有已知类进行分类。当出现新的未知类样本时，MILOSR 模型将重复进行样本识别、聚类和增量学习的流程。

5 实验与结果分析

本文在多个公开数据集上进行实验，以验证 MILOSR 方法的效果。首先，介绍实验使用的数据集和模型性能评价指标；然后，对 MILOSR 与主流 OSR 方法进行对比，并对各模块的效果进行实验分析。

5.1 数据集与实验设置

本文的实验使用了 4 个公开图像数据集：CIFAR10，CIFAR+10，CIFAR+50 和 TinyImageNet。数据集的特征信息如表 1 所列。

表 1 数据集的特征信息

Table 1 Characteristics of datasets

数据集	样本量	样本图片的分辨率	类数量	已知类的数量	未知类的数量	开放性/%
CIFAR10	60000	32×32	10	6	4	22.54
CIFAR+10	120000	32×32	110	4	10	46.55
CIFAR+50	120000	32×32	110	4	50	72.78
TinyImageNet	100000	32×32	200	20	180	68.37

参照文献[33]的数据集划分方法对本文的实验数据集进行划分。数据集 CIFAR10 包含 50000 个训练样本和 10000 个测试样本。本文随机选择 6 类作为已知类，其余 4 类作为未知类。在元训练阶段，从已知类样本集中随机采样 3 个类别作为基类，每个训练轮次包含 3 个 1-way 10-shot 任务。Neal[13]结合 CIFAR10 与 CIFAR100，提出用于 OSR 的两种特殊数据集 CIFAR+10 和 CIFAR+50，CIFAR100 包含 100 类图像。本文从 CIFAR10 中随机选择 4 类作为已知类训练模型，从 CIFAR100 中随机选择 10 类或 50 类作为未知类用于测试。在元训练阶段，随机采样 2 个已知类作为基类，每个训练轮次包含 2 个 1-way 10-shot 任务。TinyImageNet 共有 200 个类，决策空间相对复杂。选择其中 20 类作为已知类，并将其他 180 个类作为未知类。在已知类样本中，以 4∶1 的比例划分为训练集和测试集，未知类样本则用于测试。在元训练阶段，随机采样 10 个已知类作为基类，每个训练轮次包含 5 个 2-way 10-shot 任务。

本文提出的 MILOSR 模型以 ResNet50 网络作为主要结构，调制网络模块与编码器模块结构相似。在元训练阶段和测试阶段，使用一层大小为 $2048\times n$ 的全连接层网络作为分类器，其中 n 为类别的数量。在模型预训练过程中，设数据批大小 $batchsize=128$，学习率 $lr=0.1$，训练轮数 $max\_epoch=300$。在模型元训练阶段，$batchsize$ 由具体任务决定，$lr=0.001$，$max\_epoch=200$。

本文使用 OSR 任务常用的 macro-F1 分数和 AUROC 作为评价指标。macro-F1 分数也称宏 F1 分数，是分类任务中综合考虑查准率和查全率的性能度量，常用于评价分类模型的性能。AUROC 即 ROC 曲线下的平均面积，适用于未知类别样本极少到未知类别样本占据大多数的情况[23]，可用于评价模型的未知类识别效果。本文使用 AUROC 评价模型对未知类样本的识别效果，用 macro-F1 评价模型对 OSR 任务的整体效果，并用准确率评价模型在封闭集环境下对已知类样本的分类效果。

5.2 未知类样本的识别效果

为了评估 MILOSR 方法识别未知类样本的效果，本文将其与 SoftMax，OpenMax[7]，G-OpenMax[12]，OSRCI[13]，C2AE[37]，GFROSR[14]，PROSER[9]进行比较。使用表 1 中的数据集（对数据集进行 5 次随机划分）开展实验，统计每次实验的 AUROC，计算 5 个 AUROC 的平均值。具体实验方法参见 4.5 节。MILOSR 方法与现有主流 OSR 方法的 AUROC 数值对比如图 6 所示。

