ReLSL:基于可靠标签选择与学习的半监督学习算法

魏 翔 王靖杰 张顺利 张 迪 张 健 魏小涛
(北京交通大学软件学院 北京 100044)

摘 要 深度神经网络在众多视觉表征领域取得了显著的成功,如目标检测、识别等.然而,需要大量良好标记的数据进行训练是它们最普遍的限制之一.在实际应用中,为每一个要学习的新任务建立庞大的标记数据集是极其昂贵,甚至是不可行的.半监督深度学习,通过在有限标记数据的条件下充分挖掘大量的未标记数据信息,从而达到与监督学习相媲美的分类精度.然而,当标记数据极其稀少时,现有半监督算法的性能会受到严重影响.因此,本文提出了一种可靠标签选择与学习(Reliable Label Selection and Learning,ReLSL)算法,以解决在仅有极少量标签图像数据时半监督深度学习所面临的问题.具体地,本文首先运用无监督学习方法提取样本特征,并应用基于图的标签传染算法得到无标签样本的伪标签.而后,为了筛选出更为可靠、有更多信息的样本,本文提出了一种综合考虑样本输出均值和一致性的伪标签学习与标定策略.在获得具有扩展标签的数据集后,考虑到训练样本中引入一定比例的标签噪声无可避免,因此本文提出两种策略来训练高鲁棒半监督深度模型:标签平滑策略(Label Smoothing Strategy,LS),用以避免标签过于尖锐;均值偏移校正策略(Mean Shifting Correction Strategy,MSC),用以降低样本输出偏移风险.实验结果表明,在 CNN-13、WRN-28-2 及 ResNet-18 各种网络结构下,本文所提出的 ReLSL 算法在 CIFAR-10/100、SVHN、STL-10 和 Mini-ImageNet 数据集上均表现出先进的性能.特别地,本文算法在 WRN-28-2 网络结构下仅有 10 个标记数据的 CIFAR-10 上,相较于最新算法具有 6.78%的准确率提升;在 CNN-13 网络下仅有 100 个标记数据时,可以达到目前主流半监督学习算法 4000 标记时的测试误差 6.39±0.47%.

关键词 半监督深度学习;极少标签;鲁棒性;标签传播;特征提取
中图法分类号 TP391 **DOI 号** 10.11897/SP.J.1016.2022.01147

ReLSL: Reliable Label Selection and Learning Based Algorithm for Semi-Supervised Learning

WEI Xiang WANG Jing-Jie ZHANG Shun-Li ZHANG Di ZHANG Jian WEI Xiao-Tao
(*School of Software Engineering, Beijing Jiaotong University, Beijing* 100044)

Abstract Deep neural networks have achieved remarkable success in many visual representation fields, such as object detection, recognition, etc. However, requiring the large quantity of well labeled data for training is one of their most prevalent limitations. Many real-world classification applications are concerned with samples that are not presented in standard benchmark datasets, and building large labeled dataset for each new task to be learned is not practically feasible. Although enormous quantities of unlabeled data are accessible and can be collected with minimal effort, the data labeling process is still extremely expensive. Semi-supervised learning (SSL) provides a way to improve a model's performance with the surplus of unlabeled data when only limited labeled data are available. However, when the labeled data is extremely scarce, the performance of the existing SSL algorithms can be severely affected. For example, on the prevalent

收稿日期:2021-03-02;在线发布日期:2021-09-16.本课题得到国家自然科学基金(61906014,61976017,61902019)、北京市自然科学基金(4202056)资助.**魏 翔**(通信作者),博士,讲师,中国计算机学会(CCF)会员,主要研究方向为半监督深度学习、高鲁棒性深度学习.E-mail:xiangwei@bjtu.edu.cn.**王靖杰**,硕士研究生,主要研究方向为半监督深度学习和计算机视觉.**张顺利**,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为视觉跟踪、机器学习和深度学习.**张 迪**,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为边缘智能、普适计算、移动网络与系统.**张 健**,博士,讲师,主要研究方向为智能交通、机器学习和模式识别.**魏小涛**(通信作者),博士,副教授,主要研究方向为智能信息处理、机器学习.E-mail:weixt@bjtu.edu.cn.

CIFAR-10 dataset, when each class is supported by only one label sample, the accuracy of most SSL algorithms degrades seriously. The problem is mainly manifested as: the initial informative information for classification is extremely limited, the model faces cold-start problem; in the process of training, the proportion of pseudo-label noise is difficult to control and the model has a much larger potential risk to be collapsed. In this paper, we propose a Reliable Label Selection and Learning (ReLSL) framework, which tackles the problem semi-supervised deep learning facing when only few-shot labeled image data is available. In brief, we exploit synergies among unsupervised learning, SSL and robust learning to bootstrap additional reliable labels for robust network training. For the unsupervised learning, it is used to ease the problem of cold-start under scarce labeled conditions. For SSL and robust learning, they are used to obtain good learning performance in the presence of noise labels. To be specific, for our whole ReLSL, we first implement Anchor Neighborhood Discovery (AND), an unsupervised learning algorithm to extract features of all training samples, and then obtain their pseudo-label by applying graph-based label propagation algorithm. Then, in order to screen out more reliable and informative samples, a pseudo-label learning and calibration strategy is proposed that comprehensively considers the mean and consistency of the sample's output, and conduct effective screening of samples through Small-Loss theory. After obtaining the dataset with extended labels, considering that a certain proportion of label noise is inevitably introduced into the training set, we therefore propose two strategies to train a robust SSL model, namely, a Label-Smoothing strategy (LS) for regularizing labels from being too sharp, thus reducing noise label interference to loss function; Mean-Shifting Correction strategy (MSC) for reducing the risk of sample output deviation. As a result, the proposed ReLSL achieves state-of-the-art performance on CIFAR-10/100, SVHN, STL-10 and Mini-ImageNet across a variety of SSL conditions with the CNN-13, WRN-28-2 and ResNet-18 networks. In particular, our framework achieves a 6.78% accuracy boosting on CIFAR-10 with only 10 labeled data under WRN-28-2. Moreover, our algorithm can achieve the test error of 6.39±0.47% with only 100 labeled data under CNN-13, which is comparable to the one with typical SSL under 4000 labeled conditions.

Keywords semi-supervised learning; few-shot labels; robustness; label propagation; feature extraction

1 引 言

卷积神经网络(Convolutional Neural Networks, CNNs)目前是视觉表征学习[1-3]的公认标准,但其最普遍的局限性之一是需要大量标记数据来更好地进行模型训练.尽管目前可以轻易获取海量的原始未标记数据,然而,标注样本仍然是一项费时费力的工程[4-7].充分挖掘大量未标记数据中蕴含的潜在信息来提高深度学习准确率一直是解决这一问题的重要研究方向之一.

半监督学习(Semi-Supervised Learning, SSL)旨在充分利用少量有标记数据,并有效挖掘大量无标记数据的潜在信息,以提升模型的泛化能力.目前,最新的半监督深度学习(同样用 SSL 标记)图像分类方法主要集中于以下三方面的探索:(1)利用同一样本在不同扰动下预测的一致性(一致性正则化)[8-10];(2)在训练过程中采用伪标签策略进行标签扩充[11-12];(3)通过数据增强提高模型的鲁棒性[13-14].以上三类方法利用未标记样本的机制不尽相同,然而,在某些情况下,它们可以有效地融合,以进一步提高模型精度.简而言之,伪标记利用模型对未标记样本的预测作为训练的标签,以达到扩充数据集的目的.类似地,一致性正则化在随机变换输入样本或模型函数后,通过模型的输出预测得到"软标签"以进行更新与限制.数据增强类方法通常通过添加各种基于图像预处理的数据增强或混合样本增强(Mixed Sample Augmentation, MSA)[15]来提高模

型的泛化能力.

然而，以上 SSL 算法仍需要一定比例的标记数据作为训练基础，此类算法在标记数据量极少的情况下往往不能进行有效训练. 其通常表现为：初始信息量过少，模型启动困难；训练过程中伪标签噪声比例难以控制，模型容易崩溃. 如在通用的 CIFAR-10 数据集上，当每一类仅有 1 个标签样本作为支撑时，绝大多数 SSL 算法的准确率退化严重[14,16]；同时，在更为复杂的 CIFAR-100 及 Mini-ImageNet 数据集上，极少标签条件下的半监督训练几乎是不可进行的.

针对极少标签样本条件下 SSL 中的启动困难及噪声干扰问题，本文提出了一种基于可靠标签选择与学习(Reliable Label Selection and Learning，ReLSL)的半监督训练算法. 具体地，本文首先运用 Anchor Neighborhood Discovery(AND)[17]无监督学习算法对所有样本进行特征提取，并运用基于图的标签传播算法[18]得到无标签样本的伪标签. 而后，为了筛选出更可靠、更有信息的伪标签样本，本文提出了一种综合考虑样本输出均值与一致性的伪标签学习与标定策略，并通过 Small-Loss 理论[19]对样本进行有效筛选. 在获得具有扩展标签的数据集后，考虑到训练样本中会不可避免地掺杂一定比例的噪声标签，本文提出两种策略来训练高鲁棒的半监督深度模型：标签平滑策略(Label Smoothing Strategy，LS)，通过对伪标记样本输出进行自适应平滑，用以避免标签过于尖锐，从而降低由于标签扩充及后续训练过程中由错误标记数据对损失函数的干扰；均值偏移校正策略(Mean Shifting Correction Strategy，MSC)，通过对历史记录中各类样本特征分布进行统计与加权，用以校正单个样本由于过分扰动所产生的输出偏差，从而降低样本输出偏移风险.

