摘要

智慧城市能够促进城市精细化运作，提升人民幸福感和城市竞争力，对国家和社会发展的意义重大。数字视网膜是智慧城市建设中必不可少的智能系统，通过在前端摄像装置完成数据智能化解析来平衡云边两侧的成本与效率关系，但是系统中视频数据分析模型的建立存在数据传输和隐私泄露等问题。联邦学习是一种面向隐私保护的分布式学习技术，将联邦学习应用于数字视网膜系统能够缓解这些问题，同时提升模型的泛化性和鲁棒性，因此联邦学习对数字视网膜系统建立具有重要意义。

然而，数字视网膜系统中的数据集偏移问题给联邦学习方法带来了本地模型偏移和全局模型偏移的问题。具体地，联邦学习应用于数字视网膜时需要摄像设备使用自身采集的数据训练本地模型，由于环境限制采集的数据与模型部署时的测试数据分布不一致，摄像设备上的数据集偏移将造成本地模型偏移。进一步地，联邦学习通过汇总本地模型的学习成果更新全局模型，因此数据集偏移将通过本地模型进一步引发全局模型偏移。本地模型和全局模型相互影响，最终使得模型性能低下。此外，真实场景下摄像设备采集数据的分布复杂多变，而数据隐私保护约束下采集数据分布未知，因此难以针对数据分布特性设计联邦学习方法。

针对上述的本地模型偏移、全局模型偏移两方面挑战，本文从一般数据集偏移下的本地模型学习优化、长尾分布下的本地模型学习优化、全局模型更新优化这三个角度出发，研究面向数据集偏移的联邦学习方法，从而完成数字视网膜系统中视频分析模型的建立。此外，针对数据隐私保护下的联邦学习方法设计困难，从数据贡献评估角度出发初步完成对本地模型训练数据的分析。本文的贡献包括以下四个方面：

- 针对一般性数据集偏移引发的本地模型偏移问题，提出了一种基于层次对齐的本地模型学习方法，对各本地模型在潜在特征空间和任务目标空间的输出响应进行对齐。首先设计对抗学习机制并设计统一对抗损失，对齐各本地模型提取的数据潜在特征。之后基于迁移学习技术设计组共识损失和全局共识损失，分别在本地模型之间和本地模型与全局模型之间建立统一预测值，以实现预测值对齐。实验结果表明，该方法显著提高了数据集偏移场景下的模型性能，在 VeRI776、MSMT17 和 Market1501 数据集上分别提升了 1.22% mAP，1.15% mAP 和 1.52% mAP，在 CUB200 数据集上提高了 4.83% 的分类准确率。
- 针对长尾分布下的本地模型偏移问题，提出一种基于自适应数据增强的集成式本地模型学习方法，平衡本地模型对头部类和尾部类的学习程度。具体地，设计了一种基于细粒度数据簇的集成学习方法，将本地数据划分为头部类占比不同

的多个数据簇并训练多个模型，最后集成所有模型作为本地模型，从而加强本地模型对尾部类的学习。为了解决数据簇的数据数量较少和不均衡的问题，设计了聚焦尾部类的自适应数据增强方法，通过结合数据簇分布自适应地调整尾部类生成概率并提升尾部类数据的比重。实验显示，该方法在 CIFAR10，CIFAR100 和 Tiny-ImageNet 上取得了 1.54%，2.53% 和 1.88% 的分类准确率提升，在车辆分类数据集 MIO-TCD 和 CompCars 上的分类准确率提升了 1.13% 和 1.72%。

- 针对本地模型偏移引发的全局模型偏移问题，提出一种基于知识蒸馏的全局模型学习方法，从知识的角度汇总本地模型学习成果，提升全局模型更新的鲁棒性。该方法设计集成式知识蒸馏技术，促使全局模型学习各本地模型目标输出空间以实现全局模型更新。进一步地，为了弥补服务器缺少训练数据的问题，设计语义损失和分散损失训练数据生成器，并提出基于对抗学习的难样本挖掘来提升生成数据的学习难度，从而提升知识蒸馏的效率。实验显示，该方法在 CIFAR10 和 CIFAR100 实现了 2.24% 和 3.62% 的分类准确率提升，在车辆分类数据集 MIO-TCD 和 CompCars 上实现了 0.69% 和 1.39% 的分类准确率提升。
- 针对隐私保护下的模型学习方法设计困难，提出一种基于类级边际收益的数据贡献评估方法，完成对本地模型训练数据的初步分析。首先提出类关联的评估模型将数据贡献分解为细粒度类级贡献，通过开展类自适应评估降低类别分布差异的负面影响。进一步地，从边际收益角度设计了节点数据对模型性能影响的量化指标，并结合模型性能变化规律与小规模数据评估鲁棒性需求，设计了基于预测损失和均值损失的数据贡献转换模型。该方法在满足数据隐私要求的前提下，利用模型性能完成节点数据到数据贡献的评估映射，以辅助联邦学习方法的设计。实验显示，在 DukeMTMC-reID 和 VeRI776 数据集上，该方法的评估准确性优于现有方法一个数量级，在 CUB200 上，该方法的评估时间可缩短至对比方法的 10%。

综上所述，为促进联邦学习在数字视网膜系统中的应用，加速数字视网膜技术发展，本文对数据集偏移场景下的联邦学习方法展开探索。针对数据集偏移造成的本地模型偏移和全局模型偏移问题，提出了一种基于层次对齐的本地模型学习方法、一种基于自适应数据增强的集成式本地模型学习方法和一种基于知识蒸馏的全局模型学习方法。针对数据隐私保护下的联邦学习方法设计困难，提出了一种基于类级边际收益的数据贡献评估方法。实验表明提出的方法在各任务中均表现出显著性能优势，验证了本文研究路线的优越性。本文主要研究成果以第一作者身份发表于计算机视觉领域顶级国际会议 ICCV、CVPR。

关键词：联邦学习，数据集偏移，智慧城市，隐私保护