软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software [doi: 10.13328/j.cnki.jos.007233]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

融合扩增技术的无监督域适应方法*

曹 艺[1], 郭茂祖[2], 吴伟宁[1]

[1](哈尔滨工程大学 计算机科学与技术学院, 黑龙江 哈尔滨 150001)

[2](北京建筑大学 电气与信息工程学院, 北京 102616)

通信作者: 吴伟宁, E-mail: wuweining@hrbeu.edu.cn

摘 要: 域适应 (domain adaptation, DA) 是一类训练集 (源域) 和测试集 (目标域) 数据分布不一致条件下的机器学习任务. 其核心在于如何克服数据域的分布差异对分类器泛化能力的负面影响, 即设计合理而有效的训练策略, 通过最小化数据域之间的差异, 获得高泛化能力的分类模型. 研究了源域中包含标注信息, 目标域中缺少标注信息条件下的无监督域适应 (unsupervised domain adaptation, UDA) 任务. 将其形式化为如何利用部分标注样本和其余未标注样本进行分类器训练的半监督学习问题, 进而引入伪标签 (pseudo label, PL) 和一致性正则化 (consistent regularization, CR) 这两种半监督学习技术, 对所观测数据域有目的进行标记和样本扩增, 使用扩增后的训练样本学习分类器, 从而, 在无监督域适应任务上取得了良好的泛化能力. 提出一种融合扩增技术的无监督域适应 (augmentation-based unsupervised domain adaptation, A-UDA) 方法, 在分类器的训练过程中: 首先, 使用随机数据增强技术 (random augmentation) 对目标域中的未标注样本进行扩增, 即样本扩增; 其次, 利用模型的预测输出结果, 对高置信度的未标注样本添加伪标记, 即标注扩增; 最后, 使用扩增后的数据集训练分类模型, 利用最大均值差异 (maximum mean difference, MMD) 计算源域和目标域的分布距离, 通过最小化该分布距离获得具有高泛化能力的分类器. 在 MNIST-USPS, Office-Home 和 ImageCLEF-DA 等多个无监督域适应任务上对所提出方法进行比较, 与现有其他工作相比, 获得了更好的分类效果.

关键词: 无监督域适应; 半监督学习; 数据扩增; 伪标签; 一致性正则化

中图法分类号: TP18

中文引用格式: 曹艺, 郭茂祖, 吴伟宁. 融合扩增技术的无监督域适应方法. 软件学报. http://www.jos.org.cn/1000-9825/7233.htm

英文引用格式: Cao Y, Guo MZ, Wu WN. Unsupervised Domain Adaptation Method with Augmentation Technology. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7233.htm

Unsupervised Domain Adaptation Method with Augmentation Technology

CAO Yi[1], GUO Mao-Zu[2], WU Wei-Ning[1]

[1](College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China)

[2](School of Electrical and Information Engineering, Beijing University of Civil Engineering and Architecture, Beijing 102616, China)

Abstract: Domain adaptation (DA) is a group of machine learning tasks where the training set (source domain) and the test set (target domain) exhibit different distributions. Its key idea lies in how to overcome the negative impact given by these distributional differences, in other words, how to design an effective training strategy to obtain a classifier with high generalization performance by minimizing the difference between data domains. This study focuses on the tasks of unsupervised DA (UDA), where annotations are available in the source domain but absent in the target domain. This problem can be considered as how to use partially annotated data and unannotated data to train a classifier in a semi-supervised learning framework. Then, two kinds of semi-supervised learning techniques, namely pseudo labels (PLs) and consistent regularization (CR), are used to augment and annotate data in the observed domain for learning the classifier.

* 基金项目: 国家自然科学基金 (61976067, 62271036)
曹艺和郭茂祖对本文有同等贡献.
收稿时间: 2023-04-20; 修改时间: 2023-09-01; 采用时间: 2024-06-05; jos 在线出版时间: 2024-08-28

Consequently, the classifier can obtain better generalization performance in the tasks of UDA. This study proposes augmentation-based UDA (A-UDA), in which the unannotated data in the target domain are augmented by random augmentation, and the high-confident data are annotated by adding pseudo-labels based on the predicted output of the model. The classifier is trained on the augmented data set. The distribution distance between the source domain and the target domain is calculated by using the maximum mean difference (MMD). By minimizing this distance, the classifier achieves high generalization performance. The proposed method is evaluated on multiple UDA tasks, including MNIST-USPS, Office-Home, and ImageCLEF-DA. Compared to other existing methods, it achieves better performance on these tasks.

Key words: unsupervised domain adaptation (UDA); semi-supervised learning (SSL); data augmentation; pseudo label (PL); consistent regularization (CR)

近年来, 深度学习在视觉对象分类、识别与检测、自然语言处理、语义分析以及生物信息挖掘等多种现实任务中取得了重要进展. 这类学习任务的特点是, 需要预先收集大量带有详细语义标注信息的数据作为训练集, 使用大规模训练样本对多层卷积网络等模型进行训练. 同时, 使用部分来自相同任务的标注样本对超参数进行调整, 直至模型精度提高或错误率降低到指定阈值为止. 当训练停止后, 将所学习的模型用于对测试集中的样本进行预测, 获得预测结果. 通常, 所收集的训练集和测试集中的数据来自相同的学习任务, 即数据具有相同的分布信息. 然而, 在某些情况下, 深度学习难以获得大量来自相同任务的标注数据, 但可以收集到类似任务的一组标注样本用于训练, 即训练数据和测试数据的分布信息不同的条件下学习一个深度网络, 即域适应任务[1]. 特别地, 当训练数据含有标注信息, 而测试数据缺少标注信息时, 也称为无监督域适应任务.

目前, 无监督域适应的研究工作[2−8]可被分为两个趋势, 即基于源域和目标域之间距离最小化的域适应策略和基于源域和目标域之间样本生成的域适应策略. 这里, 在第 1 种趋势中, 大部分研究工作通过设计距离或度量函数[9−14]来衡量源域和目标域的分布差异, 在训练过程中, 将这种差异与分类器损失函数相结合, 逐步最小化这一差异, 从而, 克服数据偏置, 获得分类器泛化性能最大化. 例如, 在文本语义识别中常见的对齐技术[15,16], 矩匹配[13,14]方法, 以及自解码器中的隐空间等. 在第 2 种趋势中, 研究人员则利用域判别器 (domain discriminator) 对源域和目标域中的样本进行区分[3,16−23], 在训练过程中, 生成部分特征用于混淆域判别器, 最小化两个数据域之间的样本差异, 达到使分类器性能提升的目的. 另外, 在生成特征的过程中, 也有部分研究工作将模型在目标域上的预测结果引入到训练过程中[12,24−34], 希望能够保持数据域中的结构以及类别信息等. 但是, 这类做法对目标域上预测结果的准确度要求较高, 如果模型预测结果与真实标注差距较大, 则会对模型训练过程产生负面影响, 降低分类器的泛化性能.

本文在现有无监督域适应研究工作的基础上, 将此任务视作是在部分样本有标注、其余样本无标注条件下的半监督学习问题, 然后, 引入了半监督学习中的两种数据扩增技术, 即用于样本扩增的一致性正则化 (consistent regularization, CR) 技术和用于标注扩增的伪标签 (pseudo label, PL) 技术, 对有标注的源域和无标注的目标域中的数据进行扩增, 在生成后的数据集上对分类器进行训练. 这里, 在一致性正则化过程中, 使用了随机数据增强技术 (random augmentation) 对目标域中的未标注样本进行样本扩增; 在添加伪标签过程中, 利用了分类模型的预测结果, 为高置信度的未标注样本添加伪标记来进行标记扩增. 在训练过程中, 使用了最大均值差异 (maximum mean difference, MMD) 计算源域和目标域的分布距离, 通过最小化该分布距离达到分类器泛化能力最大化的目的. 在图 1 中, 本文给出了基于扩增技术的无监督域适应方法的框架图.

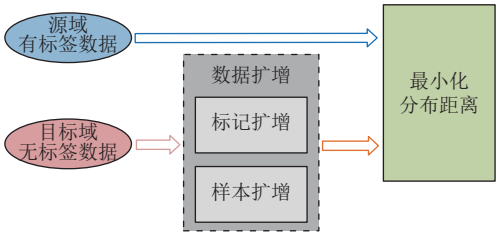


图 1 基于扩增技术的无监督域适应方法框架

本文第 1 节简要介绍了无监督域适应和基于半监督学习的数据扩增技术. 第 2 节详细说明了本文的主要工作. 第 3 节是实验部分, 通过在多个无监督域适应领域的学习任务, 对本文所提出方法进行了比较, 说明了方法的有效性. 第 4 节为结论和未来研究趋势.

1 相关工作

1.1 无监督域适应

无监督域适应是一类在训练数据和测试数据来自不同分布条件下的机器学习问题. 其中, 带有标注信息的训练数据为源域, 缺少标注信息的测试数据为目标域, 学习任务是使得源域上训练得到的分类器能够在目标域上获得最佳泛化能力[35]. 在贝叶斯理论框架下, 训练数据和测试数据应具有相同的先验分布, 以保证分类器的泛化能力. 因此, 现有无监督域适应的研究力图减少训练数据和测试数据之间的这种分布差异. 其方法可大概分为两类: 基于数据域分布距离或度量的最小化方法和基于样本或特征生成的训练方法.

基于数据域分布距离或度量最小化方法的主要思想是设计能够合理度量数据域之间差异的函数, 使用此函数度量源域和目标域之间的分布距离. 通常情况下, 此分布距离越小, 则源域和目标域之间的差异越小. 在分类器训练过程中, 将分布距离最小化与损失函数的最小化相结合, 使用优化方法最小化组合后的结果, 从而得到最优的分类器训练结果. 采用这种思想的无监督域适应方法包括: 最大均值差异 (maximum mean difference, MMD)[10,36], 基于多项式核 MMD 的相关对齐 (correlation alignment, CORAL)[15,37]和 KL 散度距离[38]等技术. 在最大均值差异的基础上, DDC (deep domain confusion) 模型[10]引入了此距离, 用于在多层卷积网络中学习混淆域中的不变特征. 多核最大均值差异 (multi kernel-maximum mean discrepancies, MK-MMD)[9]使用多个核对距离进行度量, 拉近数据域之间的特征分布距离, 以及同时考虑边缘和条件概率分布的联合 MMD 方法[26]. 除最大均值差异的工作外, 其他分布距离的方法还有基于欧氏距离的映射相关对齐技术[39], 测地线距离[40]和无限维协方差矩阵[40], 这些工作的特点是试图找到数据域间的共享特征表示. 而另外一些工作则针对数据域中的个体, 对源域和目标域中的属性进行建模, 找到有意义的特征表示, 保证数据域不变[41]. 以及, 使用数据域中的伪标签建立条件分布, 使用此条件分布对齐的形式代替两个数据域之间语义对齐的问题, 力图解决使用边缘分布无法保证数据域的语义对齐的问题[17,42].