总结来说，本文针对极少标签样本条件下的 SSL 问题，主要贡献和创新之处有以下三方面：

(1) 提出了一种综合考虑样本输出均值与一致性的伪标签学习及标定策略，用于筛选出更为可靠、更有信息的样本以解决极少标签条件下 SSL 中的启动困难问题；

(2) 提出了 LS 自适应标签平滑策略用以避免标签过于尖锐，从而降低错误标记数据对损失函数的干扰；

(3) 提出了 MSC 均值偏移校正策略，用以校正单个样本所产生的输出偏差，从而进一步降低样本输出偏移风险.

本文针对极少标签条件下的 SSL 问题，所提出的 ReLSL 算法框架在 CIFAR-10/100、SVHN、STL-10 和 Mini-ImageNet 数据集上获得了目前最先进的实验结果. 特别地，本文算法在 WRN-28-2[2]下仅有 10 个标记数据(每一类别 1 个标记数据)的 CIFAR-10 上相较于最新算法具有 6.78%的测试误差下降，并且在仅有 100 个标记数据条件下的 CNN-13[9]模型中已可以达到目前主流 SSL 算法 4000 标记时的测试误差(6.39±0.47%). 此外，在 CIFAR-100 数据集上，同样在每一类别仅有 1 个标记数据的条件下，本文算法相较于基线模型获得了 10%+的测试误差下降.

本文第 2 节简要回顾已有的 SSL 相关工作；第 3 节详细介绍本文所提出的算法框架及创新点；第 4 节给出 ReLSL 在多个数据集上的测试结果以及对比讨论；第 5 节对本文工作进行总结并对接下来的工作进行展望.

2　相关工作

以往关于半监督深度学习研究的主要趋势为使用一致性正则化来约束输入预测，使其在不同的数据或网络扰动下保持一致. 最近，伪标记策略进一步提高了模型的准确性，该策略一般通过在训练过程中对未标记数据进行筛选性标记以对数据集进行有效扩展. 在上述两类策略的基础上，研究者们引入了数据增强技术以进一步提高测试准确性.

2.1　一致性正则化

一致性正则化方法首先由 Sajjadi 等人[8]提出，作者运用随机数据增强和 Dropout 等操作，同时通过距离函数，如 L2 范数或交叉熵损失，鼓励在同一样本下两次运行的预测输出尽量一致. 随后，Laine 等人[9]提出了 Temporal Ensembling(TE)概念，对样本输出结果进行指数加权平均以减少一次样本输入，同时实现更为稳定及鲁棒的一致性约束. 考虑到在 TE 方法中，每个 Epoch 的预测只会改变一次，其在学习大型数据集时变得很笨拙. 为了克服这一问题，Tarvainen 等人[20]提出了 Mean Teacher(MT)来平均模型权值，而非样本历史输出. 此外，与对模型及样本进行随机扰动不同，Miyato 等人[21]使用虚拟对抗训练(Virtual Adversarial Training，VAT)将学习到的最有效扰动注入数据样本，以便对预测进行一致性正则化. 最近，Verma 等人[22]提出了插值一致性训练(Interpolation Consistency Training，ICT)，这是一种受 MSA[15]启发的算法，通过对两样本混合位置的一致性约束以进一步稳定模型输

出.在文献[10]中,作者将 Lipschitz 约束运用到用于 SSL 的生成对抗网络(Generative Adversarial Networks,GANs)[23]中,以进行类一致性约束.最近,ReMixMatch[16]也采用了一致性正则化策略,其将约束作用于多个强增强样本的输出与同一弱增强版本输出以进一步发挥数据增强在一致性约束中的作用.

2.2 伪标记策略

针对半监督学习中的伪标签策略早在数十年前便已经为研究者所知.Shi 等人[24]将网络预测转换为对未标记样本的硬标签,并引入了不确定性加权损失指导网络训练;此外,方案进一步进行了最小-最大特征(Min-Max Feature,MMF)正则化,以鼓励类内一致性和类间分离性.最近的一项工作使用了一种基于图的标签传播方法[18],该方法对整个数据集进行预测,并使用这些预测为未标记数据生成伪标签以共同训练深度神经网络.最近,FixMatch 方法[14]被提出,其通过使用模型对弱增强无标记样本的预测来生成伪标签,当输入同一个样本的强增强版本时,模型利用其伪标签进行监督训练.类似地,Wei 等人[25]提出一种增量式伪标签标定策略,在训练过程中动态改变标签数据集,并运用动态平衡因子调整数据损失权值.不同于为每个未标记数据设置硬伪标签,Arazo 等人[11]提出了一种针对 SSL 的软伪标签策略,其中所采用的软标签由模型最后一次预测得到的.最近,针对极少标签样本条件下的 SSL 问题,Albert 等人[26]提出了一种有效筛选噪声标签的训练形式以在训练初期获得较为稳定、有效的伪标签.此外,Chen 等人[27]使用类知识蒸馏策略进行 SSL 任务,并在 ImageNet 上获得了最佳的半监督表现.据调研的最新成果,谷歌团队通过使用元学习生成伪标签[28]以达到在 CIFAR-10 数据集上 4000 标签样本条件下的最佳效果.

2.3 数据增强

对于使用深度模型的上述两类 SSL 策略,最近的大多数工作都将不同的数据增强策略集成至他们的基础模型中,以获得更高的性能.对于 MSA 方法,Verma 等人[22]首次提出对训练数据进行混合增强以达到一个强基线,并通过增强两个训练样本之间的插值平滑性进一步稳定模型输出.以同样的方式,文献[11]和[29]通过数据混合增强以帮助校准深度神经网络,从而减少确认偏差.最近,Wei 等人[30]提出了一种基于 FMixCut 的数据增强策略,通过改进 FMix[31]算法并运用于半监督深度学习任务中以获得更高的分类准确率.此外,其方法还引入了动态标签样本混合策略以进一步加速模型收敛.近期,针对 SSL 的另一种基于传统"强"图像处理的数据增强策略引起了研究者的关注.在文献[13]中,无监督数据增强方法被提出,以对模型在一个未标记样本和它的强增强版本之间预测的一致性进行约束.进一步,Berthelot 等人[16]提出了一种名为 ReMixMatch 的数据增强 SSL 框架变体,在其提出的基于控制理论的"CTAugment"中,不需要任何形式的基于强化学习的训练便可以执行数据增强,从而大大增加了"强"数据增强组合策略的效率.此外,FixMatch[14]提出综合利用 Cutout[32]、CTAugment[16]和 RandAugment[33]进行数据增强的方法以获得更为准确的半监督分类效果.

3 算法描述

本文将 SSL 问题描述为通过在数据集 $\mathcal{D}$ 上训练深度神经网络 $f_\theta(\cdot)$ 用于 C 分类问题,其中 $\mathcal{D}$ 分为无标签数据集 $\mathcal{D}_U=(\boldsymbol{x}_i^U)_{i=1}^{N_U}$ 以及标签数据集 $\mathcal{D}_L=(\boldsymbol{x}_i^L,\boldsymbol{y}_i^L)_{i=1}^{N_L}$,$\boldsymbol{y}_i^L$ 为标签,通常采用 one-hot 向量表示,即长度为 C 的向量中仅有 1 个位置值为 1,其余为 0.对于极少标签样本下的 SSL 问题,有 $N_L \ll N_U$.针对本文提出的 ReLSL 算法,其流程如图 1 所示,主要分为三个步骤:特征提取与基于图的标签传染(3.1 节);

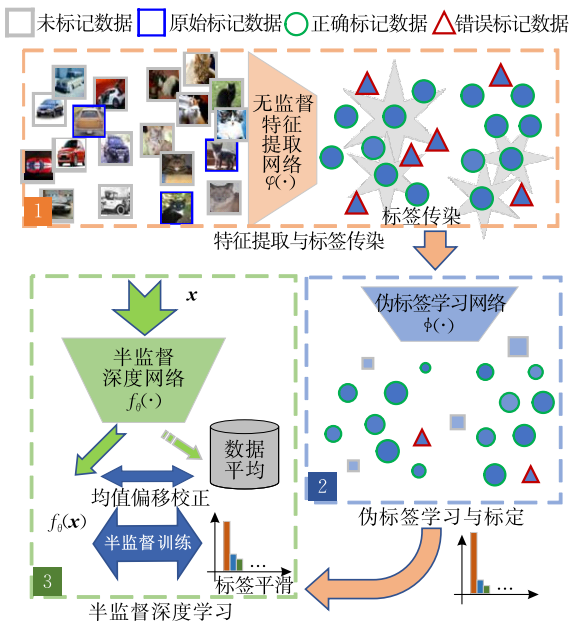

图 1 本文 ReLSL 算法流程图(步骤 1 为特征提取与标签传染过程(上);步骤 2 为伪标签学习与标定过程(右下),其中图形大小代表了输出置信度,图形越大,置信度越高;图形填充灰度代表了历史输出稳定程度(一致性),颜色越深,输出越稳定;步骤 3 为半监督深度学习过程(左下))

基于均值与一致性的伪标签学习与标定(3.2 节)；利用 LS 及 MSC 策略进行半监督学习(3.3 节).