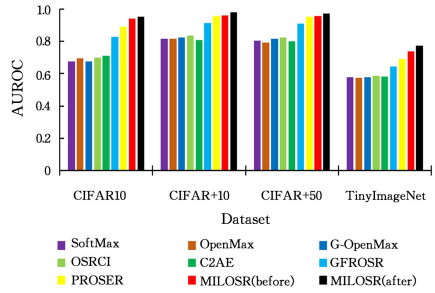


图 6 不同 OSR 方法的 AUROC 对比

Fig. 6 Comparison of AUROC of different OSR methods

在图 6 中，MILOSR 方法包括 2 种情况：MILOSR（before），指未对未知类样本进行增量学习的 MILOSR 模型；MILOSR（after），指已对未知类样本进行增量学习的 MILOSR 模型。从图 6 中可以看出，相对于其他 OSR 方法，MILOSR 方法在未进行增量学习前并没有显著的提升，这是因为 MILOSR 方法为了提高模型小样本增量学习的能力，在提高模型泛化能力的同时降低了分类能力。对未知类样本进行增量学习后，MILOSR 方法的提升效果较为明显。MILOSR 方法在 TinyImageNet 数据集上展现了显著的增量学习效果，提升了约 7%，这归因于 TinyImageNet 的大规模类别和丰富数据，使得 MILOSR 能够更有效地捕捉类别间的差异和共性。相比之下，在 CIFAR+10 和 CIFAR+50 这样类别较少且数据规模较小的数据集上，MILOSR 的提升效果相对较小，约为 1%～2%，这主要是由数据集规模限制和类别信息有限所致。相较于主流 OSR 方法，在 4 个公开数据集上 MILOSR 方法的 AUROC 均取得了最好结果，表明 MILOSR 方法对未知类的识别能力更优。

为了对比 MILOSR 方法与其他方法对已知类的分类能力，本文选取 CIFAR10 和 Tiny-ImageNet 开展实验，测试 MILOSR 方法在封闭集中的分类准确度。图 7 展示了 MILOSR 与部分已公开封闭集准确度的 OSR 方法的结果对比。可以看出，MILOSR 方法在 Tiny-ImageNet 中的封闭集准确度高于其他方法，在 CIFAR10 中略低于其他方法。原因是 CIFAR10 中样本类别较少，在元增量学习训练过程中每类

训练样本量较少，影响了模型分类效果。

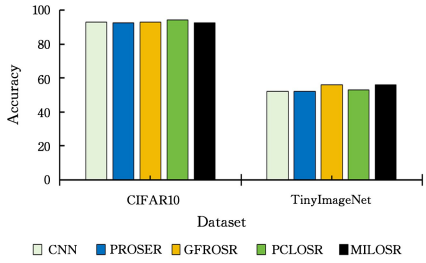


图 7 不同 OSR 方法在封闭集下的准确率对比

Fig. 7 Comparison of accuracy of different OSR methods on closed sets

5.3 开放集识别的整体效果

OSR 的目标不仅是识别未知类，还要对已知类进行正确分类。本文借鉴文献[9]中的实验方法，在 ImageNet-crop，ImageNet-resize，LSUN-crop 和 LSUN-resize 数据集上使用 macro-F1 分数综合评估 MILOSR 模型在 OSR 问题上的整体效果。使用 CIFAR10 的所有训练样本作为训练集，以 CIFAR10 测试集为已知类测试集，并选择 ImageNet 和 LSUN 的测试集作为未知类测试集，通过裁剪和调整大小的方法使其与 CIFAR10 中的样本匹配。数据集设置与实验步骤如 4.5 节所述，结果如图 8 所示。

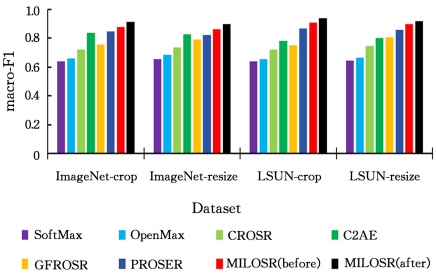


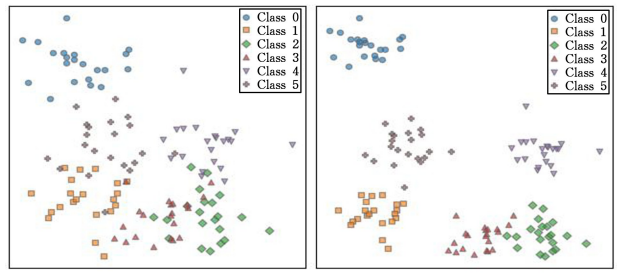
图 8 不同 OSR 方法的 Macro-F1 对比

Fig. 8 Comparison of Macro-F1 scores of different OSR methods

从图 8 可以看出，在进行增量学习前，MILOSR 方法相比于其他 OSR 方法并没有明显优势，因为模型为了适应增量学习而提高了模型泛化能力。在进行增量学习后，MILOSR 方法在 4 个数据集上均取得最好效果，提升 5%～7%。这说明 MILOSR 方法的效果会随着已识别出的未知类样本的增加而不断显示出优势。