基于样本特征生成的训练方法[3,16−23]则受到了对抗网络训练的启发, 使用对抗网络生成一组能够使分类器混淆的样本, 使用这组样本训练分类器, 达到分类性能最大化. 这里, 生成对抗网络[43]的训练方法是指利用两个神经网络进行对抗训练, 尽可能生成使判别网络迷惑的“真”样本, 而分类器则尽可能对包含这些生成样本的数据集进行判断, 给出准确的预测结果. 例如: 通过最小化分类模型误差, 最大化判别器误差的 ADDA[44]方法; 通过增加梯度翻转层达到对抗效果的 DANN[3]方法; 使用信息熵计算分类器预测结果的不确定度, 从而增加数据域知识迁移的 CDAN[17]方法等. 此外, 也有一些工作间接地利用了对抗-协作的思想来完成域适应任务, 例如: 通过多层卷积网络的权值共享, 在多个数据域中找到样本的联合分布, 间接完成对抗训练任务[45], 基于数据域之间的协作和对抗策略的域适应任务[25]和基于重构编码和共享编码表示的深度重构网络 DRCN[46]等.

1.2 基于半监督技术的数据扩增

半监督学习 (semi-supervised learning, SSL) 是一种利用少量标注数据和大量未标注数据联合训练分类器的学习技术[47]. 在数据扩增任务中, 常用的半监督学习方法包括用于标记扩增的伪标签技术和用于样本扩增的一致性正则化技术.

伪标签技术一般用于对数据集中的标记信息进行扩增, 其过程是, 首先利用标注好的数据训练分类器, 使用该分类器对其余未标注数据的标记信息进行预测, 根据预测结果为未标记数据添加标记信息, 将这些标注后的样本用于后续分类器的训练过程, 从而达到提高分类器性能的目的. 基于这种思想, 这部分的研究工作包括使用多层卷积网络的预测结果作为伪标签信息[48], 使用当前分类器的预测结果作为未标注样本的伪标签[49], 其方法特点是, 为每个未标注样本引入权重, 用于衡量与该样本距离最近的若干个样本的不确定程度. 距离越近, 其不确定度越高, 权值越大. 另外, 也有研究工作借鉴了主动学习中样本不确定性的思想[50], 使用样本的不确定性作为衡量标准,

对未标注节点添加伪标签信息. 伪标签技术对标记信息的扩增依赖于分类器的预测结果, 因此, 在初始数据集上, 对分类器训练精度具有较高的要求. 同时, 初始数据集的选择对分类器的训练也有一定影响.

与伪标签技术不同, 一致性正则化技术则是对样本进行扩增. 其基本思想是, 给定某个输入样本, 若对数据添加扰动, 对于分类器而言, 其输出应当保持一致. 这种思想也是用于判断当前分类器是否过拟合的标准, 因此, 基于一致性正则化技术的数据扩增方法的主要手段是强制使模型对添加扰动后的数据的预测输出与原始数据的预测输出结果保持一致. 其分类器训练过程是, 对于数据域中的样本, 通过各种手段为其添加扰动, 在训练过程中, 使用度量函数计算添加扰动后的数据项与原始数据分别对应的预测结果的差异, 并迭代训练, 使该差异最小化. 研究结果表明, 这一做法可以减少分类器过拟合, 有效地提升分类器的泛化性能, 特别是当数据域中的样本数量不足时. π-model 算法[51]是最先被提出的一种一致性正则化方法, 其做法是使用数据增强技术为某样本添加扰动, 分类模型分别给出该样本对应的增强样本的输出结果, 使用此结果计算预测输出的差异值, 并强制该值最小化. 在这一算法思想的基础上, 研究人员又开发了其他在数据中添加扰动的方法[52−54], 例如: 当数据形式为图像时, 通过设计合理的搜索策略对平移、旋转、翻转或随机裁剪后的原始图像进行变换等[52], 在实际任务中取得了良好的效果. 此外, 对抗训练的思想也大量被用于这一领域, 即采用两个模型之间进行竞争的方式获得有利于提高分类器泛化能力的样本, 从而达到对原始数据进行扩增的目的. 比较有代表性的工作包括: VAT 模型[55], 其一致性正则化过程是使所生成的对抗样本的预测结果与原始数据对应的预测结果一致; Mean teacher[56]算法, 其一致性正则化过程是使两个网络的结构一致, 其中一个网络的参数为另一个网络参数的指数移动平均值. 此外, 在一致性正则化损失的衡量方面, 研究人员通常采用均方误差[51]或交叉熵损失函数[53]等计算模型输出的差异.

2 基于扩增技术的无监督域适应方法

在现有工作的基础上, 本文将数据扩增技术引入到无监督域适应任务中. 分别引入了伪标签技术对目标域中的样本标记进行了扩增和一致性正则化技术对目标域中的样本进行了扩增. 在分类器的训练过程中, 使用最大均值差异函数对两个数据域的分布差异进行计算, 通过最小化扩增后数据集上的分布差异达到分类器在目标域上性能提升的目的.

2.1 问题形式化

假定源域 $D_s=\{(x_i^s,y_i^s)\}_{i=1}^{n_s}$, 其中 $x_i^s\in R^d$. 其中, $x_i^s\in X_s$ 表示第 i 个 d 维样本, $y_i^s\in Y_s$ 表示该样本对应的标注. n_s 表示源域中的样本数量, X_s 表示源域样本集, Y_s 表示源域标记集. 令目标域为 $D_t=\left\{x_j^t\right\}_{j=1}^{n_t}$, 其中 $x_j^t\in R^d$ 表示第 j 个 d 维样本, n_t 表示目标域中的样本数量, 则无监督域适应学习问题可形式化为:

$$\theta=\arg\min_{\theta\in\Theta}(L_s+L_d) \tag{1}$$

其中, θ 是分类器参数, L_s 是源域上分类器的损失函数, 此损失函数一般使用标注数据进行计算. L_d 是目标域上分类器的损失函数, 在现有无监督域适应任务中, 通常使用源域 D_s 和目标域 D_t 之间的距离作为损失函数. 较为常用的距离函数有最大均值差异 MMD, 其做法是假定存在连续且有界的半正定核且 H 是相应的再生希伯特核空间, 通过引入映射 $\Phi: X\to H$, 来计算源域和目标域之间的最大均值差异, 即:

$$MMD(p(x),p(y))=\left\|E_{x\sim p(x)}[\Phi(x)]-E_{y\sim p(y)}[\Phi(y)]\right\|_H^2 \tag{2}$$

其中, $\|\cdot\|$ 表示再生核希尔伯特空间范数. 假设 X 和 H 属于同一空间 R^d 且 $\Phi(x)=x$, 则最大均值差异的目的是减少两个分布之间均值的差异, 即有下式成立:

$$Loss(D_s,D_t)=\left\|\frac{1}{n_s}\sum_{i=1}^{n_s}\phi(x_i^s)-\frac{1}{n_t}\sum_{j=1}^{n_t}\phi\left(x_j^t\right)\right\| \tag{3}$$

这里, 在实际任务中, 对于映射函数 ϕ 的选择是衡量分布差异的重点. 同时, 为了保证特征映射的多样性, 本文采用了多核 (multiple kernel) 形式, 使用多个带有权重的内核对变换后的特征所分布差异进行计算. 其计算式如下:

$$L_d = d_k^2(D_s, D_t) = \left\| \frac{1}{n_s}\sum_{i=1}^{n_s}\phi(x_i^s) - \frac{1}{n_t}\sum_{j=1}^{n_t}\phi\left(x_j^t\right) \right\|_H^2 \tag{4}$$

在实际应用中, 由于现有 MMD 是基于单一核函数进行特征映射, 而选择合适的核函数可以从更高阶的角度衡量两个分布间的差异, 故本文在单一核函数基础上采用多个核函数的组合. 为了保证特征映射的多样性, 本文采用 MK-MMD 对源域和目标域进行分布差异的度量, 即通过多个核函数的线性组合得到距离计算的结果, 目的是使变换后的特征具有更好的表达能力.

在上述无监督域适应工作基础上, 本文将源域 D_s 和目标域 D_t 分别视作标注数据和未标注数据, 引入两种半监督技术对域适应工作进行改进, 改进后的损失函数计算式如下:

$$L_{\text{total}} = L_s + \lambda_t L_t + \lambda_d L_d \tag{5}$$

其中, λ_t 和 λ_d 是权重因子, 分别用于不同任务下对损失函数进行加权. 其权重根据所学习任务的数据集大小来设置, 例如: 在本文数据分类任务中, λ_t 和 λ_d 均设为 1; 在视觉对象分类任务中, $\lambda_t = 1$, λ_d 则采用循序渐进的方式, 逐步从 0 增长为 1, 其计算式如下:

$$\lambda_d = \frac{2}{1+\mathrm{e}^{-10\times\frac{i}{T}}} - 1 \tag{6}$$

其中, i 表示当前学习器所在迭代步, T 表示预先设置的学习器总共需要的迭代步数. λ_d 的设置是考虑到图片尺寸较大, 单个迭代步中所选择的样本数目较少, 为了避免初始所选择源域样本数目较少而对整个损失造成的负面影响, 故采用根据迭代步骤的增加而逐步加大这部分损失的策略. L_s 是源域上基于样本真实标注信息所产生的损失项, 其计算式为:

$$L_s = L_{\text{cls}}\left(Y^s, \hat{Y}^s\right) = -\sum_{i=1}^{n_s} y_i^s \log\left(\hat{y}_i^s\right) \tag{7}$$

其中, x_i^s 表示源域中的样本, $\phi(x_i^s)$ 是该样本在核空间中所映射的特征, $\hat{y}_i^s$ 表示学习器对该样本的预测软标签. L_t 则是基于伪标签和基于一致性正则化技术所产生的扩增后的损失项, 下面分别在第 2.2 节和第 2.3 节中进行介绍.

