计算机科学
COMPUTER SCIENCE

联邦学习在医学图像处理任务中的研究综述

刘育铭, 代煜, 陈公平

引用本文

刘育铭, 代煜, 陈公平. 联邦学习在医学图像处理任务中的研究综述[J]. 计算机科学, 2025, 52(1): 183-193.

LIU Yuming, DAI Yu, CHEN Gongping. Review of Federated Learning in Medical Image Processing[J]. Computer Science, 2025, 52(1): 183-193.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231200057

联邦学习在医学图像处理任务中的研究综述

刘育铭　代　煜　陈公平
南开大学人工智能学院　天津 300350
(2120220517@mail.nankai.edu.cn)

摘　要　在医学领域,由于患者隐私问题,图像很难集中收集和标注,这给深度学习模型的训练和部署带来了较大困难。联邦学习作为一种能有效保护数据隐私的分布式学习框架,能够在参与方不共享数据的基础上进行联合建模,从技术上打破数据孤岛,其凭借这些优势在许多行业已经得到广泛应用。由于与医学图像处理的需求高度契合,近年来也涌现出许多应用于医学图像处理的联邦学习研究,然而大部分新的方法仍未被归纳分析,不利于后续的进一步探索。文中对联邦学习进行了简单的介绍,列举了其在医学图像处理方面的部分应用,并根据改进的方向对目前已有的研究进行了分类总结。最后,讨论了目前医学图像方向联邦学习所面临的问题和挑战,并对未来的研究方向进行了展望,希望给后续研究提供一定的帮助。

关键词:联邦学习;医学图像;深度学习;图像处理;分布式学习;隐私保护
中图分类号　TP391

Review of Federated Learning in Medical Image Processing

LIU Yuming,DAI Yu and CHEN Gongping
College of Artificial Intelligence,Nankai University,Tianjin 300350,China

Abstract　In the medical field,due to patient privacy concerns,it is difficult to collect and label images,which brings great difficulties to the training and deployment of deep learning models. As a distributed learning framework that can effectively protect data privacy,federated learning can conduct joint modeling on the basis that participants do not share data,and technically break the data island. With these advantages,it has been widely used in many industries. Due to the high degree of compliance with the needs of medical image processing,many federated learning research works applied to medical image processing have emerged in recent years. However,most of the new methods have not been summarized and analyzed,which is not conducive to further exploration. This paper gives a brief introduction to federated learning,lists some of its applications in medical image processing,and classifies and summarizes the existing research according to the improvement direction. Finally,the problems and challenges of federated learning in medical image are discussed,and future research directions are prospected,hoping to provide some help for subsequent research.

Keywords　Federated learning,Medical image,Deep learning,Image processing,Distributed learning,Privacy protection

1　引言

随着深度学习的引入,计算机视觉取得了巨大进步。由于骨干网络(如 AlexNet[1],VGG[2],ResNet[3]等)的迭代升级和快速发展,卷积神经网络在目标检测、分类和分割等视觉任务中展现出越来越强大的性能。与此同时,在自然语言处理方面表现出色的 Transformer[4]也被运用到图像处理问题中。最近的研究表明,视觉 Transformer[5]由于强大的建模能力和较好的可解释性,在 ImageNet[6],CIFAR-10[7]和 ADE20K[8]等多个基准数据集上取得了优异的效果。

基于深度学习的医学图像分析近年来也受到越来越多的关注,并在许多研究中取得了成功[9-12],这些成功在很大程度上归功于构建大规模医学图像数据集的重大努力。然而,理想的大型数据集在实际应用中往往很难实现。首先,部分模态的医学图像(如 CT)占用的存储空间较大,给数据传输和储存带来了困难;其次,医疗数据包含许多敏感的个人信息,在学习过程中共享患者数据往往存在法律或道德障碍;再次,医院或研究机构所掌握的医学图像具有较高的科研和教学价值,对于合作机构之外的第三方不会直接共享,而促成多方合作难度很大;最后,由于不同仪器成像协议及图像模态不同,各机构之间的数据具有一定的异构性,因此很难得到一个完备可靠的大型医疗图像数据集以供模型训练。

到稿日期:2023-12-07　返修日期:2024-05-07
基金项目:国家自然科学基金(U1913207);天津市研究生科研创新项目(2022BKY004)
This work was supported by the National Natural Science Foundation of China(U1913207)and Tianjin Research Innovation Project for Postgraduate Students(2022BKY004).
通信作者:代煜(daiyu@nankai.edu.cn)