3.1　特征提取与标签传染

特征提取及标签传染的整体过程如图 1 中步骤 1 所示.针对 SSL 问题,本文首先借鉴文献[26]中的结论,且为了公平地比较,我们选用了(Anchor Neighborhood Discovery,AND)算法[17]进行特征学习,表示为 $\boldsymbol{e}_i=\varphi(\boldsymbol{x}_i)$,其中 $\varphi(\cdot)$对应 AND 网络,默认采用 ResNet-50 结构.由于特征提取网络 $\varphi(\cdot)$在本文中扮演黑盒特征提取器的角色,且此部分并非本文工作重点,因此这里不再赘述其训练过程.

当获得提取的特征$\{\boldsymbol{e}_i\}_{i=1}^{N_L+N_U}$后,我们采用式(1)进行相似度矩阵 $\boldsymbol{A}$ 的计算.

$$\boldsymbol{A}_{m,n}=\begin{cases}\left(\dfrac{\boldsymbol{e}_m^{\mathrm{T}}\boldsymbol{e}_n}{\|\boldsymbol{e}_m\|\|\boldsymbol{e}_n\|}\right)^{\gamma}, & \text{若 } m\neq n \text{ 且 } \boldsymbol{e}_m\in kNN(\boldsymbol{e}_n)\\ 0, & \text{其他}\end{cases}\tag{1}$$

其中 γ 为超参数,用于控制对远距离样本的敏感程度,其值越大则代表对特征距离相差较大的样本相似度越小.本文参照文献[18],将其设置为 3.$kNN(\boldsymbol{e})$用于计算 $\boldsymbol{e}$ 的 k 临近样本特征,为进行公平比较,本文将 k 值统一设置为 50.

而后对矩阵 $\boldsymbol{A}$ 进行规范化操作,获得矩阵 $\boldsymbol{W}$:

$$\boldsymbol{W}=\boldsymbol{D}^{-1/2}\boldsymbol{A}\boldsymbol{D}^{-1/2}\tag{2}$$

其中 $\boldsymbol{D}$ 为对角矩阵,其对角线上的值为图中对应节点的度.

接下来,本文定义维度为$(N_L+N_U)\times C$ 的标签矩阵 $\boldsymbol{Z}$ 用以获得每一个无标签样本 $\boldsymbol{x}_i^U$ 的伪标签隶属度向量,其表达式为

$$\boldsymbol{Z}=(\boldsymbol{I}-\alpha\boldsymbol{W})^{-1}\boldsymbol{Y}\tag{3}$$

其中,α 代表跳向图中相邻节点的概率,$\boldsymbol{I}$ 为单位矩阵,$\boldsymbol{Y}$ 为与 $\boldsymbol{Z}$ 同维度的初始化标签矩阵,对于标签样本 $\boldsymbol{x}_i^L$,$\boldsymbol{Y}_{i,c}=1$,其中 $\arg\max(\boldsymbol{y}_i^L)=c$,而其余未标记样本对应位置的 $\boldsymbol{Y}$ 行值均为 0.考虑到求解$(\boldsymbol{I}-\alpha\boldsymbol{W})^{-1}$的困难性,本文实验中同样采用共轭梯度法[34]求解该问题.

当获得了稳定的标签矩阵 $\boldsymbol{Z}$ 后,对于无标签样本,我们通过取最大值以将隶属度向量转化为 one-hot 向量;而对于标签样本,其对应位置值与 $\boldsymbol{Y}$ 保持一致,本文将调整后的标签矩阵记为 $\widetilde{\boldsymbol{Z}}$.

3.2　基于均值与一致性的伪标签学习与标定

针对一般的 SSL 问题,采用 3.1 节所述的标签传播策略后,其伪标签的标定准确率已具有较高保障.依靠基于一致性正则项半监督模型所天然具有的鲁棒性,其最终分类准确率已逼近监督学习[14].然而,针对本文所关注的极少标签条件下的半监督学习问题,由于初始信息的极度匮乏,其伪标签质量无法仅通过以上标签传染得到保障.因此,本文需进一步对伪标签样本进行再学习与重标定.

依据 Small-Loss 理论,即正确标记的样本往往在学习率较大的训练前期更容易被网络记忆,其损失也相对较小.本文将在此理论基础上,设计一个综合考虑样本输出均值与一致性的伪标签学习与标定策略.

首先,对基于传统 Small-Loss 理论进行模型$\phi(\cdot)$的训练过程中,我们采用被广泛应用的 WRN-28-2 网络结构,其损失函数被定义为标准交叉熵(Cross Entropy,CE)损失函数,即:

$$loss_{\mathrm{ce}}=-\sum_{c=1}^{C}\widetilde{\boldsymbol{Z}}_{i,c}\log(\phi(\boldsymbol{x}_i)_c)\tag{4}$$

其中 $\widetilde{\boldsymbol{Z}}_{i,c}$ 表示样本 $\boldsymbol{x}_i$ 对应标签属于类别 c 的概率,相应地,$\phi(\boldsymbol{x}_i)_c$ 表示 $\boldsymbol{x}_i$ 经过网络输出属于类别 c 的概率.

然而,随着训练的进行,Small-Loss 理论仍然无法保证模型不会过拟合于噪声样本,尤其当噪声比例过高时.考虑到噪声样本在训练过程中天然具有的输出强不确定性,即输出损失方差大,因此,本文在模型 $\phi(\cdot)$的训练过程中引入一致性惩罚项,其目的在于令错误分类或难分类样本在训练过程中关注其输出的一致性(确定性),从而缓解由于过度训练造成的 CE 损失过早收敛.因此,本文将 $\phi(\cdot)$的训练优化函数改写为

$$loss_{\mathrm{ce}+}=loss_{\mathrm{ce}}+\varsigma\|\phi(\boldsymbol{x}_i)-\phi(\hat{\boldsymbol{x}}_i)\|_2\tag{5}$$

其中 $\boldsymbol{x}_i$ 与 $\hat{\boldsymbol{x}}_i$ 表示同一样本经过两次数据增强后的结果,ς 为权重超参数,其值越大,则代表损失函数更关注模型对样本输出的稳定性,反之,更关注其对标签的一致程度,具体设置请参照 4.1 节.

虽然依据式(5)可以进一步相对准确地挑选出具有正确标记的样本,然而,这些样本往往为易分类样本,即并非均具有代表性,因而导致其对模型的训练贡献受限.通过观察,我们发现某些样本虽然损失较高,即置信度不高,但损失的波动并不明显,即一致性较强(如图 1 中步骤 2 所示),而此类样本往往也能够被正确预测并更具有分类价值.因此,与直接对样本输出损失进行排序并筛选的方法不同,本文将记录样本在训练后期的输出损失,并通过均值与方差的综合考量,即由式(6)确定标签样本.

$$Choose_i=mean(loss_{\mathrm{ce}}(-d:)_i)+std^2(loss_{\mathrm{ce}}(-d:)_i)\tag{6}$$

注意此处仍以 $loss_{\mathrm{ce}}$ 作为筛选依据,$loss_{\mathrm{ce}}(-d:)_i$ 表示样本 $\boldsymbol{x}_i$ 在模型最后 d 个 epoch 获得的损失.当为每个训练样本获取 $Choose_i$ 后,我们将其进行升序排序,并为依据最后一次训练获得的 one-hot 标签

$\arg\max(\phi(\boldsymbol{x}_i))$进行标记的每一类别组保留前 κ 个样本，而其余样本则重新标定为未标记样本(如图 1 中步骤 2 所示). 我们将重标定后的训练数据集记为 $\widetilde{\mathcal{D}}$，其中，标签数据集为 $\widetilde{\mathcal{D}}_L=(\boldsymbol{x}_i^L,\boldsymbol{y}_i^L)_{i=1}^{N_L+\widetilde{N}_L}$，无标签数据集为 $\widetilde{\mathcal{D}}_U=(\boldsymbol{x}_i^U)_{i=1}^{N_U-\widetilde{N}_L}$，对于极少标签条件下，有 $N_L\ll\widetilde{N}_L$.

3.3 基于 LS 及 MSC 策略的半监督学习

本节将以 $\widetilde{\mathcal{D}}$ 作为数据集进行 $f_\theta(\cdot)$ 模型训练. 为了进行公平地比较并证明所提出 LS 及 MSC 策略的有效性，本文选用了当下最先进的研究成果作为半监督骨干网络与方法框架，分别为 Pseudo-label[11]、FMCmatch[30]、ReMixMatch[16] 以及 FixMatch[14]. 考虑到相关模型的共通性与差异性，且为保证方法描述的完整性，本文在骨干模型与方法框架描述中仅列出关键部分.

一般地，SSL 问题的优化函数表达为

$$loss=(loss_{\text{ssl}}+loss_{\text{sl}})\oplus\widehat{strategy} \tag{7}$$

其中 $loss_{\text{ssl}}$ 代表半监督损失函数，如一致性正则项、Mixup[15]、FCut[30]、FMix[31] 以及一些无监督损失函数(熵最大化[11]、旋转不变[16])等，此项一般同时作用于数据集 $\mathcal{D}_U$ 与 $\mathcal{D}_L$ 上. $loss_{\text{sl}}$ 为传统监督学习损失函数，一般为作用于 $\mathcal{D}_L$ 或 $\widetilde{\mathcal{D}}_L$ 上的 CE 损失函数. 符号$\oplus$表示作用关系，其后的 $\widehat{strategy}$ 为作用于模型训练过程中的策略，如动态标签样本混合策略[30]、自学习标签传染策略[14,25]、多路预测混合自标定策略[16,31]、Training Signal Annealing[31] 以及 Distribution Alignment[16]等.