在图 2 中, 本文给出了基于扩增技术的无监督域适应方法的结构图, 其中, classification loss 表示对分类器在源域上进行训练所使用的损失函数, 本文在各个任务中使用交叉熵函数. domain loss 表示基于 MK-MMD 距离的源域与目标域损失. consistency regularization loss 表示基于伪标记和一致性正则化技术所产生的目标域上的损失, 将在第 2.2 节和第 2.3 节对此进行详细解释.

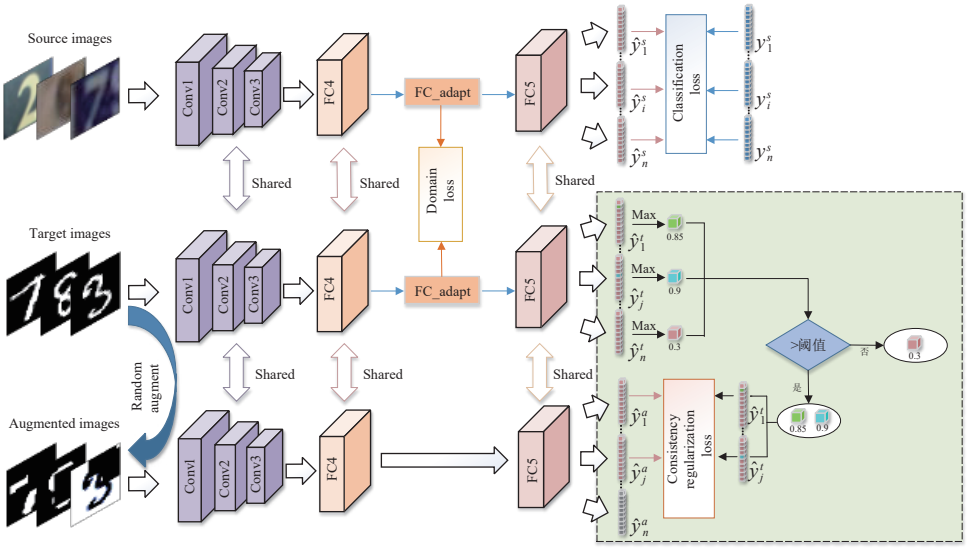


图 2 基于伪标签和一致性正则化的无监督域适应方法

2.2 基于伪标记技术的标注扩增

根据第 2.1 节中问题形式化部分, 本节介绍如何引入伪标记技术对目标域中的样本进行标注扩增. 其基本思想是利用源域或者目标域中的带标签的样本训练分类器, 将目标域中未标注样本传入分类器, 获得样本的预测结果作为“硬”或“软”标记. 在训练中设定一个固定的阈值, 根据预测结果选择置信度较高的样本添加伪标签并加入目标域的训练集. 上述过程迭代进行, 直至分类器的泛化精度达到一定程度后终止. 这一做法的理论依据是样本间的聚类假设, 在样本空间中, 若两个样本位于同一个数据簇中, 那么它们具有相同类别标记的可能性较大. 因此, 本文在目标域中选择能够位于同一个数据簇中的样本, 添加标记后进行损失计算, 用于增加标注样本的数量. 在图 3 中, 给出了目标域上的伪标签添加过程.

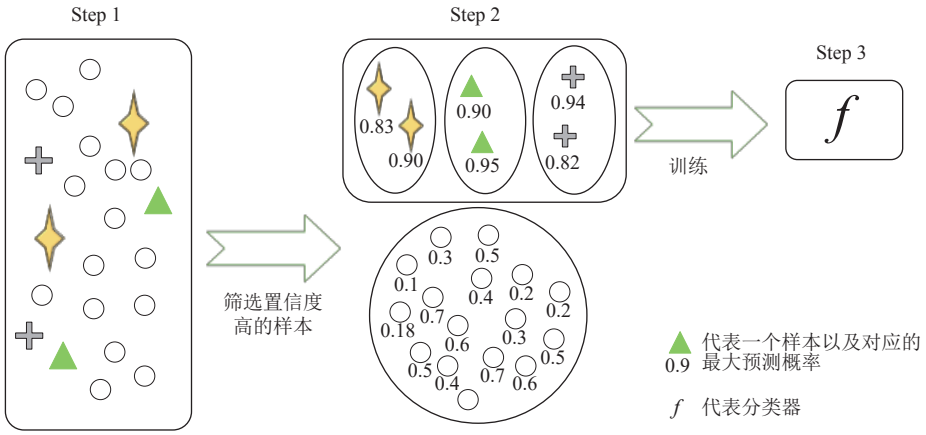


图 3 目标域中样本伪标签添加过程

在图 3 中, Step 1 表示目标域中的未标注样本, 空心圆圈表示样本对应的预测概率低于预设阈值的样本, 其他符号则表示样本的预测概率高于阈值的样本, 符号不同则样本被预测的类别也不同. Step 2 表示根据预测概率将样本划为不同类别, 并添加伪标记, 使用添加伪标记后的样本进行分类器训练过程. 此部分样本也被称为高置信度的样本. 在第 3 节中, 本文使用了深度神经网络经过 Softmax 层归一化后得到的预测概率, 即“软”标签作为高置信度样本的伪标签, 目的是减少“硬”标签在样本数量较少情况下对分类器准确性的负面影响. 在实验部分, 使用源域上的预训练模型作为分类器的初始化参数, 在训练过程中将源域和目标域样本同时送入分类器中进行训练. 根据预测概率和阈值对目标域中样本添加伪标注的流程如图 4 所示.

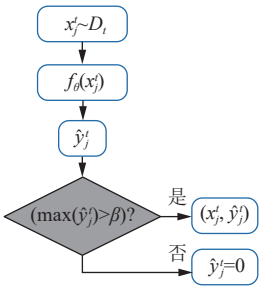


图 4 根据预测概率和阈值为目标域中样本添加伪标注流程

令阈值为 β, 在实验中令 $\beta = 0.8$. $\hat{y}_j^t$ 为目标域中为高置信度的未标注样本 x_j^t 添加的软标签, 若低于此置信度阈值, 则丢弃此样本, 即 $\hat{y}_j^t = 0$, 其选择标准如下式:

$$\hat{y}_j^t = \begin{cases} \hat{y}_j^t, & \text{if } \max\left(\hat{y}_j^t\right) > \beta \\ 0, & \text{others} \end{cases} \tag{8}$$

在实验部分, 本文说明了通过设定阈值的方式, 选择高置信度的样本添加伪标签和加入训练过程, 可以有效地利用源域上的数据信息, 有效提升目标域上分类器的各项性能. 随着分类器训练次数的增加, 可以有效提高扩增数据的标记质量, 加快目标域上分类器的收敛速度.

2.3 基于一致性正则化的样本扩增

本节给出了如何基于一致性正则化技术对目标域中的样本进行扩增. 一致性正则化是通过对输入数据添加扰动的方式, 强制添加扰动后的数据与原始数据的预测输出结果保持一致, 目的是使分类器具有更好的抗干扰能力, 而不需要依赖具体的标记信息. 因此, 本文采用此方式对目标域中的部分数据进行扩增, 并结合第 2.2 节中标记扩增的部分, 共同达到增加目标域中有效训练样本的数量、更好的迁移分类模型的目的.

给定目标域中任意样本 x_j^t, 通过增强技术可以得到添加扰动后的样本 x_j^a. 同时, 可以得到此样本的软标记 $\hat{y}_j^t$, 以及添加扰动后的样本 x_j^a 所对应的软标记 $\hat{y}_j^a$. 在实际任务中, 为了能够使目标域中样本对应的预测结果更具有区分度, 本文使用了锐化预测 (sharpening predictions) 技术对样本的软标记进行锐化处理, 锐化后的软标签 $\hat{y}_j^{t(\text{sharp})}$ 可通过下式计算得到:

$$\hat{y}_j^{t(\text{sharp})} = \frac{\exp(v_a/\tau)}{\sum_{b=1}^{k}\exp(v_b/\tau)} \tag{9}$$

其中, k 表示任务对应的类别数目. τ 为锐化参数, 其值越小, 则锐化结果 $\hat{y}_j^{t(\text{sharp})}$ 越集中. 本文设置 $\tau = 0.4$. v 表示深度神经网络的输出结果, 其中, v_a 和 v_b 分别是向量 v 中的第 a 个和第 b 个分量的值. 设 $\hat{Y}^{t(\text{sharp})} = \left\{\hat{y}_j^{t(\text{sharp})}\right\}_{j=1}^{n_t}$ 和 $\hat{Y}^a = \left\{\hat{y}_j^a\right\}_{j=1}^{n_t}$ 分别表示经过锐化处理后的目标域样本软标记和扩增后样本的软标记, 则一致性正则化损失 L_t 可通过下式计算:

$$L_t = L_t\left(\hat{Y}^{t(\text{sharp})}, \hat{Y}^a\right) = -\frac{1}{|B|}\sum_{j=1}^{B} I\left(\max\left(\hat{y}_j^t\right) > \beta\right)\hat{y}_j^{t(\text{sharp})}\log\left(\hat{y}_j^a\right) \tag{10}$$

其中, $I(\cdot)$ 为指示函数, 结合第 2.2 节中的伪标记技术, 仅选择高置信度的样本所对应的软标记参与计算. B 代表参与一致性正则化损失计算的目标域样本数目. 在实际任务中, 本文采用了随机数据扩增 (random augment) 的方式对目标域中的样本添加扰动. 值得注意的是, 虽然本文采用了随机数据扩增的方式对图像样本进行了扩增, 然而, 在实际场景下, 可以采用其他样本扩增方式. 例如: 在小样本学习任务中, 可以采用生成对抗网络等其他样本生成技术根据源域与目标域域间的差异生成相应的样本等.

2.4 基于扩增技术的无监督域适应方法

在无监督域适应任务中, 源域和目标域分别包含了标记样本和无标记样本, 且源域和目标域中的数据分布不同. 无监督域适应工作是通过减少源域样本和目标域样本的分布差异, 将源域上预训练的分类器迁移到目标域中, 提高分类器在目标域上的性能, 获得较高的准确率. 在现有无监督域适应工作的基础上, 本文将两种半监督技术引入到域适应方法中, 即通过伪标注的方式进行标注扩增和通过一致性正则化的方式进行样本扩增. 利用扩增后的样本和标注信息拉近源域和目标域之间的距离, 即减少两者之间的损失差异, 获得更快更好的分类训练效果. 优点是不需要在现有深度神经网络的结构中补充任何模块, 简单明确地反映了目标域上分类的损失. 所提出的无监督域适应方法的过程简要概括如下.