本文使用 t-SNE 方法对特征空间进行可视化。t-SNE 通过计算高维数据点的相似度并将其映射到低维空间，同时最小化两者相似度分布之间的 KL 散度，来保留数据的局部结构。该算法使用梯度下降法优化低维表示，使得相似的高维数据点在低维空间中紧密聚集。使用 CNN 与 MILOSR 方法进行对比。选用数据集 CIFAR10 中的 6 种样本，分别使用 CNN 和 MILOSR 方法获得样本特征向量。使用 t-SNE 方法将这些样本特征向量映射到二维空间，并将所得的降维样本坐标绘成散点图。图 9 展示了两种方法的模型中样本在特征空间中的分布情况。

可以看出，图 9(a)中 CNN 方法的样本分布比较分散，占用了较多的特征空间，表明 CNN 对类别的区分能力较差；而图 9(b)中 MILOSR 方法的同类样本间分布更紧密，占用特征空间较小，并且各类样本距离较远，表明 MILOSR 方法对类别的区分能力更强，且未知类样本在特征空间中不易与已知类样本混淆。



(a)CNN (b)MILOSR

图 9 CNN 方法和 MILOSR 方法的样本分布

Fig. 9 Sample distribution of CNN and MILOSR

5.4 消融实验

为了评估 MILOSR 方法的元增量学习机制、调制网络模块和深度聚类模块对分类效果的影响，开展了消融实验。将 MILOSR 方法分别与不进行元训练、没有调制网络或不对未知类样本进行聚类的 MILOSR 方法进行对比。首先，使用传统的基于 CNN 的 OSR 方法作为基准进行对比。然后，在此基础上引入元增量学习机制，对不含调制网络模块的 OSR 方法(MILOSR w/o MN)进行测试。最后，添加调制网络模块，对没有深度聚类模块的 MILOSR 方法(MILOSR w/o Deep DBSCAN)进行测试。实验步骤如 4.5 节所述。MILOSR 方法与 CNN，MILOSR w/o MN 和 MILOSR w/o DeepDBSCAN 方法在 CIFAR10，CIFAR+10，CIFAR+50 上的实验结果如图 10 所示。

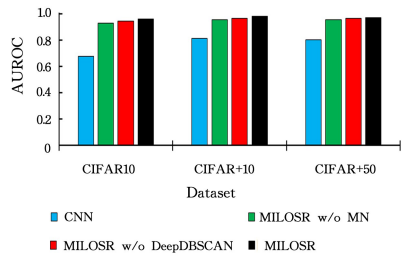


图 10 各模块的未知类识别效果对比

Fig. 10 Comparison of unknown class recognition effects of each module

从图 10 可以看出，MILOSR 模型的元增量学习对模型对未知类样本的增量学习性能起到了显著的提升作用。这表明元增量学习有效地提高了 MILOSR 模型对增量学习环境的适应能力，从而有效提高了 MILOSR 模型性能。其次，深度聚类模块通过对未知类样本进行分类处理，进一步提高了 MILOSR 模型对未知类样本的识别效果，提升约 3%～4%。这是因为增量学习过程不可避免地会对模型已有分类能力产生影响，而聚类模块将离散样本识别出来，拒绝将其增量学习进 MILOSR 模型，降低了离散样本对 MILOSR 模型的影响。调制网络模块对 MILOSR 模型的性能提升约 2%～3%。这是因为调制网络模块可以区分 MILOSR 模型中参数的重要性，同时允许非关键参数学习新的未知类知识，避免遗忘的同

时提高了模型增量学习的能力。由以上分析可得，MILOSR 模型的元增量学习框架、调制网络模块和深度聚类模块在提升模型分类能力方面都起到了积极作用。

5.5 MILOSR 模型的时间效率分析

本节主要讨论 MILOSR 模型中的各模块对模型训练时间的影响。将 MILOSR 模型分别与 CNN，MILOSR w/o MN 和 MILOSR w/o DeepDBSCAN 方法进行对比。实验过程与 4.5 节相同。图 11 展示了 MILOSR 模型在数据集 CIFAR10 和 TinyImageNet 上的训练时间对比。