3.3.1 标签平滑策略

尽管依据式(6)可进一步对标记数据进行提纯，然而，$\widetilde{\mathcal{D}}_L$ 中仍然具有一定量的错误标签样本，并且随着训练的进行，错误标签可能逐渐扩散. 因此，在模型训练过程中，我们将采用标签平滑策略 LS 对 $\widetilde{\mathcal{D}}$ 中样本所对应的“标签”$\boldsymbol{y}_i$ 等比例平滑，以缓解由于错误标记导致无法修正的问题.

$$\tilde{\boldsymbol{y}}_i=\lambda_i[(1-\lambda_i)/(\lambda_i C)+\boldsymbol{y}_i] \tag{8}$$

其中：

$$\lambda_i=\begin{cases}(1-\tau)+\beta\tau, & \text{若 } \boldsymbol{y}_i<(1-\tau)+\beta\tau\\ 1, & \text{其他}\end{cases} \tag{9}$$

τ 为基础平滑系数，β 为 0 至 1 之间均匀采样随机数. 由式(8)可知，λ 为平滑因子，其值越小，则输出向量越平滑，与此同时，式(8)仍保证了对于每一个样本的输出向量元素之和为 1. 考虑到模型的收敛问题，标签平滑策略需随着迭代的进行逐渐衰减，即 τ 需逐渐变小，而绝大多数 SSL 均采用学习率衰减策略进行模型训练，因此，本文经验性地将 τ 设置为学习率 lr，具体分析请参照 4.1 节. 由式(9)可知，随着学习率的不断衰减，λ 逐渐变大，即 LS 策略会随着迭代的进行，减小标签的不确定性，从而帮助模型收敛；与此同时，式(9)中的衰减条件也保证了模型训练的稳定性. 值得一提的是，本策略与知识蒸馏中教师模型的 Soft Target[35] 功能类似，也可为本文所涉及的单网络训练提供更多类间和类内信息.

针对 $\boldsymbol{y}_i$ 的获取，为进一步稳定训练，本文采用指数加权平均操作对样本每一次的输出结果进行加权平均，即：

$$\tilde{\boldsymbol{s}}_{i(t)}=\mu\tilde{\boldsymbol{s}}_{i(t-1)}+(1-\mu)\boldsymbol{f}_{\theta(t-1)}(\boldsymbol{x}_i),$$
$$\boldsymbol{y}_i=\tilde{\boldsymbol{s}}_{i(t)}/(1-\mu^t) \tag{10}$$

其中 $\boldsymbol{f}_{\theta(t-1)}(\boldsymbol{x}_i)$ 代表样本 $\boldsymbol{x}_i$ 在模型 $f_\theta(\cdot)$ 训练的第 $t-1$ 个 epoch 时的输出向量. $\tilde{\boldsymbol{s}}_{i(t-1)}$ 为样本 $\boldsymbol{x}_i$ 在 epoch $t-1$ 时的移动平均值，μ 为动量权重用以控制更新力度，对于伪标签样本 $\boldsymbol{x}_i\in\widetilde{\mathcal{D}}_L$，我们将其设置为 0.99，而对于无标签样本 $\boldsymbol{x}_i\in\widetilde{\mathcal{D}}_U$，$\mu$ 设置为 0.4.

3.3.2 均值偏移校正策略

受错误标签及扰动的影响，单个样本输出结果仍有一定概率发生偏移，而考虑到整体训练数据具有更强的统计意义以及稳定性，本文提出一种均值偏移校正策略，即通过对每一类样本分别求其输出的均值分布，而后对单个样本进行加权融合以进行偏移校正.

具体地，我们首先将数据集 $\widetilde{\mathcal{D}}$ 中每个样本在 Softmax 的输入向量进行指数加权平均操作：

$$\tilde{\boldsymbol{z}}_{i(t)}=\mu\tilde{\boldsymbol{z}}_{i(t-1)}+(1-\mu)\boldsymbol{f}^{\text{logit}}_{\theta(t-1)}(\boldsymbol{x}_i),$$
$$\tilde{\boldsymbol{\xi}}_i=\tilde{\boldsymbol{z}}_{i(t)}/(1-\mu^t) \tag{11}$$

与式(10)类似，$\boldsymbol{f}^{\text{logit}}_{\theta(t-1)}(\boldsymbol{x}_i)$ 代表样本 $\boldsymbol{x}_i$ 在模型 $f_\theta(\cdot)$ 训练的第 $t-1$ 个 epoch 时 Softmax 的输入向量，μ 为动量权重用以控制更新力度.

当为每一个训练样本在每下一 epoch 设置了更为稳定的指数加权平均输出 $\tilde{\boldsymbol{\xi}}_i$ 之后，本文进而对每一虚拟类中的输出进行平均操作，即：

$$\boldsymbol{Center}_t(c)=mean(\tilde{\boldsymbol{\xi}}_i),\ \text{for}\ \arg\max(\tilde{\boldsymbol{\xi}}_i)=c \tag{12}$$

其中 $\boldsymbol{Center}_t$ 为 $C\times C$ 矩阵，每一行 $\boldsymbol{Center}_t(c)$ 代表了当前 epoch t 下类别 c 所对应类的平均输出概率向量，既包含原始有标签样本也包含原始无标签样本.

接下来，对于 $\boldsymbol{x}_i^U\in\mathcal{D}_U$ 的输出向量 $\boldsymbol{f}^{\text{logit}}_{\theta(t)}(\boldsymbol{x}_i^U)$，本文采用损失函数(13)对其进行偏移校正.

$$loss_{\text{msc}}=\sigma\left\|\boldsymbol{f}^{\text{logit}}_{\theta(t)}(\boldsymbol{x}_i^U)-([\boldsymbol{f}_{\theta(t)}(\boldsymbol{x}_i^U)]\boldsymbol{Center})\right\|_2 \tag{13}$$

其中 $\boldsymbol{f}_{\hat{\theta}(t)}(\boldsymbol{x}_i^U)$ 表示固定且不参与参数更新的模型输出概率向量，σ 为权重因子，用以控制校正比例. 与 LS 策略类似，随着训练的进行，模型希望这种不确定性或矫正力度逐渐减小，为简单起见，此处我们仍将 σ 设置为 lr，具体分析请参照 4.1 节.

最后，我们即可将现有最新基于伪标签 SSL 算法中的有监督学习中伪标签 $\boldsymbol{y}^L$ 替换为式(8)中的 $\tilde{\boldsymbol{y}}_i$，并代入式(7)的传统监督损失函数 $loss_{\mathrm{sl}}$ 中进行训练. 与此同时，我们将式(13)中的均值偏移校正项 $loss_{\mathrm{msc}}$ 加入式(7)中一并进行优化. 可以看出，对于统一的伪标签半监督学习模式，本节所提出的两个校正策略均为在原有损失基础上的增量修正策略，具有普适性，并且对于 Mixup 类数据增强方式也同样适用.

4　实验结果及分析

为证明本文所提出算法框架的有效性与通用性，本节将 ReLSL 应用于当下流行的半监督图像分类任务，包括 CIFAR-10/100、SVHN、STL-10 和 Mini-ImageNet 数据集，并在最新的 SSL 算法框架 Pseudo-label[11]、FMCmatch[30]、ReMixMatch[16] 以及 FixMatch[14] 基础上进行对比测试. 经过在数据集 CIFAR-10 及模型 FMCmatch 下的 WRN-28-2，40 标签数据条件下超参数调优，同时参照文献中的相关设置，在以下的实验中，本文将 3.2 节中的 $\phi(\cdot)$ 设置为 ResNet-50；式(1)中的 $\gamma=3$，$k=50$；式(3)中的 $\alpha=0.99$；式(5)中的 $\varsigma=0.5$；式(10)及式(11)中的 $\mu=0.99(0.4)$. 此外，在伪标签标定的训练过程中，每一类保留的总标签样本数目默认为 $\kappa=5000/C$，即总数目 $N_L+\widetilde{N}_L=5000$，学习率固定为 0.1，batch size 为 512，总迭代 epoch 数为 60，且 $d=15$. 在半监督训练过程中，包括数据处理、训练方式、其他超参数设置及网络结构均遵循原骨干模型方法框架.

接下来，4.1 节将主要对模型中的重要超参数设置进行讨论，4.2～4.6 小节将分别展示 5 种图像分类任务数据集下的算法表现，4.7 小节将对本文所提出的三个创新点进行消融研究分析，以验证用于 SSL 的 ReLSL 算法框架的有效性. 所有实验均在 Ubuntu 18.04 环境完成，深度学习框架为 Pytorch 1.5.1 以及 TensorFlow 1.14.0，GPU 为 GTX 1080 Ti 及 RTX 2080 Ti.

4.1　模型超参数学习

在伪标签标定阶段，ReLSL 算法中核心超参数为式(5)中的 ς. 因此，本节将首先考察超参数的设置问题. 表 1 展示了不同超参数条件下，针对 40 个初始标签样本并挑选 5K(K 代表千)个作为伪标签样本时最终被错误标记的样本比例(%)及最终半监督学习错误率，其中粗体为相对最佳值. 由表 1 可以发现，当 $\varsigma=0.5$ 时伪标签标注正确率最高，与此同时，其最终的分类准确率也相对最高，因而在本文所有相关实验中，将 ς 设置为 0.5.