(1) 在源域上, 利用标记样本训练分类器, 利用这一分类器对目标域中的未标注样本进行预测;

(2) 在目标域上, 使用伪标记和一致性正则化方式对样本及其标记进行扩增, 并使用扩增后的标记样本对网络进行训练. 在这个过程中, 选择高置信度的样本及其标记参与目标域上损失计算;

(3) 在目标域上, 保留原有的基于 MK-MMD 的无监督域适应损失, 用于衡量源域和目标域上样本之间的分布差异;

(4) 使用上述 (1)–(3) 作为所提出方法的损失项, 用于训练分类器.

基于数据扩增的无监督域适应方法的流程见算法 1.

算法 1. 基于扩增技术的无监督域适应方法 (A-UDA).

输入: 源域中标记样本 $D_s=\{(x_i^s,y_i^s)\}_{i=1}^{n_s}$, 目标域中无标记数据 $D_t=\left\{x_j^t\right\}_{j=1}^{n_t}$, 迭代步骤 i, 总迭代次数 T, 阈值为 β 和 τ, 权重因子 λ_t 和 λ_d;

输出: 分类器 f_θ.

1. 在源域上对分类器进行预训练
2. **For** $i=0:T$
3. 通过源域数据 D_s 训练分类器 f_θ, 利用公式 (7) 计算源域损失 L_s
4. 对目标域数据 D_t 应用数据扩增, 得到其扩增数据 $D_a=\left\{x_j^a\right\}_{j=1}^{n_t}$
5. 使用分类器 f_θ 对目标域数据 D_t 和扩增数据 D_a 进行预测, 得到 $\hat{Y}^t$ 与 $\hat{Y}^a$
6. 利用公式 (8) 选择具有高置信度的伪标签以及对应目标域样本训练分类器 f_θ
7. 利用公式 (9) 对目标域数据未经过 Softmax 的网络输出进行锐化操作得到 $\hat{Y}^{t(\text{sharp})}$
8. 根据公式 (4) 和公式 (10) 分别计算损失 L_d 和 L_t, 得到总损失 L_{total}
9. 使用损失 L_{total} 对分类器 f_θ 进行训练
10. **End**
11. 输出分类器 f_θ

A-UDA 方法的性能取决于是否能够生成具有较高置信度的、有效的目标域扩增样本. 针对不同的任务场景, 可以采用不同的样本扩增技术, 生成更加准确的、鲁棒的目标域样本, 用于提高一致性正则化损失的计算准确性. A-UDA 方法可以根据这些目标域中的样本及其扩增样本计算一致性正则化损失, 分类器的性能并不受到影响.

这里, MMD 损失用于计算源域与目标域之间样本分布的差异大小, 其损失计算项中未使用标记信息, 仅仅是单一计算特征分布之间的距离, 并通过最小化此距离获得分类器性能的提升. 与 MMD 损失不同, 一致性正则化损失项则描述了目标域中扩增样本及伪标记的损失大小对分类器的影响程度. 由于伪标记是分类器对目标域中的样本或者扩增样本进行添加得到的, 因此, 利用了分类器在源域中的知识来增加目标域中的训练样本及标记, 提升域适应任务中分类器的泛化性能. 这里, 一致性正则化技术通过对目标域中数据添加扰动的方式, 增加了能够使分类器更加具有鲁棒性的扩增样本. 继而, 通过最小化这部分样本与其他目标域中样本间的损失, 获得分类性能更加稳定的训练模型. 基于伪标记技术的标注扩增则为目标域中的扩增样本和原始样本增加了高置信度的伪标签, 其目的是充分利用源域上所学习分类器对目标域中每个样本的置信度来提升分类器的学习效果, 并仅选择置信度较高的目标域中的样本及其标记参与损失计算. 这些扩增样本和伪标记直接用于计算一致性正则化损失项, 旨在充分利用分类器的知识逐步提升目标域上分类器的性能.

3 实验结果与分析

本节首先在常用的数字和视觉对象两个分类任务上与常用基线方法进行比较, 之后, 基于消融实验验证 A-UDA 方法中各损失的有效性. 用于数字分类任务的数据集有 MNIST[57]、USPS[58]、SVHN[59], 而对于视觉对象分类数据集, 选择 Office-Home[60]、ImageCLEF-DA 进行域适应任务实验. 本文使用 PyTorch 框架进行实现, 训练数据仅使用有标记源域数据和无标记目标域数据, 源域和目标域具有不同的特征分布. 针对所有任务采取在线数据增强的方式, 优点在于训练时可以在不同的周期针对同一样本产生不同的增强示例. 一边训练一边对样本进行数据扩增, 极大节省数据存储空间, 获得更加接近真实数据的扩增结果.

数据扩增部分采用 Python 图像库 (Python image library, PIL) 中的所有图像处理变换作为基础, 包括: Invert,

Cutout, Sharpness, AutoContrast, Posterize, ShearX, TranslateX, TranslateY, ShearY, Rotate, Equalize, Contrast, Color, Solarize, Brightness 等变换方法. 每次增强过程从其中抽取两两组合为一个增强策略并进行随机采样, 幅度范围 [1, 10], 范围越大表示图像变换程度越大, 随机抽样概率为 0.5. 每个子策略包括图像变换名称、概率和强度这 3 个参数, 用于对目标域中的样本进行扩增.

本文采用模型在测试数据集 (即目标域无标注数据) 上准确率 (*Accuracy*) 作为评价指标, 准确率计算如下式:

$$Accuracy = \frac{\sum_{j=1}^{m} I\left(f\left(x_j^t\right) == y_j^t\right)}{m} \tag{11}$$

其中, $f\left(x_j^t\right)$ 表示训练后的模型对目标域样本 x_j^t 的预测标记, y_j^t 为样本 x_j^t 的真实标记, $I(\cdot)$ 为指示函数. 当 $f\left(x_j^t\right)$ 与 y_j^t 相同, 取值为 1, 否则为 0.

在所有实验中, 我们将所提方法 A-UDA 与基于分布差异的方法 (包括 DDC[10]、DAN[9]、D-CORAL[15]和 JAN[26])、基于对抗的方法 (包括 DANN[3]、ADDA[44]、CoGAN[45]、MCD[61]以及 MADA[24]等) 以及基于重构编码进行域适应的研究工作 (包括 DSN[41]和 DRCN[46]) 进行比较, 可以确定 A-UDA 在实践中的有效性. 其中, 我们将 A-UDA 方法与 DDC[10]和 DAN[9]方法相比较, 这两种方法都是利用数据映射到可再生核希尔伯特空间来减小边界分布间的差异, 或增加域间混淆程度的方法. D-CORAL[15]则是在深度网络中添加 CORAL 度量准则. JAN[26]方法针对域的特定层, 提出 JMMD 准则用于对齐联合分布.

同时, 我们还与基于对抗的研究工作进行了对比, DANN[3]在神经网络的训练中引入对抗性机制. ADDA[44]首先固定源域的相关映射, 随后通过使损失函数的值最小达到目标域与源域距离最小的目的. 这两种模型都是经典的基于对抗的方法. CoGAN[45]通过共享底层网络的权重参数, 间接利用对抗训练实现域适应任务. MCD[61]利用两个分类器和两个特征提取器进行对抗学习. MADA[24]在多个域识别器的基础上, 实现了不同数据分布的数据域的细粒度对齐.

此外, 本文还将 A-UDA 与基于重构编码的域适应研究工作进行比较, 其中包括 DSN[41]和 DRCN[46]两个模型, 这些方法在先前的工作中已经表现出良好的分类性能. 其中 DSN[41]主要是利用自动编码器重构出源域数据的特征表示. DRCN[46]则采用在域之间重构样本的方法来处理域适应问题.

3.1 手写数字分类任务

3.1.1 数据集介绍

本文依据相关实验设置, 在 3 种无监督域适应任务: MNIST→USPS, USPS→MNITS 和 SVHN→MNIST 上对所提出方法及各种基线方法进行实验验证. 其中, 所使用数据集信息如表 1 所示.

表 1 数据集信息

数据集	训练集样本数量	测试集样本数量	类别数量	图像尺寸大小
MNIST	60 000	10 000	10	28×28
USPS	7 291	2 007	10	16×16
SVHN	73 257	26 032	10	32×32

MNIST[57]数据集: MNIST 数据集来自美国国家标准与技术研究所, 由 250 个人的手写数字组成, 数据集共有 70 000 张图片, 包含“0”–“9”这 10 类数字, 其中训练集包含 60 000 张图像, 测试集包含 10 000 张图像, 每张图片的大小为 28×28 维灰度图像.

USPS[58]数据集: 美国国家邮政局 USPS 手写数字库包括“0”–“9”这 10 类数字, 数据集共有 9 298 张图片, 其中训练集包含 7 291 张图像, 测试集包含 2 007 张图像, 每张图片的大小为 16×16 维灰度图像.

SVHN[59]数据集: SVHN 数据集是通过裁剪谷歌街景图片中的门牌号来获得的数字数据集, 数字颜色以及数字背景更具有多样性. 该数据集共有 99 289 张图像. 训练集包含 73 257 张图像, 测试集包含 26 032 张图像, 每张图片的大小为 32×32.

3.1.2 实验设置

MNIST↔USPS: 在 USPS 和 MNIST 数据集上评估两种域适应场景. MNIST 数据集分为 60 000 张训练图像和 10 000 张测试图像, 而 USPS 数据集包含 7 291 张训练图像和 2 007 张测试图像. 本文分别将 MNIST 和 USPS 作为源域和目标域, 获得两组域适应任务. 在每个域适应任务中, 使用 JDA[62]提供的协议, 分别在 USPS 中随机抽取 1 800 幅图像, MNIST 中随机抽取 2 000 幅图像作为训练集. 这里, 使用通道拷贝将单通道的 MNIST 和 USPS 转变为三通道. 为匹配 MNIST 图像, 将 USPS 图像从 16×16 分辨率放大到 28×28 分辨率, 每张的图片像素都归一化至 [0, 1] 之间.

SVHN→MNIST: SVHN 和 MNIST 数据集分别作为源域和目标域. SVHN 相比于 MNIST 在彩色背景、对比度、旋转、比例等方面有显著的变化. 在这种域适应场景中, 根据 DANN[17,45]使用整个训练集 (标记的 73 257 张 SVHN 图像和未标记的 60 000 张 MNIST 图像) 进行训练, 并对目标域 (MNIST 数据集) 的训练集进行评估. 将 SVHN 重新缩放到 28×28 像素, 并且将 MNIST 灰度通道复制到 3 个 RGB 通道.