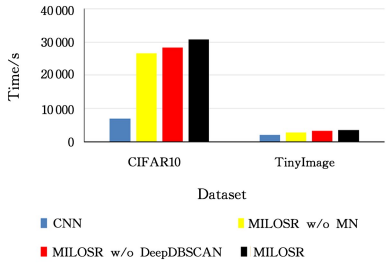


图 11 训练时间对比

Fig. 11 Comparison of training time

由图 11 可得，与 CNN 相比，MILOSR 模型的训练时间明显增加。这是因为 MILOSR 的参数量约为 2.56×10^7，需要进行两轮训练。首先使用原型对比学习方法进行预训练，然后使用双层优化方法进行多轮元训练。调制网络模块与深度 DBSCAN 模块对 MILOSR 模型训练时间的影响较小。这是因为调制网络模块仅在元更新阶段与编码器一起更新参数，故对训练时间影响有限。而深度 DBSCAN 模块不需要再训练新的编码器，只需要少量时间进行 DBSCAN 聚类，故对训练时间影响较小。

结束语 传统的开放集识别方法可以识别出未知类样本并拒绝对其分类，但未能有效利用这些样本蕴含的知识。在实际应用中，开放集识别模型还面临着难以提前确定未知类别数量、样本数量有限等困难。这些情况影响了开放集识别模型的准确性和泛化性。鉴于此，本文提出基于元增量学习的开放集识别方法 MILOSR，对识别出的未知类样本进行增量学习，以提高开放集识别模型的分类准确性和泛化性。为了有效利用未知类样本的知识和解决未知类样本数量有限的问题，本文构造了基于元增量学习的开放集识别模型。该模型使用双层优化机制进行增量学习训练，通过一系列小样本增量学习任务进行训练来微调模型参数，使其具有小样本增量学习能力。为了进一步提高模型的增量学习能力，引入权重激励机制获取模型参数的重要性，使用非关键参数进行增量学习。为了解决模型不能提前确定未知类别数量的问题，本文设计深度 DBSCAN 方法对识别出的未知类样本进行聚类，进而确定聚类簇数；使用成簇的未知类样本对 MILOSR 模型进行增量学习。最后，在 4 个公开数据集上开展实验，实验结果表明，相比主流 OSR 方法，MILOSR 方法在 AUROC 和 F1 分数上均具有更好的效果。这表明，MILOSR 方法可以有效学习识别出未知类样本的知识，提高了开放集识别模型的准确性和泛化性。

未来计划探索其他元学习方法，如使用 Reptile 元学习方法，通过单层循环调整开放集识别模型的参数，降低其计算复杂度，提高模型训练效率。

参 考 文 献

[1] ZHAO H W，WU H，MA K，et al. Image classification framework based on knowledge distillation. [J]. Journal of Jilin University(Engineering and Technology Edition)，2024，54(8)：2307-2312.

[2] ZHANG H Y，XIA Y L，ZHOU K W，et al. A Method of Multi-label Image Classification with Fusing Powerful Semantic Correlation[J]. Journal of Chongqing Technology and Business University(Natural Science Edition)，2023，40(5)：8-15.

[3] SCHEIRER W J，DE REZENDE ROCHA A，SAPKOTA A，et al. Toward open set recognition[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence(TPAMI)，2012，35(7)：1757-1772.

[4] ZHOU D W，WANG Q W，QI Z H，et al. Deep class-incremental learning：A survey[J]. arXiv：2302.03648，2023.

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

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

[7] BENDALE A，BOULT T E. Towards open set deep networks[C]//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition(CVPR). 2016：1563-1572.

[8] SHU L，XU H，LIU B. Doc：Deep open classification of text documents[C]//Conference on Empirical Methods in Natural Language Processing. 2017：2243-2979.

[9] ZHOU D W，YE H J，ZHAN D C. Learning placeholders for open-set recognition[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). 2021：4401-4410.

[10] YANG H M，ZHANG X Y，YIN F，et al. Convolutional prototype network for open set recognition[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence，2022，44(5)：2358-2370.

[11] LU J，XU Y，LI H，et al. Pmal：Open set recognition via robust prototype mining[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2022：1872-1880.

[12] GE Z Y，DEMYANOV S，CHEN Z T，et al. Generative openmax for multi-class open set classification[C]//Computer Vision and Pattern Recognition(CVPR). 2017.

[13] NEAL L，OLSON M，FERN X，et al. Open set learning with counterfactual images[C]//Proceedings of the European Conference on Computer Vision(ECCV). 2018：613-628.