表 1　受 ς 影响下初始 40 标签样本挑选 5K 伪标签样本标定错误及最终分类错误率　(单位：%)

ς	伪标签错误率	最终半监督错误率
0	1.34	7.87
0.5	**1.12**	**6.93**
1.0	1.14	7.22
5.0	1.22	7.38

在接下来的半监督训练中，核心超参数为伪标签总数目 κC、式(9)及式(13)中的平滑系数 τ 及权重因子 σ. 因此，我们将原始 CIFAR-10 训练集中的 5K 个训练样本用于验证，其余 45K 用于训练. 表 2 展示了 ReLSL 算法在 40 标签条件下 WRN-28-2 上的半监督学习验证误差，同时我们将伪标签错误率也一并展示(伪标签总数右侧). 考虑到运算量，此处我们针对每一个超参数组合随机训练模型 $\phi(\cdot)$ 一次，并且将 τ 与 σ 直接设置为相等.

表 2　受 κC、τ 及 σ 影响下的 40 标签样本伪标签错误率及 SSL 验证误差　(单位：%)

$\kappa C\backslash\tau$ 与 σ	0.1	0.2	lr
1K(0.20)	8.53	8.98	8.37
5K(1.12)	8.02	9.23	**7.58**
10K(2.44)	8.06	9.02	7.74
30K(9.06)	11.69	12.35	11.87
50K(15.00)	22.64	23.60	21.56

由表 2 可知：当伪标签总数为 50K 时，其测试效果最差，即此时的伪标签学习与标定策略并无作用，所有原始无标签样本的伪标签均被当作训练标签处理. 而虽然 1K 伪标签条件下可获得近 100%的标记准确率，但由于 $\widetilde{\mathcal{D}}_L$ 总数受限，训练结果依然不及 5K(1.12%)与 10K(2.44%). 经过综合考察，本文默认将伪标签总数设置为 5K，平滑系数 τ 及权重因子 σ 均等于学习率，并随着训练的进行逐渐衰减. 至于在 $\tau=0$ 及 $\sigma=0$ 下的对比实验，见 4.7 节.

4.2　CIFAR-10 数据集测试结果

CIFAR-10 包含大小为 32×32 的 10 类共计 60K 张自然图像，其中 10K 张用于测试. 在本数据集的测试过程中，标签学习与标定的训练过程中均采用默

认值.在半监督训练过程中,我们分别选用 4 种 SSL 算法框架[11,14,16,30]进行针对性测试对比.为验证本文针对极少标签及一般条件下半监督学习的优越表现,我们将标签样本总数分别设置为 10、40、100、1K 及 4K 进行测试,并同时选用了 CNN-13 及 WRN-28-2 作为骨干网络.实验结果均取 3 次随机运行结果的均值与标准差进行展示,如表 3 所示,其中"—"代表无可用对比实验.

表 3 ReLSL 算法及最新算法在 CIFAR-10 上测试误差率对比 (单位:%)

方法	CNN-13				WRN-28-2 (1.5M)			
	40	100	1K	4K	10	40	1K	4K
Π model[9]	—	—	—	12.36±0.31	—	—	23.07±0.66	17.41±0.37
MT[20]	—	—	21.55±1.48	12.31±0.28	—	—	17.32±4.00	10.36±0.25
SNTG[36]	—	—	18.41±0.52	10.93±0.14	—	—	—	—
MT-SWA[37]	—	—	15.58±0.12	9.05±0.21	—	—	—	—
ISL-GAN[25]	—	—	11.18±0.20	8.75±0.23	—	—	—	—
ICT[22]	—	—	15.48±0.78	7.29±0.02	—	—	—	7.66±0.17
UDA[13]	**29.05±5.93**	—	—	—	—	29.05±5.93	6.39±0.32	5.27±0.11
MixMatch[29]	—	—	—	6.84		47.54±11.50	7.75±0.32	6.24±0.06
UPS[38]			**8.18±0.15**	**6.39±0.02**	—	—	—	—
MPL[28]	—	—	—	—	—	—	—	**3.89±0.07**
TC-SSL[39]	—	—	—	—	—	—	**6.15±0.23**	5.07±0.05
ReLaB+PL[26]	—	11.41±0.29	—	—	**30.40±11.20**	16.75±3.81	—	—
ReLaB+RMM[26]	—	—	—	—	30.79±14.24	**9.35±2.71**	—	—
PL[11]	—	12.83±0.68	6.85±0.15	5.97±0.15	55.61±5.28	29.65±5.71	—	**6.28±0.30**
ReLSL+PL	—	**10.84±0.70**	**6.46±0.16**	**5.78±0.17**	**27.02±6.94**	**10.23±0.91**	**6.59±0.21**	6.34±0.14
FMCmatch[30]	26.60±4.19	11.81±0.92	5.87±0.11	**4.54±0.06**	46.96±9.20	23.59±7.45	6.48±0.13	4.66±0.12
ReLSL+FMCmatch	**7.64±0.36**	**6.39±0.47**	**5.63±0.23**	4.63±0.06	**23.62±8.00**	**6.91±0.38**	**5.61±0.21**	**4.43±0.09**
RMM[16]	—	—	—	—	58.80±1.98	31.36±4.37	**5.73±0.16**	5.14±0.04
ReLSL+RMM	—	—	—	—	**24.72±7.88**	**8.19±0.65**	5.75±0.18	**4.72±0.08**
FixMatch[14]	—	—	—	—	≈40.00	11.39±3.35	—	**4.31±0.15**
ReLSL+FixMatch	—	—	—	—	**24.89±8.24**	**6.94±0.44**	**5.11±0.10**	4.34±0.13

由表 3 可以观察到,本文所提出的 ReLSL 性能在现有最新算法基础上的绝大部分半监督条件下均有所提升.特别地,ReLSL 算法在极少标签半监督条件下的性能提升更为显著.在仅有 10 个标签样本的 WRN-28-2 模型上,本文算法相较于最新的 ReLaB 平均错误率下降了 6.78%(23.62 VS. 30.40);在仅有 40 个标签样本条件下,测试误差下降了 2.44%(6.91 VS. 9.35);在 CNN-13 模型上的 100 标签条件下,测试误差已可与典型算法 4K 条件相持平(6.39).

值得一提的是,由于 ReLSL 在伪标记样本选择时统一将每一类的标记数量 κ 设置为 500,而对于拥有较多初始标签的条件,尤其当标签样本总数超过 1K 时,其效果提升并不明显.通过实验观察,在拥有 1K 标记样本的半监督学习中,经过一定轮数的模型更新,95%以上的未标记样本已具有了正确标记,而此时的 ReLSL 相关策略作用并不凸显.并且,在拥有 1K 或以上标签数据的半监督学习条件下,模型已不受启动困难问题的影响.

图 2 为 1K 初始标签样本半监督条件以及 ReLSL+FMCmatch 算法的 WRN-28-2 网络结构下,将总标签值分别设置为 1K、5K、10K、15K 以及 20K 时的半监督学习过程错误率收敛曲线,其中 1K 总标签数对应的算法即为原始 FMCmatch.

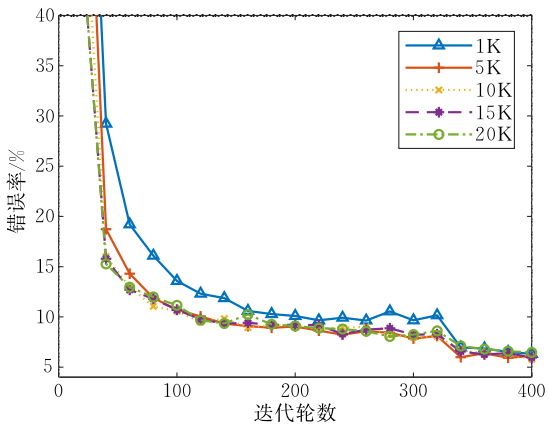

图 2 1K 标签样本半监督条件下不同伪标签总数对于模型收敛的影响

由图 2 可知,通过不断扩大伪标签样本比例可进一步提升模型前期收敛速度,然而其最终准确率仍维持在一个相对固定的水平,而过多的伪标签则会在一定程度上影响最终效果.并且,即使正确伪标签样本总数与 4K 条件下的标定结果持平(均约为 100%),1K 条件下的半监督错误率仍无法达到 4K 条件下的水平.其原因在于标签传染过程所标定的伪标签样本与原标签样本具有较强相关性,其实际信息量并不能达到完全随机抽取标签样本的水平.

进一步，参照文献[14]、[16]及[26]，我们考察了 8 组固定标签样本条件下模型性能表现. 图 3 对 8 组数据进行了可视化展示，从左至右组内图像代表性依次减弱，2～7 组与随机挑选效果相似. 图 4 绘出本文 ReLSL＋FMCmatch 算法与 ReLaB、RMM 及 FixMatch 在 8 组半监督条件下测试错误率对比结果（均采用 WRN-28-2 网络）. 可以看到，在 8 组固定标签样本条件下，本文算法有着更佳的整体表现. 特别地，在最具代表性的 10 标签条件下（组 1），ReLSL＋FMCmatch 已可将测试误差降至 10％以下. 此外，我们继续在 CNN-13 网络下进行了随机 10 标签样本对比实验，实验结果表明相较于 FMCmatch 的 48.03±5.11 错误率，本文提出的 ReLSL＋FMCmatch 降低至 25.28±7.95，进一步证明本文方法的通用性及有效性.