本任务中采用 3 层卷积层、两层全连接层的 LeNet 网络. 在进行 MNIST↔USPS 任务中, 因所需的两个数据集训练样本较少, 为防止过拟合, 设置实验在迭代 500 次后停止训练. SVHN→MNIST 任务中设置训练迭代次数为 3 000 次. 使用小批量随机梯度下降 (mini-batch SGD) 训练网络, 学习率设置为 0.1, 动量为 0.05, 权重衰减为 0.003. 批量大小设置为 64.

3.1.3 实验结果与分析

表 2 列出了 A-UDA 方法与其他无监督域适应方法在数字分类数据集上进行对比的结果. 每个实验结果由 5 次随机实验的平均值和标准差组成, 最优的准确率用粗体表示, −表示未报告结果.

表 2 各种方法在数字分类任务上的准确率 (%)

方法	SVHN→MNIST	USPS→MNIST	MNIST→USPS	Avg
Source only	59.3±0.1	48.2±5.9	74.7±0.1	60.7
DANN[3]	71.1	73.0	77.1	73.7
DSN[41]	82.7	−	91.3	87.0
ADDA[44]	76.0±1.8	90.1±0.8	89.4±0.2	85.2
CoGAN[45]	−	89.1	91.2	90.2
DRCN[46]	91.0±0.2	73.4±0.0	91.8±0.1	85.4
MCD[61]	96.2±0.4	94.1±0.3	94.2±0.7	94.8
A-UDA	**97.6±0.1**	**96.5±0.6**	**94.6±0.7**	**96.2**

实验结果表明, 本文所提方法在 3 种数字分类域适应任务中均取得了最好的性能. Source only 表示仅在源域数据上进行训练, 然后直接在目标域数据上进行测试的结果. 如表 2 所示, 在 SVHN→MNIST、USPS→MNIST 和 MNIST→USPS 任务上相比于其他基线的最佳准确率分别提高了 1.4%, 2.4% 和 0.4%. SVHN→MNIST 任务的准确率在 3 个域适应任务中相比于所表示的最佳基线提升效果最为明显, 反映了本文模型在更加困难的域适应任务中有着更好的分类效果. 具体来说, A-UDA 与 DRCN 方法相比, 平均精度提升了 10.8%, MCD 通过训练两个分类器来减少源域和目标域之间的距离. 与 MCD 方法进行比较, 其平均精度升了 1.4%. 由此可以看出, 利用目标领域的分类信息来指导无监督域适应的学习是尤为重要的, 正确的伪标签信息可以起到显著的正向促进模型预测准确的效果. 当源域分类器预测更为准确时, 目标域中无标记样本的正确预测标签概率更大, 反馈到网络中使得模型在训练过程中不断进行优化. 本文所提出的算法在匹配特征分布的基础之上, 引入伪标签策略, 并结合一致性正则化技术, 从而进一步改善域适应模型性能, 验证了 A-UDA 方法在无监督域适应场景下有效性.

此外, 为观察特征分类情况. 在图 5 中, 使用 t-SNE[63]将 A-UDA 与 MCD 两个方法在 MNIST→USPS、SVHN→MNIST 任务上的结果在二维空间进行展示, 将所学习的特征可视化. 这里, 红色和蓝色的点分别表示源域样本和目标域样本的特征, 不同的簇代表不同的分类类别. Before adaptation 表示不进行域适应而直接将源域训练的模型用于目标域, 所学习到的特征可视化的结果. Adapted 表示使用域适应方法对目标域特征进行可视化得到的

结果. 特征聚类效果越好, 表明模型具有更好的域适应性能.

借助 t-SNE 图可以看出: 不使用 A-UDA 方法, MNIST→USPS 与 SVHN→MNIST 任务的源域与目标域的类别决策边界较为模糊, 不同类别之间的距离较小; 使用 A-UDA 方法, 属于同一类别的目标域数据更为集中, 不同类别的数据之间的间距增大, 从而, 便于对目标域的数据进行分类. 将 A-UDA 和 MCD 算法的可视化特征效果进行比较, 结果表明, A-UDA 能够使得源域与目标域的特征分布呈现出较为明显的聚类的特点, 目标域与源域的数据分布更为接近, 表现出较好的域适应能力.

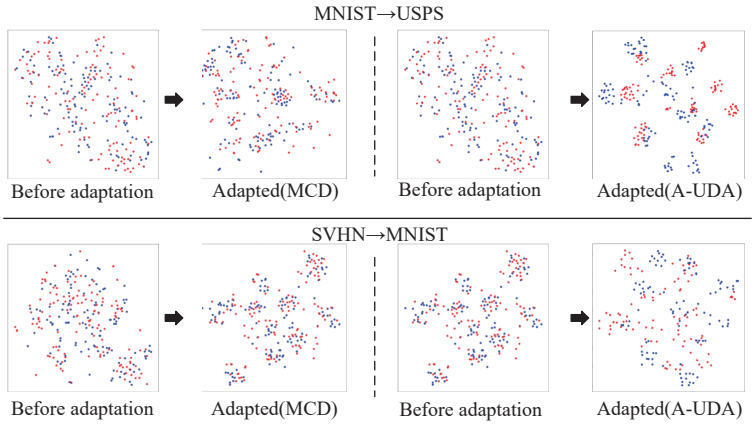


图 5 不同域适应场景下的 t-SNE 可视化结果

3.2 视觉对象分类

3.2.1 数据集介绍

本节采用 ImageCLEF-DA 和 Office-Home 两个常用于域适应任务的数据集对所提出方法的有效性进行验证, 目的是说明所提出方法在视觉对象分类任务上的有效性. 这里, 所使用数据集的信息如表 3 所示.

表 3 视觉对象分类数据集信息

数据集	样本数量	任务数量	类别数量
ImageCLEF-DA	1 800	6	12
Office-Home	15 500	12	65

ImageCLEF-DA 数据集: ImageCLEF-DA 数据集是 ImageCLEF-DA 2014 领域自适应挑战赛的基准数据集, 包括 3 个领域: Caltech-256 (C)、ImageNet ILSVRC 2012 (I) 和 Pascal VOC 2012 (P). 每个域有 12 个类别, 每个类别包含 50 幅图像, 每个域共有 600 幅图像. 实验过程中, 本文使用所有的域组合共计 6 个迁移任务: I→P, P→I, I→C, C→I, C→P, P→C.

Office-Home 数据集: Office-Home 数据集是领域自适应的基准数据集, 包含 4 个不同的领域: Artistic (A)、Clipart (C)、Product (P) 和 Real-World (R). 其中每个域由 65 个日常用品类别组成, 共有 15 500 幅图像. 本文使用将所有的域组合成为 12 个域适应任务.

3.2.2 实验设置

对于 ImageCLEF-DA 数据集和 Office-Home 数据集, 本文使用 ImageNet 图像库上预训练的 ResNet-50[64]模型提取图像特征, 修改 ResNet-50 网络的最后一层全连接层的输出数量, 用于适应不同类别数量的分类任务. 在训练中, 使用动量为 0.9 的小批量随机梯度下降 (mini-batch SGD) 更新模型参数, 采用与 DANN[3]中的所提到的学习率调整策略来训练网络, 学习率调整方式如下:

$$\eta = \frac{\eta_0}{\left(1+\gamma\frac{i}{T}\right)^{\beta}} \tag{12}$$

其中, 初始学习率 η_0 为 0.01, 参数 γ=10, β=0.75. 其中, $\frac{i}{T}$ 表示随着训练进程从 0 线性增加到 1, i 表示当前周期, T 表示总训练周期, 批量大小设置为 16, 训练周期为 40.

3.2.3 实验结果与分析

对于 ImageCLEF-DA 数据集, 将 A-UDA 与 ResNet[64], DDC[10], DAN[9], DANN[3], D-CORAL[15], JAN[26], MADA[24], CAN[25], SPCAN[25]进行比较. 对于 Office-Home 数据集, 将 A-UDA 与 ResNet[64], DAN[9], DANN[3], CDAN[17]和 SPCAN[17]进行比较. 本文每个实验重复 5 次, 并报告了 Office-Home 数据集上准确率的平均值以及 ImageCLEF-DA 数据集上准确率的平均值和标准差. 这里, ImageCLEF-DA 数据集和 Office-Home 的实验结果分别列于表 4 和表 5.

表 4 ImageCLEF-DA 数据集上的分类准确率 (%)

方法	I→P	P→I	I→C	C→I	C→P	P→C	Avg
ResNet[64]	74.8±0.3	83.9±0.1	91.50.3	78.0±0.2	65.5±0.3	91.2±0.3	80.7
DDC[10]	74.6±0.3	85.7±0.8	91.10.3	82.3±0.7	68.3±0.4	88.8±0.2	81.8
DAN[9]	75.0±0.4	86.2±0.2	93.3±0.2	84.1±0.4	69.8±0.4	91.3±0.4	83.3
DANN[3]	75.0±0.6	86.0±0.3	96.2±0.4	87.0±0.5	74.3±0.5	91.5±0.6	85.0
D-CORAL[15]	76.9±0.2	88.5±0.3	93.6±0.3	86.8±0.6	74.0±0.3	91.6±0.3	85.2
JAN[26]	76.8±0.4	88.0±0.2	94.7±0.2	89.5±0.3	74.2±0.3	91.7±0.3	85.8
MADA[24]	75.0±0.3	87.9±0.2	96.0±0.3	88.8±0.3	75.2±0.2	92.2±0.3	85.8
CAN[25]	78.2	87.5	94.2	89.5	75.8	89.2	85.7
SPCAN[25]	79.5	89.7	94.7	89.9	78.5	92.0	87.4
CDAN[17]	76.7±0.3	90.6±0.3	97.0±0.4	90.5±0.4	74.5±0.3	93.5±0.4	87.1
CDAN+E[17]	**77.7±0.3**	90.7±0.2	**97.7±0.3**	91.3±0.3	74.2±0.2	94.3±0.3	87.7
A-UDA	77.0±0.5	**92.7±0.5**	96.0±0.2	**91.9±0.2**	**76.4±0.9**	**95.1±0.3**	**88.2**

表 5 Office-Home 数据集上的分类准确率 (%)