为了解决上述问题，一种通用的方法是首先在大型自然图像数据集上进行预训练，然后将带有预训练权重的模型在特定的医学图像处理任务上进行进一步训练和调整。但正如我们所知，由于成像原理等方面的差异，通用的自然图像数据集与医疗数据之间存在较大的领域偏差，上述预训练方法可能并不能有效地提升模型性能。例如，Segment Anything Model(SAM)[13]代表了图像分割领域较为先进的研究进展，然而，由于缺少医疗领域的专业知识，直接将预训练的 SAM 应用于医学图像分割，效果并不理想。另一种方法是进行分布式训练。分布式训练最初的目的是解决数据过大和算力不足的问题，以提高训练效率，方法通常是将数据集平均拆分成多个部分分布到不同的节点上。由于数据集是向下拆分，因此各节点上的数据是同分布的。但在实际情况中，由于成像设备不同和标注质量参差不齐，医学图像在不同医院和临床研究中的质量存在很大差异，很难满足独立同分布数据的假设，另外，数据的上传和下载也是不被允许的。

与传统的分布式学习不同，Google 于 2017 年提出的联邦学习[14]使得不同数据集的数据异质性、大小不平衡等问题都能很好地解决。此外，服务器和本地客户端站点之间的传输也仅限于参数和权重，它允许研究人员在不破坏数据所有权的情况下应用机器学习方法，能够很好地保护本地机构的数据隐私。因此在过去几年中，出现了大量对联邦学习的研究和应用。

鉴于联邦学习和医疗数据处理的高度契合，越来越多的研究人员开始关注基于联邦学习的医学图像处理。因此，我们认为回顾医学图像处理任务下的联邦学习先进技术是有必要的。为此，本文从不同的创新角度对联邦学习在医学图像处理中的应用进行了分类和总结，希望本文能够作为已有研究工作的一个快速参考，为解决相关问题和进行特定研究提供指导。

本文第 2 章简单介绍了联邦学习；第 3 章从原始方法以及算法、框架和隐私保护机制 3 个方面的改进对已有的研究工作进行了分析总结；第 4 章分析了联邦学习在医学图像处理任务中存在的问题和挑战，并探索了未来的研究方向；最后总结全文。

2 联邦学习

2.1 联邦学习概述

联邦学习是 Google 提出的带有隐私保护、安全加密技术的分布式机器学习范式，能有效帮助多个分散的机构在满足数据安全和政府法规的要求下，协作进行数据使用和机器学习建模，如图 1 所示。

标准的联邦学习训练过程如下：

1)在全局服务器处初始化模型，并将该全局模型的权重传递给每个本地客户端站点；

2)每个客户端站点在各自数据集上训练模型的本地版本，将更新后的权重发送给全局服务器；

3)全局服务器汇总接收各个客户端上传的权重并进行聚合，对全局模型进行更新；

4)将更新后的全局模型权重参数传递给参与训练的客户端。

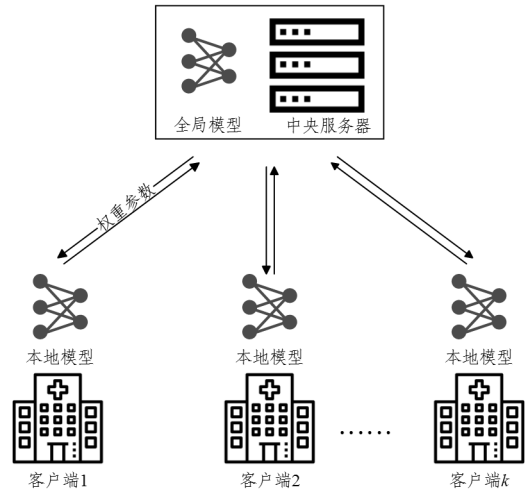


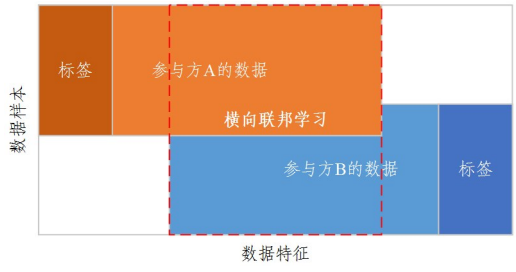
图 1 联邦学习架构

Fig. 1 Architecture of federated learning

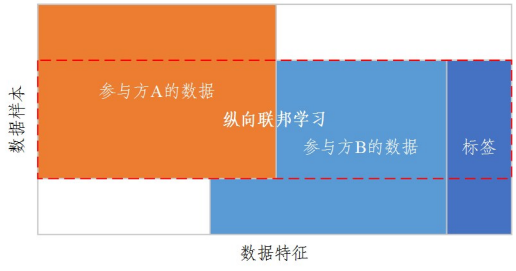
在联邦学习训练期间，重复上述步骤多轮直至全局模型收敛达到预期的性能。在此过程中，所有用于训练的数据严格保存在本地，服务器与客户端之间的信息传递仅限于模型权重，让参与方能够在不共享数据的基础上协作训练，有效解决了数据孤岛问题。