图 3　每类 1 个标签样本的半监督实验的标记训练数据

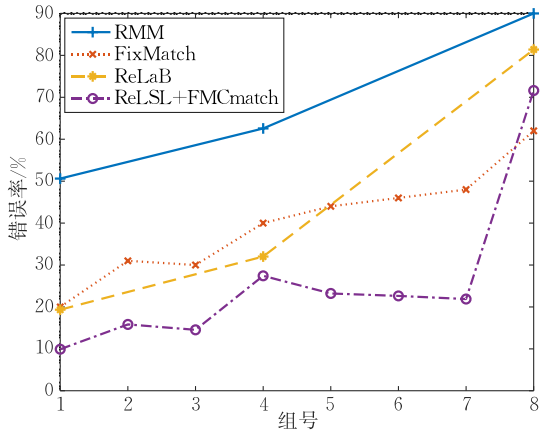

图 4　8 组标签样本下半监督测试错误率对比结果

4.3　CIFAR-100 数据集测试结果

与 CIFAR-10 类似，CIFAR-100 包含大小为 32×32 的 60K 张自然图像，共 100 个类，其中保留 10K 张样本用于测试. 在标签传染操作的模型训练过程中，κ 采用默认值 $5000/C$. 在半监督训练过程中，我们同样选用 4 种 SSL 算法框架[11,14,16,30]进行针对性测试与对比. 为突出本文针对极少标签及一般条件下半监督学习的优越表现，我们将标签样本总数分别设置为 100、400、2.5K、4K 及 10K（$\kappa=10000/C$）进行测试，并且同时选用了 CNN-13 及 WRN-28-135 或 WRN-28-128 作为骨干网络模型. 由于运算量较大，此处实验结果仍取 3 次随机运行结果的均值与标准差进行展示，如表 4 所示，其中绝大部分对比结果来源于原文或引文. 参照相关文献，表中 PL*、ReLaB* 与 ReLSL＋PL* 右半表格及带有 * 号位置数值为 WRN-28-2(1.5M) 上的运行结果.

表 4　ReLSL 算法及最新算法在 CIFAR-100 上测试误差率对比　（单位：％）

方法	CNN-13			WRN-28-135(26M)或 WRN-28-128(24M)			
	2.5K	4K	10K	100	400	2.5K	10K
Π model[9]	57.25±0.48	—	39.19±0.36	—	—	57.25±0.48	37.88±0.11
MT[20]	**53.91±0.57**	45.36±0.49	36.08±0.51	—	—	53.91±0.57	35.83±0.24
SNTG[36]	—	—	37.97±0.29	—	—	—	—
MT＋LP[18]	—	43.73±0.20	35.92±0.47	—	—	—	—
MT-SWA[37]	—	—	33.62±0.54	—	—	—	—
UPS[38]	—	**40.77±0.10**	**32.00±0.49**	—	—	—	—
MixMatch[29]	—	—	—		67.61±1.32	39.94±0.37	28.31±0.33
TC-SSL[11]	—	—	—	—	—	**31.95±0.55**	**22.10±0.37**
ReLaB＋PL*[26]	—	—	—	73.88±1.52	57.29±1.17	44.48±1.01	—
ReLaB＋RMM*[26]	—	—	—	**68.93±1.97**	**48.87±1.08**	36.46±0.34	—
PL*[11]	—	37.55±1.09	32.15±0.50	88.23±0.32	67.57±0.58	45.42±0.68	—
ReLSL＋PL*	—	**36.25±0.79**	**31.94±0.49**	**72.79±1.84**	**53.68±0.81**	**40.11±0.70**	**31.25±0.34**
FMCmatch[30]	43.97±0.64	36.01±0.61	**29.55±0.38**	77.91±1.48	46.97±0.43	29.08±0.62	26.26±0.53
ReLSL＋FMCmatch	**40.25±0.62**	**35.08±0.40**	30.19±0.36	**66.90±1.45**	**44.28±1.21**	**28.93±0.76**	**25.91±0.73**
RMM[16]	—	—	—	81.18±2.36*	44.28±2.06	27.43±0.31	**23.03±0.56**
ReLSL＋RMM	—	—	—	**67.44±1.98***	**42.59±1.27**	**27.35±0.35**	23.10±0.70
FixMatch[14]	—	—	—	—	48.85±1.75	**28.29±0.11**	22.60±0.12
ReLSL＋FixMatch	—	—	—	—	**45.22±1.07**	28.43±0.34	**22.39±0.12**

由表 4 可观察到，在 CIFAR-100 数据集上，本文所提出的 ReLSL 性能在现有最新算法基础上的大部分半监督条件下均有所提升. 同样地，ReLSL 算法在极少标签半监督条件下的性能有着显著的提升. 相较基于 WRN 的基线模型，在每一类别仅有 1 个标签样本的条件下，本文算法有着超过 10% 的测试误差下降（见表 4 中第 5 列）. 与此同时，在 CNN-13 网络结构的 100 标签样本条件下，ReLSL+FMCmatch 相较于 FMCmatch 算法将测试误差由 84.19±0.71 下降至 71.18±1.33. 同样地，当标记数据样本总量相对充足时，本文算法的效果提升并不明显，如在 WRN-28 模型下的 2.5K 及 10K 标签条件下，本文算法与基线模型测试误差率已十分接近，考虑到模型本身训练的波动以及调参影响，其性能存在一定波动也是合理的. 此外，在本节挑选的 4 种基线框架中，PL 与 FMCmatch 并未采用 AutoAugment 类方法进行强数据增强，而后两种则采用了此策略，且 PL 相对于后三者在 WRN 模型上选用了更为轻量的 WRN-28-2. 经过实验对比可以看出，基于强数据增强策略的算法在CIFAR-100 上的性能表现更为突出，更大的模型结构也可帮助算法获得更低的测试错误率，且本文方法并未与已有各算法框架发生冲突.

4.4 Mini-ImageNet 数据集测试结果

Mini-ImageNet 数据集采样自 ImageNet，其共包含 60K 张分辨率为 84×84 的 100 类自然图像，其中 10K 张用于测试. 与以上两个数据集不同，本数据集相对而言更难以分类，并且更贴近真实应用中的图像采集清晰度. 与 CIFAR-100 相同，在标签传染操作的模型训练过程中 κ 采用默认值. 在半监督训练过程中，我们选用 2 种已在此数据集上经过验证的 SSL 算法框架[11,30]进行针对性测试与对比. 为了突出本文对于极少标签条件下的优越表现，我们将标签样本总数分别设置为 100、400、1K、4K 及 10K（$\kappa=10000/C$）进行测试，并且同时选用了 WRN-28-2 及 ResNet-18 作为骨干网络模型进行公平比较，实验结果取 3 次随机运行结果的均值与标准差进行展示，如表 5 所示.

表 5 ReLSL 算法及最新算法在 Mini-ImageNet 上测试误差率对比 （单位：%）

方法	WRN-28-2				ResNet-18	
	100	400	1K	4K	4K	10K
MT[20]	—	—	—	—	72.51±0.22	57.55±1.11
MT+LP[18]				—	72.78±0.15	**57.35±1.66**
LP[18]	—	—	—	—	**70.29±0.81**	57.58±1.47
ReLaB[26]	**81.50±0.73**	**69.25±0.78**	**62.18±0.92**	**48.53±0.58**	—	—
PL[11]	90.89±0.62	85.00±0.94	75.47±0.52	**48.53±0.58**	56.49±0.51	**46.08±0.11**
ReLSL+PL	**79.11±0.64**	**68.89±0.96**	**61.78±0.83**	48.89±0.60	**55.78±0.52**	46.94±0.44
FMCmatch[14]	—	—	—	—	52.79±0.30	**41.25±0.11**
ReLSL+FMCmatch	—	—	—	—	**52.53±0.44**	41.61±0.13

依据现有相关工作，表 5 实验中运用两个骨干网络，即 WRN-28-2 与 ResNet-18 展开相关实验. 其中 WRN-28-2 用于极少标签条件下的对比实验，ResNet-18 主要用于常规半监督条件下的性能检测. 由表 5 可知，在极少标签条件下，本文方法达到了目前针对该数据集半监督分类问题的最佳性能. 而同样地，随着标签数目的增多，ReLSL 作用并不明显. 这里需要强调，本文方法中的超参数设置几乎是完全固定的，而针对更为复杂的数据集进行超参数调优将会获得更显著的效果提升.

4.5 STL-10 数据集测试结果

STL-10 数据集仍采样自 ImageNet，包含 5K 张分辨率为 96×96 的 10 类有标签训练数据，100K 张无标签数据以及 8K 张测试数据. 为了公平比较，我们沿用文献[14]中的数据划分及骨干网络超参数设置，选用 WRN-37-2(5.9M)网络及 1K 标签样本进行测试. 由于 STL-10 原始标签样本总数仅为 5K，为此，本实验中将 κC 设置为 2K 以与无标签筛选的学习过程相区分. 此外，由于额外的 100K 无标签数据样本具有 10 类以外的类别数据，因此，在伪标签学习与标定过程中并不对这部分数据进行处理. 实验结果如表 6 所示.

表 6 ReLSL 算法及最新算法在 STL-10 测试误差率对比 （单位：%）

方法	测试误差率
Π model[9]	26.23±0.82
Pseudo-Labeling[12]	27.99±0.80
FixMatch[14]	7.98±1.50
ReLSL+FixMatch	**7.61±1.29**
RMM[16]	5.23±0.45
ReLSL+RMM	**5.20±0.44**

由表 6 可知，在 1K 标记条件下，本文方法在原有 RMM 及 FixMatch 模型效果基础上均有所提

升.同样需要强调的，由于本文所述半监督学习方法在超参数设置上并没有经过大量的网格搜索与测试，且相关骨干对比模型中的所有超参数设置均与对比实验保持原状，因此，本文算法在有效性上具有保障，且性能仍具有一定的提升空间.