方法	A→C	A→P	A→R	C→A	C→P	C→R	P→A	P→C	P→R	R→A	R→C	R→P	Avg
ResNet[64]	34.9	50.0	58.0	37.4	41.9	46.2	38.5	31.2	60.4	53.9	41.2	59.9	46.1
DAN[9]	43.6	57.0	67.9	45.8	56.5	60.4	44.0	43.6	67.7	63.1	51.5	74.3	56.3
DANN[3]	45.6	59.3	70.1	47.0	58.5	60.9	46.1	43.7	68.5	63.2	51.8	76.8	57.6
JAN[26]	45.9	61.2	68.9	50.4	59.7	61.0	45.8	43.4	70.3	63.9	52.4	76.8	58.3
CDAN[17]	49.0	69.3	74.5	54.4	66.0	68.4	55.6	48.3	75.9	68.4	55.4	80.5	63.8
CDAN+E[17]	50.7	**70.6**	76.0	57.6	70.0	70.0	57.4	50.9	77.3	70.9	56.7	81.6	65.8
A-UDA	**55.4**	70.1	**76.8**	**62.6**	**71.2**	**70.7**	**61.5**	**56.4**	**78.2**	**72.7**	**61.7**	**83.3**	**68.4**

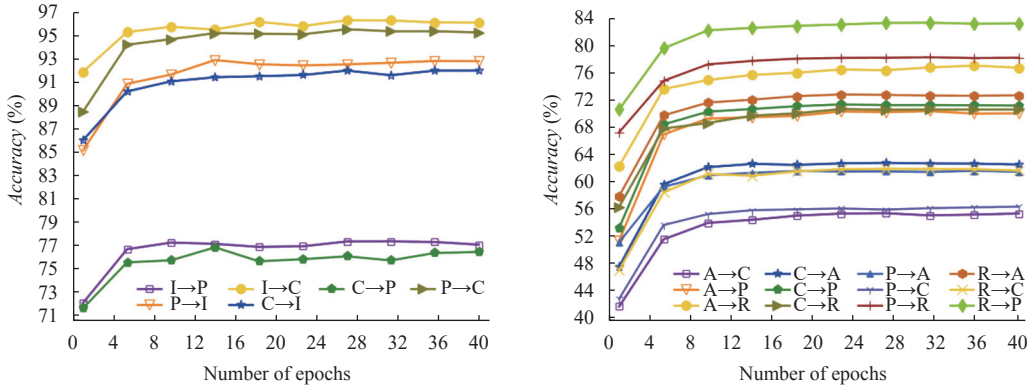
表 4 和表 5 展示了所提出的模型与基线方法在源域→目标域中各个域适应任务上的平均准确率. 在每个表格中, 粗体和下划线分别表示每个任务的最佳和次佳的结果. 从 ImageCLEF-DA 数据集上 6 组域适应任务的实验结果可以看出, 本文所提出的 A-UDA 算法的效果优于所有对比的算法. 与其他模型进行比较, A-UDA 在 ImageCLEF-DA 数据集的其中 4 个任务中获得最好的性能, 平均准确率为 88.2%, 相比于 SPCAN 算法, 平均准确率提高了 0.8%, 相比于 CDAN+E 算法, 平均准确率提高了 0.5%. 这说明本文提出的算法可以在场景较为丰富的领域达到较好的分类效果.

从实验结果可以看出, 相比较于现有的算法, 本文所提出的 A-UDA 算法在 Office-Home 数据集的 12 个域适应任务中的其中 11 个任务上获得了最佳性能. 从均值上看, 在 Office-Home 数据集这个具有挑战性的数据集上对应于算法 DAN, DANN, JAN, CDAN, CDAN+E, 分类精度分别提升了 12.1%, 10.8%, 10.1%, 4.6%, 2.6%, 平均准确率为 68.4%, 与最佳对比算法 CDAN+E 相比提高 2.6%. 说明本文方法对于域适应任务有明显的提升作用. 一些基

于度量的算法, 例如 DAN 和 JAN, 通过最小化源域与目标域之间的距离获得域共享特征, 进而实现域适应效果. 但此类方法忽略了目标域数据的分类信息, 本文提出的 A-UDA 算法使用阈值筛选的伪标签技术减少目标域伪标签的分类不确定性, 从而降低使用错误标注的样本在迭代学习过程中所带来的负面影响, 间接实现增加带有正确标注的训练数据的效果, 同时利用一致性正则化技术提高模型的泛化性能.

在表 4 和表 5 中, A-UDA 方法在 ImageCLEF-DA 数据集中 I→P 任务、I→C 任务以及 Office-Home 数据集中 A-P 任务上均稍逊于 CDAN+E 方法取得的最佳结果, 但与最佳结果的准确率较为接近. 其原因是 CDAN+E 方法采用了条件生成对抗网络生成域适应任务中的训练样本, 其样本生成过程考虑了类别信息和样本特征之间的联合分布. 而本文通过添加伪标签的方式为分类器学习添加类别分布信息, 在保证准确率的同时, 显著减少了深度模型迭代训练过程中所需要的时间和空间代价. 另外, 通过 CDAN 方法、CDAN+E 方法和 A-UDA 方法与其他方法的实验结果比较可以看出, 同时考虑类别信息与样本的特征学习无监督域适应任务上的分类器, 可以获得更高的准确率和更好的性能.

为了验证本文算法的稳定性及收敛性, 图 6 给出了 ImageCLEF-DA 以及 Office-Home 数据集上各个域适应任务中目标域分类准确率随迭代周期的变化. 其中, 横轴为迭代周期, 纵轴表示目标域分类准确率. 由折线图可以看出, 随迭代训练过程的推进, 准确率不断上升, 模型快速收敛 (6 个训练周期就基本收敛), 并逐渐趋于稳定, 进一步验证了 A-UDA 方法的有效性以及稳定性.



(a) ImageCLEF-DA (b) Office-Home

图 6 视觉对象分类任务中准确率随迭代次数变化情况

3.3 参数影响分析

为了充分探讨在不同情况下, A-UDA 受不同权重因子 λ_t 和 λ_d 的影响状况, 我们以 MNIST-USPS 任务为例, 当 λ_t=1, λ_d 在范围{0.01, 0.1, 0.2, 0.4, 0.6, 0.8, 1, 2}内, 以及 λ_d = 1, 对 λ_t 在范围{0.01, 0.1, 0.2, 0.4, 0.6, 0.8, 1, 2}内时, 本文对各个任务上的准确率进行了比较. 实验结果如表 6 所示.

表 6 不同 λ 下的分类准确率 (%)

Task (λ)	0.01	0.1	0.2	0.4	0.6	0.8	1	2
MNIST→USPS (λ_t)	85.9	89.5	92.4	93.5	94.3	92.9	94.6	94.4
USPS→MNIST (λ_t)	92.1	94.5	95.1	96.1	95.6	96.1	96.5	95.9
MNIST→USPS (λ_d)	90.9	92.2	93.6	94.7	94.0	93.8	94.6	88.3
USPS→MNIST (λ_d)	77.0	84.1	87.0	91.9	96.3	95.7	96.5	93.4

在表 6 中, 前两行展示了不同参数 λ_t 在 MNIST→USPS 以及 USPS→MNIST 任务上的分类准确率. 后两行则反映了不同参数 λ_d 在 MNIST→USPS 以及 USPS→MNIST 任务上的分类准确率. 由表中可以看出, 对于不同的损失项, 往往其参数调节的范围难以确定, 许多情况下, 过大或者过小的权重都会导致模型的不稳定. 例如, 在

MNIST→USPS 任务中, 当一致性正则化损失项前的权重因子 λ_t 的值为 0.01 时, 模型的分类性能急剧下降, 其准确率为 85.9%. 在相同任务中, 当 MK-MMD 度量损失项前的权重因子 λ_d 的系数为 2 时, 模型的分类性能较低, 其准确率为 88.3%. 但当抛开两个相对极端的系数值时, 我们从中可以观察到, 超参数的值在 0.1–1 的范围内准确性以稳定的方式逐步增长.

由于模型在不同参数下的运行比较稳定, 所以在整个实验过程中选择固定超参数 $\lambda_t = 1$ 和 $\lambda_d = 1$ 来获得最佳性能. 实验证明本文所提出的模型在超参数上具有泛化性, 同样也进一步验证了 A-UDA 算法的鲁棒性.

3.4 消融实验

为了更好地验证 A-UDA 方法中每部分的有效性, 本节在数字分类数据集上设置 4 组对比实验, 使用准确率的平均值和标准差, 对 A-UDA 方法中各个损失项的有效性进行验证. 各个实验的设置如下.

(1) 实验 1. l_s: 源域交叉熵分类损失;

(2) 实验 2. $l_s + l_d$: 源域交叉熵分类损失和 MK-MMD 度量损失;

(3) 实验 3. $l_s + l_t$: 源域交叉熵分类损失, 一致性正则化损失;

(4) 实验 4. $l_s + l_t + l_d$: 源域交叉熵分类损失, 一致性正则化损失和 MK-MMD 度量损失, 即 A-UDA 方法.

各种方法的消融实验对比结果如表 7 所示.

表 7 消融实验的分类准确率 (%)

方法	SVHN→MNIST	USPS→MNIST	MNIST→USPS	Avg
实验1	61.8±1.9	57.2±5.5	71.1±0.4	63.4
实验2	71.4±0.8	89.5±0.1	88.7±0.7	83.2
实验3	88.3±0.5	76.8±9.4	84.8±2.9	83.3
实验4	**97.6±0.1**	**96.5±0.6**	**94.6±0.7**	**96.2**

从表 7 的对比实验结果可以看出, 在 MNIST→USPS 任务中实验 1 准确率达到 71.1%, 说明现有深度学习方法在面对跨域的任务时, 也有一定的效果. 但在更加困难的 SVHN→MNIST 任务中, 准确率为 61.8%, 表明使用传统的机器学习方法, 利用源域数据进行训练, 直接测试目标域数据分类准确率, 在源域和目标域特征分布差异较大的情况下, 分类性能会逐渐降低. 实验 3 比实验 2 的准确率高, 说明在实验 3 的情况下, 通过在目标域数据训练过程中, 加入一致性正则化损失项, 可以使得生成的特征远离决策边界, 从而达到更高的域适应准确率. 在实验 4 中, 即 A-UDA 方法, 将源域交叉熵分类损失、MK-MMD 度量以及一致性正则化损失相结合, 在 SVHN→MNIST, USPS→MNIST 和 MNIST→USPS 任务上分别达到了 97.6%, 96.5% 和 94.6% 的分类准确率. 与单独使用 MK-MMD 度量或一致性正则化损失相比有更加突出的表现, 域适应准确率相较于实验 3 进一步提高, 证明了本文所提出的算法的有效性.