[14] PERERA P，MORARIU V I，JAIN R，et al. Generative-discriminative feature representations for open-set recognition[C]//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). 2020：11814-11823.

[15] YANG Y，HOU C P，LANG Y，et al. Open-set human activity

recognition based on micro-doppler signatures[J]. Pattern Recognition, 2019, 85: 60-69.
[16] FENG Q, KANG G, FAN H, et al. Attract or distract: Exploit the margin of open set[C]// Proceedings of the IEEE/CVF International Conference on Computer Vision. 2019: 7990-7999.
[17] KONG S, RAMANAN D. Opengan: Open-set recognition via open data generation[C]// Proceedings of the IEEE/CVF International Conference on Computer Vision. 2021: 813-822.
[18] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks[J]. Communications of the ACM, 2020, 63(11): 139-144.
[19] DE ROSA R, MENSINK T, CAPUTO B. Online open world recognition[J]. arXiv: 1604. 02275, 2016.
[20] PRAKHYA S, VENKATARAM V, KALITA J. Open set text classification using CNNs[C]// Proceedings of the 14th International Conference on Natural Language Processing (ICON-2017). 2017: 466-475.
[21] SHU Y, SHI Y, WANG Y, et al. P-odn: Prototype-based open deep network for open set recognition[J]. Scientific Reports, 2020, 10(1): 7146.
[22] DANG S, CAO Z, CUI Z, et al. Open set incremental learning for automatic target recognition[J]. IEEE Transactions on Geoscience and Remote Sensing, 2019, 57(7): 4445-4456.
[23] GAO F, YANG L, LI H. A survey on open set recognition[J]. Journal of Nanjing University(Natural Sciences), 2022, 58(1): 115-134.
[24] BENDALE A, BOULT T. Towards open world recognition [C]// Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition(CVPR). 2015: 1893-1902.
[25] GENG C, HUANG S, CHEN S. Recent advances in open set recognition: A survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2020, 43(10): 3614-3631.
[26] DE LANGE M, ALJUNDI R, MASANA M, et al. A continual learning survey: Defying forgetting in classification tasks[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 44(7): 3366-3385.
[27] TAO X, HONG X, CHANG X, et al. Few-shot class-incremental learning[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2020: 12183-12192.
[28] HOSPEDALES T, ANTONIOU A, MICAELLI P, et al. Meta-learning in neural networks: A survey[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2021, 44(9): 5149-5169.
[29] FINN C, ABBEEL P, LEVINE S. Model-agnostic meta-learning for fast adaptation of deep networks[C]// International Conference on Machine Learning. PMLR, 2017: 1126-1135.
[30] SUN J Y, WANG X C, SUN Z G, el at. Prototype Contrastive Learning for Open Set Recognition[J]. Journal of Chinese Computer Systems, 2024, 45(7): 1671-1678.
[31] YANN L C, DENKER J, SOLLA S. Optimal brain damage[J]. Advances in Neural Information Processing Systems, 1989, 2: 598-605.
[32] KIRKPATRICK J, PASCANU R, RABINOWITZ N, et al. Overcoming catastrophic forgetting in neural networks[J]. Proceedings of the National Academy of Sciences, 2017, 114(13): 3521-3526.
[33] CHI Z, GU L, LIU H, et al. Metafscil: A meta-learning approach for few-shot class incremental learning[C]// Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022: 14166-14175.
[34] QUADER N, BHUIYAN M M I, LU J, et al. Weight excitation: Built-in attention mechanisms in convolutional neural networks [C]// Computer Vision. 2020: 87-103.
[35] SUN J Y, ZHOU B W, WEN L J, et al. Anomaly detection of business processes based on attention mechanism[J]. Computer Integrated Manufacturing Systems, 2022, 28(10): 3039-3051.
[36] CARON M, BOJANOWSKI P, JOULIN A, et al. Deep clustering for unsupervised learning of visual features[C]// Proceedings of the European Conference on Computer Vision(ECCV). 2018: 132-149.
[37] OZA P, PATEL V M. C2ae: Class conditioned auto-encoder for open-set recognition[C]// Procee-dings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). 2019: 2307-2316.

SUN Jinyong, born in 1978, Ph. D, professor, is a member of CCF (No. 24794M). His main research interests include machine learning and business process management.

WANG Xuechun, born in 1997, master. Her main research interests include machine learning and so on.

(责任编辑:柯颖)