4.6　SVHN 数据集测试结果

SVHN 数据集采集自街道门牌号，经过切割等处理后，形成 0 至 9 共 10 类数字.数据集共包含 73257 张分辨率为 32×32 的训练数据以及 26032 张测试数据.相较于前三个数据集，SVHN 上的学习任务相对容易.在半监督训练过程中，我们选用 2 种 SSL 算法框架[16,30]进行针对性测试与对比.为了突出本文对于各种半监督条件下的优越表现以及比较的公平性，我们将标签样本总数分别设置为 40、250、500、1K 进行测试，并且同时选用了 CNN-13 及 WRN-28-2 作为骨干网络模型，实验结果如表 7 所示.

表 7　ReLSL 算法及最新算法在 SVHN 上测试误差率对比　（单位：%）

方法	CNN-13			WRN-28-2 (1.5M)		
	250	500	1K	40	250	1K
Π model[9]	—	6.65±0.53	4.82±0.17	—	18.96±1.92	7.54±0.36
MT[20]	4.35±0.50	4.18±0.27	3.95±0.19	—	**3.57±0.11**	3.42±0.07
SNTG[36]	4.29±0.23	3.99±0.24	3.86±0.27	—	—	—
ICT[22]	4.78±0.68	4.23±0.15	3.89±0.04	—	—	7.66±0.17
ISL-GAN[25]	—	**3.59±0.20**	3.48±0.08	—	—	—
MT-TSSDL[24]	4.09±0.42	3.90±0.27	**3.35±0.27**	—	—	—
MPL[28]	—	—	—	—	—	**1.99±0.07**
UDA[13]	—	—	—	52.63±20.51	5.69±2.76	2.46±0.24
MixMatch[29]	**3.59**	—	3.39	42.55±14.53	3.98±0.23	3.50±0.28
FMCmatch[30]	3.39±0.13	3.38±0.07	**3.18±0.08**	—	3.94±0.11	**2.90±0.19**
ReLSL＋FMCmatch	**3.34±0.14**	**3.34±0.10**	3.23±0.08	—	**3.92±0.11**	3.01±0.07
RMM[16]	—	—	—	3.34±0.20	**2.92±0.48**	**2.65±0.08**
ReLSL＋RMM	—	—	—	**3.16±0.25**	3.00±0.28	2.69±0.09

由表 7 可以观察到，本文算法对现有基线模型算法的提升并不明显.主要原因在于 SVHN 涉及数字识别任务，相较于物体识别更为简单，在目前强数据增强技术的推动下，仅 40 个标签样本的半监督条件下 RMM 模型的错误率已降至 3.34，而无论是标签传染还是错误平滑操作，其作用并不明显.

4.7　消融实验分析

为了验证本文针对极少标签条件下半监督深度学习问题所提出的三项创新点的有效性，本节将进行消融实验，结果仍由 3 次随机运行的测试错误率取均值及标准差进行展示，见表 8.考虑到本文涉及实验的数量庞大，此节仅关注在 CIFAR-10 上共 40 个标签样本的极少标签条件下半监督学习表现，骨干网络模型选择 FMCmatch 下的 WRN-28-2.具体地，除原始 ReLSL＋FMCmatch 外，我们将探讨：

(1) 去除标签传染及伪标签学习与标定步骤，表示为 ReLSL w/o PL；

(2) 原始 Small-Loss 机制，表示为 Small-Loss；

(3) 去除式(5)中的一致性惩罚项，即 $loss_{ce+}=Loss_{ce}$，表示为 ReLSL w/o CT；

(4) 去除式(6)中的方差项，表示为 ReLSL w/o std^2；

(5) 在半监督学习过程中去除标签平滑策略，即 $\tau=0$，表示为 ReLSL w/o LS；

(6) 在半监督学习过程中去除均值偏移校正策略，即 $\sigma=0$，表示为 ReLSL w/o MSC.

表 8　CIFAR-10 100 标签样本下 ReLSL 算法消融实验结果

方法	错误率
FMCmatch	23.59±7.45
ReLSL w/o PL	19.63±0.76
Small-Loss	8.51±0.58
ReLSL w/o CT	7.90±0.42
ReLSL w/o std^2	7.43±0.37
ReLSL w/o LS	7.25±0.31
ReLSL w/o MSC	7.39±0.39
ReLSL＋FMCmatch	**6.91±0.38**

由表 8 可知，本文算法框架中所提出的三个创新点在模型错误率下降上均有贡献.具体地，由 ReLSL w/o PL 结果可知，伪标签学习与标定策略对 ReLSL 算法模型在极少标签条件下半监督学习的效果提升最为明显.其原因在于无监督特征提取能更大限度地获得样本特征，而基于图的标签传染可对无标签样本进行初步标定，针对 Small-Loss 的改进标定策略可进一步挑选出综合考虑标签正确性及信息量的无标签样本进行伪标记.此外，表 8 中 ReLSL w/o LS 及 ReLSL w/o MSC 相较于最终版本的 ReLSL＋FMCmatch 均有一定准确率的退化，其中 MSC 策略影响更为显著.与此同时，ReLSL

w/o PL 相较于原始 FMCmatch 也有着错误率的下降,从而进一步证明 LS 及 MSC 创新策略的有效性.

此外,在算法复杂度方面,相较于端到端的基线模型 FMCmatch,本文算法 ReLSL+FMCmatch 添加了"特征提取与标签传染"以及"伪标签学习与标定"两个额外训练模块,算法复杂度相对较高.其中,在特征提取阶段,本文遵循文献[17]的训练方式.需要注意的是,由于本文工作更注重伪标签的学习及半监督学习阶段,因此,在特征提取器的训练中对每一类数据集仅需训练一次特征提取网络.其次,标签传染过程式(1)~(3)实际无需采用反向传播形式进行训练,因此该过程复杂度忽略不计.再次,在伪标签学习与标定阶段,相较于 Small-Loss 方式,由于本文需要计算 $\phi(\boldsymbol{x}_i)-\phi(\hat{\boldsymbol{x}}_i)$,因此时间复杂度大致增加一倍,但考虑到此步骤中训练 epoch 数较少,实际总时间消耗仅约为 30 min(RTX 2080 Ti).最后,在半监督模型训练阶段,本文并未对骨干网络模型做任何修改,而仅增加了 LS 及 MSC 训练策略,经过相关消融实验证实,其额外时间消耗相较于反向传播而言亦可忽略不计.

5 总结与展望

本文提出了一种可靠标签选择与学习算法 ReLSL,用于在极少量标签数据条件下进行有效的半监督深度学习.通过所提出的综合考虑样本输出均值及方差伪标签标定策略、标签平滑策略以及均值偏移校正策略,在现有最新网络模型的基础上,ReLSL 极大地降低了在极少标签图像数据条件下的半监督学习测试错误率.具体地,通过在被广泛测试的 CIFAR-10/100、SVHN、STL-10、Mini-ImageNet 数据集及 CNN-13、WRN-28、ResNet-18 骨干网络上的综合实验结果表明,本文所提出的算法在极少标签条件下的半监督学习效果相较于对比实验均有着显著的提升.与此同时,ReLSL 算法在一般半监督学习条件下的学习效果也有着出色的表现.

本文所提出的算法框架仍有待进一步优化,并且其应用场景有待进一步拓展.在未来的工作中,我们将着重探索并改进算法的整体框架,探索更可靠的无监督特征提取算法,以期构造为单阶段的端到端学习模式,从而在提高模型准确率的同时有效减少算法运行复杂度.考虑到半监督深度学习广阔的应用场景,本研究将对模型的有效性在诸如 ImageNet、COCO 等大数据集上进行有效性测试,并尝试将相关算法应用于诸如医学影像异常检测、满文识别、列车故障检测等数据集庞大但标注困难的任务中.

致 谢 感谢都柏林城市大学的 Albert 团队提供代码支持,感谢谷歌公司团队对数据及代码的共享!

参 考 文 献

[1] He K, Zhang X, Ren S, et al. Deep residual learning for image recognition//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Las Vegas, USA, 2016: 770-778

[2] Zagoruyko S, Komodakis N. Wide residual networks. arXiv preprint arXiv:1605.07146, 2016

[3] Zhou Fei-Yan, Jin Lin-Peng, Dong Jun. Review of Convolutional neural network. Chinese Journal of Computers, 2017, 40(6): 1229-1251(in Chinese)
(周飞燕, 金林鹏, 董军. 卷积神经网络研究综述. 计算机学报, 2017, 40(6): 1229-1251)

[4] Liu Jian-Wei, Liu Yuan, Luo Xiong-Lin. Semi-supervised learning methods. Chinese Journal of Computers, 2015, 38(8): 1592-1617(in Chinese)
(刘建伟, 刘媛, 罗雄麟. 半监督学习方法. 计算机学报, 2015, 38(8): 1592-1617)

[5] Liu Shao-Peng, Hong Jia-Ming, Liang Jie-Peng, et al. Medical image segmentation using semi-supervised conditional generative adversarial nets. Journal of Software, 2020, 31(8): 2588-2602(in Chinese)
(刘少鹏, 洪佳明, 梁杰鹏等. 面向医学图像分割的半监督条件生成对抗网络. 软件学报, 2020, 31(8): 2588-2602)

[6] Huang J M, Wai R J, Yang G J. Design of hybrid artificial bee colony algorithm and semi-supervised extreme learning machine for PV fault diagnoses by considering dust impact. IEEE Transactions on Power Electronics, 2019, 35(7): 7086-7099