从表 7 的实验可以看出, 当源域交叉熵分类损失不变时, 同时采用一致性正则化项和 MK-MMD 损失项 (实验 4), 分类器的准确率会明显上升. 当单独采用一致性正则化项时 (实验 3), 其分类器的准确率较为稳定, 但稍逊于单独采用 MK-MMD 损失项 (实验 2), 但多个任务上分类器的准确率平均值与其持平. 其原因是一致性正则化项计算并未基于特征分布进行样本扩增, 因此, 单独采用一致性正则化项训练无监督域适应任务上的分类器缺少源域和目标域间特征的分布信息, 而只有类别预测的结果, 导致了性能的下降. 而本文所提出的 A-UDA 方法同时采用一致性正则化项和 MK-MMD 这两个损失项 (实验 4) 学习分类器, 目的是同时利用源域和目标域之间的特征分布和目标域中的类别信息训练分类器, 获得更好的泛化性能.

4 结 论

针对无监督域适应问题, 本文提出了一种基于扩增技术的无监督域适应方法 A-UDA. 在现有无监督域适应方法的基础上, 引入伪标签和一致性正则化两种半监督技术, 目的是有效利用源域标记数据信息和目标域无标记数据信息. 其中, 伪标记技术通过设定阈值选择高置信度的样本添加标记, 降低了目标域中错误标注的概率; 一致性

正则化方法则使扩增后的标注样本与原始样本的输出保持一致, 提高目标域上的分类效果. 在多个无监督域适应任务上对所提出方法进行了比较, 实验结果验证了所提出的方法可以获得更优的适应性能. 尽管 A-UDA 方法在多个域适应数据集中都有不错的表现, 但它仍存在一些提升空间. 在今后的工作中, 将进一步从目标域无标记数据信息的角度思考, 考虑伪标签等因素对模型的影响, 以提升模型的准确率和鲁棒性. 同时将进一步探究不同距离分布度量对域适应结果的影响.

虽然本文所提出方法仅在多个不同的手写数字识别和视觉对象分类任务上进行了验证, 实验结果也说明了 A-UDA 方法在以图像作为输入数据形式的应用任务中可以取得良好的分类效果. 然而, A-UDA 方法不仅仅适用于图像这一数据形式, 也可以应用于文本、生物以及时序等其他非图像数据的分类、识别、回归等任务中. 例如: 本文采用了随机扩增技术来增加目标域中样本的数量, 从而计算一致性正则化损失, 而在文本分类、蛋白质结构预测任务中, 可以采用生成对抗网络、大型语言或蛋白质结构预测模型所生成的目标域样本来完成一致性正则化损失的计算过程. 同样, 对于所添加伪标记的置信度计算, 也可以扩展到此类序列或结构化数据标签的置信度计算过程中, 从而, 完成这些非图像数据上的无监督域适应任务. 本文未来也将进一步完善 A-UDA 方法, 针对这些应用领域中数据的特点. 即通过改进 A-UDA 方法中样本扩增和标记扩增部分, 使其在这些任务中具有更好的性能提升, 在多种场景下均具有良好的扩展性.

References:

[1] Zhuo JB, Su C, Wang SH, Huang QM. Min-entropy transfer adversarial hashing. Journal of Computer Research and Development, 2020, 57(4): 888–896 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2020.20190476]

[2] Ozyurt Y, Feuerriegel S, Zhang C. Contrastive learning for unsupervised domain adaptation of time series. In: Proc. of the 11th Int'l Conf. on Learning Representations. Kigali: OpenReview.net, 2023. 1–40.

[3] Ganin Y, Ustinova E, Ajakan H, Germain P, Larochelle H, Laviolette F, Marchand M, Lempitsky V. Domain-adversarial training of neural networks. The Journal of Machine Learning Research, 2016, 17(1): 2096–2030.

[4] Dinu MC, Holzleitner M, Beck M, Nguyen HD, Huber A, Eghbal-Zadeh H, Moser BA, Pereverzyev SV, Hochreiter S, Zellinger W. Addressing parameter choice issues in unsupervised domain adaptation by aggregation. In: Proc. of the 11th Int'l Conf. on Learning Representations. Kigali: OpenReview.net, 2023. 1–51.

[5] Kim M, Li D, Hospedales T. Domain generalisation via domain adaptation: An adversarial Fourier amplitude approach. In: Proc. of the 11th Int'l Conf. on Learning Representations. Kigali: OpenReview.net, 2023. 1–21.

[6] Saito K, Kim D, Sclaroff S, Darrell T, Saenko K. Semi-supervised domain adaptation via minimax entropy. In: Proc. of the 2019 IEEE Int'l Conf. on Computer Vision. Seoul: IEEE, 2019. 8049–8057. [doi: 10.1109/ICCV.2019.00814]

[7] Jiang P, Wu AM, Han YH, Shao YF, Qi MY, Li BS. Bidirectional adversarial training for semi-supervised domain adaptation. In: Proc. of the 29th Int'l Joint Conf. on Artificial Intelligence. ijcai.org, 2020. 130.

[8] Li D, Hospedales T. Online meta-learning for multi-source and semi-supervised domain adaptation. In: Proc. of the 16th European Conf. on Computer Vision. Glasgow: Springer, 2020. 382–403.

[9] Long MS, Cao Y, Wang JM, Jordan MI. Learning transferable features with deep adaptation networks. In: Proc. of the 32nd Int'l Conf. on Machine Learning. Lille: JMLR.org, 2015. 97–105.

[10] Tzeng E, Hoffman J, Zhang N, Saenko K, Darrell T. Deep domain confusion: Maximizing for domain invariance. arXiv:1412.3474, 2014.

[11] Sohn K, Shang WL, Yu X, Chandraker M. Unsupervised domain adaptation for distance metric learning. In: Proc. of the 7th Int'l Conf. on Learning Representations. New Orleans: OpenReview.net, 2019. 1–18.

[12] Zhang YB, Tang H, Jia K, Tan MK. Domain-symmetric networks for adversarial domain adaptation. In: Proc. of the 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019. 5026–5035. [doi: 10.1109/CVPR.2019.00517]

[13] Li XD, Hu Y, Zheng JH, Li MT, Ma WZ. Central moment discrepancy based domain adaptation for intelligent bearing fault diagnosis. Neurocomputing, 2021, 429: 12–24. [doi: 10.1016/j.neucom.2020.11.063]

[14] Peng XC, Bai QX, Xia XD, Huang ZJ, Saenko K, Wang B. Moment matching for multi-source domain adaptation. In: Proc. of the 2019 IEEE/CVF Int'l Conf. on Computer Vision. Seoul: IEEE, 2019. 1406–1415. [doi: 10.1109/ICCV.2019.00149]

[15] Sun BC, Saenko K. Deep CORAL: Correlation alignment for deep domain adaptation. In: Proc. of the 2016 European Conf. on Computer Vision. Amsterdam: Springer, 2016. 443–450. [doi: 10.1007/978-3-319-49409-8_35]

[16] Peng XC, Saenko K. Synthetic to real adaptation with generative correlation alignment networks. In: Proc. of the 18th IEEE Winter Conf.

on Applications of Computer Vision. Lake Tahoe: IEEE, 2018. 1982–1991. [doi: 10.1109/WACV.2018.00219]

[17] Long MS, Cao ZJ, Wang JM, Jordan MI. Conditional adversarial domain adaptation. In: Proc. of the 32nd Int'l Conf. on Neural Information Processing Systems. Red Hook: Curran Associates Inc., 2018. 1647–1657.

[18] Cui SH, Wang SH, Zhuo JB, Su C, Huang QM, Tian Q. Gradually vanishing bridge for adversarial domain adaptation. In: Proc. of the 2020 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Seattle: IEEE, 2020. 12452–12461.

[19] Wang XM, Li L, Ye WR, Long MS, Wang JM. Transferable attention for domain adaptation. In: Proc. of the 33rd AAAI Conf. on Artificial Intelligence. AAAI Press, 2019. 655. [doi: 10.1609/aaai.v33i01.33015345]

[20] Matsuura T, Harada T. Domain generalization using a mixture of multiple latent domains. In: Proc. of the 34th AAAI Conf. on Artificial Intelligence. New York: AAAI Press, 2020. 11749–11756. [doi: 10.1609/aaai.v34i07.6846]

[21] Wei YY, Zhang Z, Wang Y, Xu ML, Yang Y, Yan SC, Wang M. DerainCycleGAN: Rain attentive CycleGAN for single image deraining and rainmaking. IEEE Trans. on Image Processing, 2021, 30: 4788–4801. [doi: 10.1109/TIP.2021.3074804]

[22] Gao R, Hou XS, Qin J, Chen JX, Liu L, Zhu F, Zhang Z, Shao L. Zero-VAE-GAN: Generating unseen features for generalized and transductive zero-shot learning. IEEE Trans. on Image Processing, 2020, 29: 3665–3680. [doi: 10.1109/TIP.2020.2964429]

[23] Gao XJ, Zhang Z, Mu TT, Zhang XD, Cui CR, Wang M. Self-attention driven adversarial similarity learning network. Pattern Recognition, 2020, 105: 107331. [doi: 10.1016/j.patcog.2020.107331]

[24] Pei ZY, Cao ZJ, Long MS, Wang JM. Multi-adversarial domain adaptation. In: Proc. of the 32nd Conf. on Artificial Intelligence. New Orleans: AAAI Press, 2018. 3934–3941. [doi: 10.1609/aaai.v32i1.11767]

[25] Zhang WC, Xu D, Ouyang WL, Li W. Self-paced collaborative and adversarial network for unsupervised domain adaptation. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2021, 43(6): 2047–2061. [doi: 10.1109/TPAMI.2019.2962476]

[26] Long MS, Zhu H, Wang JM, Jordan MI. Deep transfer learning with joint adaptation networks. In: Proc. of the 34th Int'l Conf. on Machine Learning. Sydney: PMLR, 2017. 2208–2217.

[27] Kang GL, Jiang L, Yang Y, Hauptmann AG. Contrastive adaptation network for unsupervised domain adaptation. In: Proc. of the 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019. 4888–4897. [doi: 10.1109/CVPR.2019.00503]

[28] Chen MH, Zhao S, Liu HF, Cai D. Adversarial-learned loss for domain adaptation. In: Proc. of the 34th Conf. on Artificial Intelligence. New York: AAAI Press, 2020. 3521–3528. [doi: 10.1609/aaai.v34i04.5757]

[29] Saito K, Ushiku Y, Harada T. Asymmetric tri-training for unsupervised domain adaptation. In: Proc. of the 34th Int'l Conf. on Machine Learning. Sydney: JMLR.org, 2017. 2988–2997.