[7] Kuznietsov Y, Stuckler J, Leibe B. Semi-supervised deep learning for monocular depth map prediction//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Honolulu, USA, 2017: 6647-6655

[8] Sajjadi M, Javanmardi M, Tasdizen T. Regularization with stochastic transformations and perturbations for deep semi-supervised learning//Proceedings of the Neural Information Processing Systems (NeurIPS). Barcelona, Spain, 2016: 1171-1179

[9] Laine S, Aila T. Temporal ensembling for semi-supervised learning//Proceedings of the International Conference on Learning Representations (ICLR). San Juan, Puerto Rico, 2016: 1-13

[10] Wei X, Gong B, Liu Z, et al. Improving the improved training of Wasserstein GANs: A consistency term and its dual effect//Proceedings of the International Conference on Learning Representations (ICLR). Vancouver, Canada, 2018: 1-13

[11] Arazo E, Ortego D, Albert P, et al. Pseudo-labeling and confirmation bias in deep semi-supervised learning//Proceedings of the International Joint Conference on Neural Networks (IJCNN). Shenzhen, China, 2020: 1-8

[12] Lee D H. Pseudo-label: The simple and efficient semi-supervised learning method for deep neural networks//Proceedings of the International Conference on Machine Learning Workshop on Challenges in Representation Learning. Atlanta, USA, 2013: 1-6

[13] Xie Q, Dai Z, Hovy E, et al. Unsupervised data augmentation for consistency training//Proceedings of the Neural Information Processing Systems (NeurIPS). Virtual, 2020: 1-20

[14] Sohn K, Berthelot D, Li C L, et al. FixMatch: Simplifying semi-supervised learning with consistency and confidence//Proceedings of the Neural Information Processing Systems (NeurIPS). Virtual, 2020: 1-14

[15] Zhang H, Cisse M, Dauphin Y N, et al. Mixup: Beyond empirical risk minimization//Proceedings of the International Conference on Learning Representations (ICLR). Vancouver, Canada, 2018: 1-13

[16] Berthelot D, Carlini N, Cubuk E D, et al. ReMixMatch: Semi-supervised learning with distribution alignment and augmentation anchoring//Proceedings of the International Conference on Learning Representations (ICLR). Virtual, 2020: 1-13

[17] Huang J, Dong Q, Gong S, et al. Unsupervised deep learning by neighbourhood discovery//Proceedings of the International Conference on Machine Learning (ICML). Long Beach, USA, 2019: 2849-2858

[18] Iscen A, Tolias G, Avrithis Y, et al. Label propagation for deep semi-supervised learning//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). Long Beach, USA, 2019: 5070-5079

[19] Arazo E, Ortego D, Albert P, et al. Unsupervised label noise modeling and loss correction//Proceedings of the International Conference on Machine Learning (ICML). Long Beach, USA, 2019: 312-321

[20] Tarvainen A, Valpola H. Mean teachers are better role models: Weight-averaged consistency targets improve semi-supervised deep learning results//Proceedings of the Neural Information Processing Systems (NeurIPS). Long Beach, USA, 2017: 1195-1204

[21] Miyato T, Maeda S, Koyama M, et al. Virtual adversarial training: A regularization method for supervised and semi-supervised learning. IEEE transactions on Pattern Analysis and Machine Intelligence, 2018, 41(8): 1979-1993

[22] Verma V, Lamb A, Kannala J, et al. Interpolation consistency training for semi-supervised learning//Proceedings of the 28th International Joint Conference on Artificial Intelligence (IJCAI). Macao, China, 2019: 3635-3641

[23] Radford A, Metz L, Chintala S. Unsupervised representation learning with deep convolutional generative adversarial networks//Proceedings of the International Conference on Learning Representations (ICLR). San Diego, USA, 2016: 1-16

[24] Shi W, Gong Y, Ding C, et al. Transductive semi-supervised deep learning using min-max features//Proceedings of the European Conference on Computer Vision (ECCV). Munich, Germany, 2018: 299-315

[25] Wei Xiaotao, Wei Xiang, Xing Weiwe, et al. An incremental self-labeling strategy for semi-supervised deep learning based on generative adversarial networks. IEEE Access, 2020, 8: 8913-8921

[26] Albert P, Ortego D, Arazo E, et al. ReLaB: Reliable label bootstrapping for semi-supervised learning. arXiv preprint arXiv:2007.11866v1, 2020

[27] Chen T, Kornblith S, Swersky K, et al. Big self-supervised models are strong semi-supervised learners//Proceedings of the Neural Information Processing Systems (NeurIPS). Virtual, 2020: 1-14

[28] Pham H, Xie Q, Dai Z, et al. Meta pseudo labels. arXiv preprint arXiv:2003.10580, 2020

[29] Berthelot D, Carlini N, Goodfellow I, et al. MixMatch: A holistic approach to semi-supervised learning//Proceedings of the Neural Information Processing Systems (NeurIPS). Vancouver, Canada, 2019: 5050-5060

[30] Wei Xiang, Wei Xiaotao, Kong Xiangyuan, et al. FMixCutMatch for semi-supervised deep learning. Neural Networks, 2021, 133: 166-176

[31] Harris E, Marcu A, Painter M, et al. FMix: Enhancing mixed sample data augmentation. arXiv preprint arXiv:2002.12047, 2020

[32] DeVries T, Taylor G W. Improved regularization of convolutional neural networks with cutout. arXiv preprint arXiv: 1708.04552, 2017

[33] Cubuk E D, Zoph B, Shlens J, et al. RandAugment: Practical automated data augmentation with a reduced search space//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops. Seattle, USA, 2020: 3008-3017

[34] Zhou D, Bousquet O, Lal T N, et al. Learning with local and global consistency//Proceedings of the Neural Information Processing Systems (NeurIPS). Vancouver and Whistler, Canada, 2003: 321-328

[35] Hinton G, Vinyals O, Dean J. Distilling the knowledge in a neural network. arXiv:1503.02531, 2015

[36] Luo Y, Zhu J, Li M, et al. Smooth neighbors on teacher graphs for semi-supervised learning//Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition. Salt Lake City, USA, 2018: 8896-8905

[37] Athiwaratkun B, Finzi M, Izmailov P, et al. There are many consistent explanations of unlabeled data: Why you should average//Proceedings of the International Conference on Learning Representations (ICLR). New Orleans, USA, 2019: 1-22

[38] Rizve M N, Duarte K, Rawat Y S, et al. In defense of pseudo-labeling: An uncertainty-aware pseudo-label selection framework for semi-supervised learning. arXiv preprint arXiv:2101.06329, 2021

[39] Zhou T, Wang S, Bilmes J. Time-consistent self-supervision for semi-supervised learning//Proceedings of the International Conference on Machine Learning (ICML). Virtual, 2020: 11523-11533

WEI Xiang, Ph. D., lecturer. His main research interests include semi-supervised deep learning and robust deep learning.

WANG Jing-Jie, M. S. candidate. His main research interests include semi-supervised deep learning and computer vision.

ZHANG Shun-Li, Ph. D., associate professor. His main research interests include visual tracking, machine learning, and deep learning.

ZHANG Di, Ph. D., associate professor. His main research interests include edge intelligence, pervasive computing, mobile networks and systems.

ZHANG Jian, Ph. D., lecturer. His main research interests include intelligent transportation, machine learning, and pattern recognition.

WEI Xiao-Tao, Ph. D., associate professor. His main research interests include intelligent information processing and machine learning.

Background

Deep learning typically requires a large amount of labeled data to make fully supervised learning. However, labeling data is an expensive process for every new task, and fully exploiting unlabeled data to assist deep learning has been an important research direction to address this issue. Semi-supervised learning (SSL) provides a way to improve a model's performance with unlabeled data when only limited labeled data are available.

However, when the labeled data is extremely scarce, the performance of the existing SSL algorithms can be severely affected. The problem is usually manifested as: the initial informative information for classification is extremely limited, the model faces cold-start problem; In the process of training, the proportion of pseudo-label noise is difficult to control and the model has a much larger potential risk to be collapsed.

This paper addresses the problem of semi-supervised deep learning under the extremely scarce labeled condition. Through introducing ReLSL, a reliable label selection and learning framework, we further narrow the gap between the accuracy of semi-supervised learning with scarce labeled condition and fully supervised learning. In brief, we exploit synergies among unsupervised learning, SSL and robust learning to bootstrap additional reliable labels for robust network training. For the unsupervised learning, it is used to ease the problem of cold-start under scarce labeled conditions. For SSL and robust learning, they are used to obtain good learning performance in the presence of noise labels. As a result, the proposed ReLSL achieves state-of-the-art performance on CIFAR-10/100, SVHN, STL-10 and Mini-ImageNet across a variety of SSL conditions with the CNN-13, WRN-28-2 and ResNet-18 networks.

This work is supported by the National Natural Science Foundation of China under grant No. 61906014, whose name is "Research on Semi-supervised Deep Learning and Dual-network Ensemble based Object Tracking". In this project, we focus on the in-depth research on semi-supervised deep learning and object tracking technologies, so as to improve the robustness, stability and accuracy of the object tracking model. Besides, this work is supported by the National Natural Science Foundation of China under grant Nos. 61976017 and 61902019, the Natural Science Foundation of Beijing under grant No. 4202056.

Our research team has done a lot research on semi-supervised learning and its corresponding applications. Related works have been published in ICLR, ACM Multimedia, IEEE TMM, IEEE TNNLS, IEEE Transactions on Mobile Computing, Neural Networks etc.