[30] Xie SA, Zheng ZB, Chen L, Chen C. Learning semantic representations for unsupervised domain adaptation. In: Proc. of the 35th Int'l Conf. on Machine Learning. Stockholm: PMLR, 2018. 5419–5428.

[31] Chen CQ, Xie WP, Huang WB, Rong Y, Ding XH, Huang Y, Xu TY, Huang JZ. Progressive feature alignment for unsupervised domain adaptation. In: Proc. of the 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019. 627–636. [doi: 10.1109/CVPR.2019.00072]

[32] Pan YW, Yao T, Li YH, Wang Y, Ngo CW, Mei T. Transferrable prototypical networks for unsupervised domain adaptation. In: Proc. of the 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019. 2234–2242. [doi: 10.1109/CVPR.2019.00234]

[33] Zou Y, Yu ZD, Kumar BVK, Wang JS. Unsupervised domain adaptation for semantic segmentation via class-balanced self-training. In: Proc. of the 15th European Conf. on Computer Vision. Munich: Springer, 2018. 297–313. [doi: 10.1007/978-3-030-01219-9_18]

[34] Wang Q, Breckon T. Unsupervised domain adaptation via structured prediction based selective pseudo-labeling. In: Proc. of the 34th Conf. on Artificial Intelligence. New York: AAAI Press, 2020. 6243–6250. [doi: 10.1609/aaai.v34i04.6091]

[35] Patel VM, Gopalan R, Li RN, Chellappa R. Visual domain adaptation: A survey of recent advances. IEEE Signal Processing Magazine, 2015, 32(3): 53–69. [doi: 10.1109/MSP.2014.2347059]

[36] Rahman MM, Fookes C, Baktashmotlagh M, Sridharan S. On minimum discrepancy estimation for deep domain adaptation. In: Singh R, Vatsa M, Patel V, Ratha N, eds. Domain Adaptation for Visual Understanding. Cham: Springer, 2020. 81–94. [doi: 10.1007/978-3-030-30671-7_6]

[37] Morerio P, Cavazza J, Murino V. Minimal-entropy correlation alignment for unsupervised deep domain adaptation. In: Proc. of the 6th Int'l Conf. on Learning Representations. Vancouver: OpenReview.net, 2018.

[38] Zhuang FZ, Cheng XH, Luo P, Pan SJ, He Q. Supervised representation learning: Transfer learning with deep autoencoders. In: Proc. of the 24th Int'l Joint Conf. on Artificial Intelligence. Buenos: AAAI Press, 2015. 4119–4125.

[39] Zhang Y, Wang NB, Cai SB, Song L. Unsupervised domain adaptation by mapped correlation alignment. IEEE Access, 2018, 6: 44698–44706. [doi: 10.1109/access.2018.2865249]

[40] Zhang Z, Wang MZ, Huang Y, Nehorai A. Aligning infinite-dimensional covariance matrices in reproducing kernel Hilbert spaces for domain adaptation. In: Proc. of the 2018 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Salt Lake City: IEEE, 2018. 3437–3445. [doi: 10.1109/CVPR.2018.00362]

[41] Bousmalis K, Trigeorgis G, Silberman N, Krishnan D, Erhan D. Domain separation networks. In: Proc. of the 30th Int'l Conf. on Neural Information Processing Systems. Barcelona: Curran Associates Inc., 2016. 343–351.

[42] Cicek S, Soatto S. Unsupervised domain adaptation via regularized conditional alignment. In: Proc. of the 2019 IEEE/CVF Int'l Conf. on Computer Vision. Seoul: IEEE, 2019. 1416–1425. [doi: 10.1109/ICCV.2019.00150]

[43] Vu TH, Jain H, Bucher M, Cord M, Pérez P. ADVENT: Adversarial entropy minimization for domain adaptation in semantic segmentation. In: Proc. of the 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019. 2512–2521. [doi: 10.1109/CVPR.2019.00262]

[44] Tzeng E, Hoffman J, Saenko K, Darrell T. Adversarial discriminative domain adaptation. In: Proc. of the 2017 IEEE Conf. on Computer Vision and Pattern Recognition. Honolulu: IEEE, 2017. 2962–2971. [doi: 10.1109/CVPR.2017.316]

[45] Liu MY, Tuzel O. Coupled generative adversarial networks. In: Proc. of the 30th Int'l Conf. on Neural Information Processing Systems. Barcelona: Curran Associates Inc., 2016. 469–477.

[46] Ghifary M, Kleijn WB, Zhang MJ, Balduzzi D, Li W. Deep reconstruction-classification networks for unsupervised domain adaptation. In: Proc. of the 14th European Conf. on Computer Vision. Amsterdam: Springer, 2016. 597–613. [doi: 10.1007/978-3-319-46493-0_36]

[47] Zhang Y, Chen RR, Zhang J. Safe Tri-training algorithm based on cross entropy. Journal of Computer Research and Development, 2021, 58(1): 60–69 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2021.20190838]

[48] Bošnjak M, Richemond PH, Tomasev N, Strub F, Walker JC, Hill F, Buesing LH, Pascanu R, Blundell C, Mitrovic J. SemPPL: Predicting pseudo-labels for better contrastive representations. In: Proc. of the 11th Int'l Conf. on Learning Representations. Kigali: OpenReview.net, 2023.

[49] Shi WW, Gong YH, Ding C, Ma ZH, Tao XY, Zheng NN. Transductive semi-supervised deep learning using min-max features. In: Ferrari V, Hebert M, eds. Proc. of the 15th European Conf. on Computer Vision. Munich: Springer, 2018. 311–327. [doi: 10.1007/978-3-030-01228-1_19]

[50] Rizve MN, Duarte K, Rawat YS, Shah M. In defense of pseudo-labeling: An uncertainty-aware pseudo-label selection framework for semi-supervised learning. In: Proc. of the 2021 Int'l Conf. on Learning Representations. Vienna: OpenReview.net, 2021. 1–20.

[51] Laine S, Aila T. Temporal ensembling for semi-supervised learning. In: Proc. of the 5th Int'l Conf. on Learning Representations. Toulon: OpenReview.net, 2016.

[52] Cubuk ED, Zoph B, Mané D, Vasudevan V, Le QV. AutoAugment: Learning augmentation strategies from data. In: Proc. of the 2019 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Long Beach: IEEE, 2019. 113–123. [doi: 10.1109/CVPR.2019.00020]

[53] Xie QZ, Dai ZH, Hovy E, Luong MT, Le QV. Unsupervised data augmentation for consistency training. In: Proc. of the 34th Int'l Conf. on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2020. 525.

[54] Berthelot D, Carlini N, Goodfellow I, Oliver A, Papernot N, Raffel CA. MixMatch: A holistic approach to semi-supervised learning. In: Proc. of the 33rd Int'l Conf. on Neural Information Processing Systems. Vancouver: Curran Associates Inc., 2019. 454.

[55] Miyato T, Maeda SI, Koyama M, Ishii S. Virtual adversarial training: A regularization method for supervised and semi-supervised learning. IEEE Trans. on Pattern Analysis and Machine Intelligence, 2019, 41(8): 1979–1993. [doi: 10.1109/TPAMI.2018.2858821]

[56] Tarvainen A, Valpola H. Mean teachers are better role models: Weight-averaged consistency targets improve semi-supervised deep learning results. In: Proc. of the 31st Int'l Conf. on Neural Information Processing Systems. Long Beach: Curran Associates Inc., 2017. 1195–1204.

[57] LeCun Y, Bottou L, Bengio Y, Haffner P. Gradient-based learning applied to document recognition. Proc. of the IEEE, 1998, 86(11): 2278–2324. [doi: 10.1109/5.726791]

[58] Hull JJ. A database for handwritten text recognition research. IEEE Trans. on Pattern Analysis and Machine Intelligence, 1994, 16(5): 550–554. [doi: 10.1109/34.291440]

[59] Netzer Y, Wang T, Coates A, Bissacco A, Wu B, Ng AY. Reading digits in natural images with unsupervised feature learning. In: Proc. of the 2011 NIPS Workshop on Deep Learning and Unsupervised Feature Learning. Granada: NIPS, 2011. 5–13.

[60] Venkateswara H, Eusebio J, Chakraborty S, Panchanathan S. Deep hashing network for unsupervised domain adaptation. In: Proc. of the 2017 IEEE Conf. on Computer Vision and Pattern Recognition. Honolulu: IEEE, 2017. 5385–5394. [doi: 10.1109/CVPR.2017.572]

[61] Saito K, Watanabe K, Ushiku Y, Harada T. Maximum classifier discrepancy for unsupervised domain adaptation. In: Proc. of the 2018 IEEE/CVF Conf. on Computer Vision and Pattern Recognition. Salt Lake City: IEEE, 2018. 3723–3732. [doi: 10.1109/CVPR.2018.00392]

[62] Long MS, Wang JM, Ding GG, Sun JG, Yu PS. Transfer feature learning with joint distribution adaptation. In: Proc. of the 2013 IEEE Int'l Conf. on Computer Vision. Sydney: IEEE, 2013. 2200–2207. [doi: 10.1109/ICCV.2013.274]

[63] van der Maaten L, Hinton G. Visualizing data using t-SNE. Journal of Machine Learning Research, 2008, 9(86): 2579–2605.

[64] He KM, Zhang XY, Ren SQ, Sun J. Deep residual learning for image recognition. In: Proc. of the 2016 IEEE Conf. on Computer Vision and Pattern Recognition. Las Vegas: IEEE, 2016. 770–778. [doi: 10.1109/CVPR.2016.90]

附中文参考文献:

[1] 卓君宝, 苏驰, 王树徽, 黄庆明. 最小熵迁移对抗散列方法. 计算机研究与发展, 2020, 57(4): 888–896. [doi: 10.7544/issn1000-1239.2020.20190476]

[47] 张永, 陈蓉蓉, 张晶. 基于交叉熵的安全 Tri-training 算法. 计算机研究与发展, 2021, 58(1): 60–69. [doi: 10.7544/issn1000-1239.2021.20190838]

曹艺(1999－), 女, 硕士生, 主要研究领域为机器学习与数据挖掘, 视觉计算.

吴伟宁(1983－), 女, 博士, 副教授, 博士生导师, CCF 专业会员, 主要研究领域为机器学习与数据挖掘, 医学影像与生物计算.

郭茂祖(1966－), 男, 博士, 教授, 博士生导师, CCF 杰出会员, 主要研究领域为机器学习与数据挖掘, 智能建造与智慧城市, 生物信息学与计算生物学.