2.2 联邦学习分类

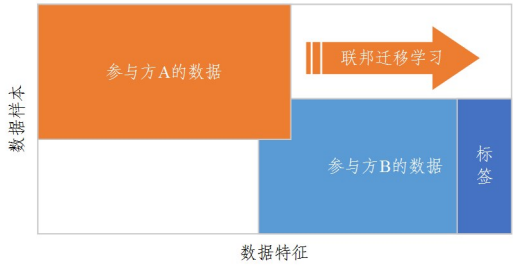
联邦学习基于数据特点可以分为 3 个主要的子类：横向联邦学习、纵向联邦学习和联邦迁移学习。如图 2 所示。



(a)横向联邦学习



(b)纵向联邦学习



(c)联邦迁移学习

图 2 联邦学习分类

Fig. 2 Federated learning classification

在横向联邦学习中，每个数据集中有不同的样本，但这些样本的特征是相似的，将数据按特征对齐进行选取，能有效增加训练样本数量；在纵向联邦学习中，数据集样本重叠较多但特征相似性小，按样本对齐数据，取出样本相同但样本特征不完全相同的部分数据进行训练，能够增加训练数据特征维数；联邦迁移学习则适用于样本和数据都重叠较少的情况，使用迁移学习可以解决数据量小或标签缺乏的问题。

针对医学图像的研究主要以横向联邦学习为主，利用不同医疗机构的同种数据集进行联邦训练，以达到增大整体数据集容量的目的。另外，在一部分针对疾病分析和诊断报告生成的研究中也应用到了纵向联邦学习，综合考虑同一患者的不同诊断信息以给出更全面、准确的判断。

2.3 应用实例

联邦学习一经问世就受到了业界的高度重视，由谷歌(TensorFlow Federated)[14]、微众银行(FATE)[15]、OpenMined(Pysyft)[16]等牵头开发了多个开源框架。

作为一种创新的建模机制，它可以在不损害数据保密性和安全性的情况下，针对多方数据训练统一模型，因此联邦学习在销售、金融和许多其他行业中有广阔的发展前景，这些行业中的数据由于诸多因素(如知识产权、隐私保护和数据安全之类)而无法直接汇总用于训练。

医学图像处理是我们预计将受益于联邦学习技术的兴起的另一个领域。医学数据非常敏感和私密，其收集难度大，并且存在于孤立的医学中心和医院中。数据和标签不足导致机器学习模型的性能不尽人意，成为当前医学图像处理的瓶颈。我们设想，如果所有医疗机构联合起来并共享其数据以形成一个大型医疗数据集，那么在该大型医疗数据集上训练的机器学习模型的性能将得到显著提高。联邦学习与迁移学习相结合是实现此愿景的主要方法，可以应用转移学习来填补缺失的标签，从而扩大可用数据的规模，并进一步提高训练模型的性能。因此，联邦迁移学习将在医学图像处理的发展中发挥关键作用，并且可能将医学图像处理提升到一个全新的水平。

目前在联邦学习的帮助下，已经开发出了一些医疗机构合作的大型项目。2019 年 10 月，英伟达将联邦学习技术引入针对医学图像领域的 Clara 平台，并与英国伦敦国王学院合作发布了用于医学影像分析的联邦学习系统，并于次年 9 月与麻省总医院等联合通过联邦学习在真实协作环境中训练医学影像模型，用于乳腺 BI-RADS 分类辅助判断[17]，又在新冠肺炎肆虐期间联合分布在各大洲的 20 家医院，借助患者胸部 X 光片训练模型分析预测氧气用量。腾讯天衍实验室和微众银行在医学影像辅助诊断等领域展开合作，联合开发了基于医疗联邦学习框架的“脑卒中发病风险预测模型”[18]，该模型预测病人脑卒中发病风险准确率可达 80%。不少机构和团队仍在进行相应的探索，力求将其应用到具体的医疗场景中。

3 医学影像联邦学习的研究现状

我们发现目前已经有很多联邦学习在医学图像方面的探索，本章将从联邦学习原始方法、基于算法的改进、基于框架的改进和基于隐私保护的改进几个方面对现有的研究进行详细阐述，所回顾的研究整体结构如图 3 所示。

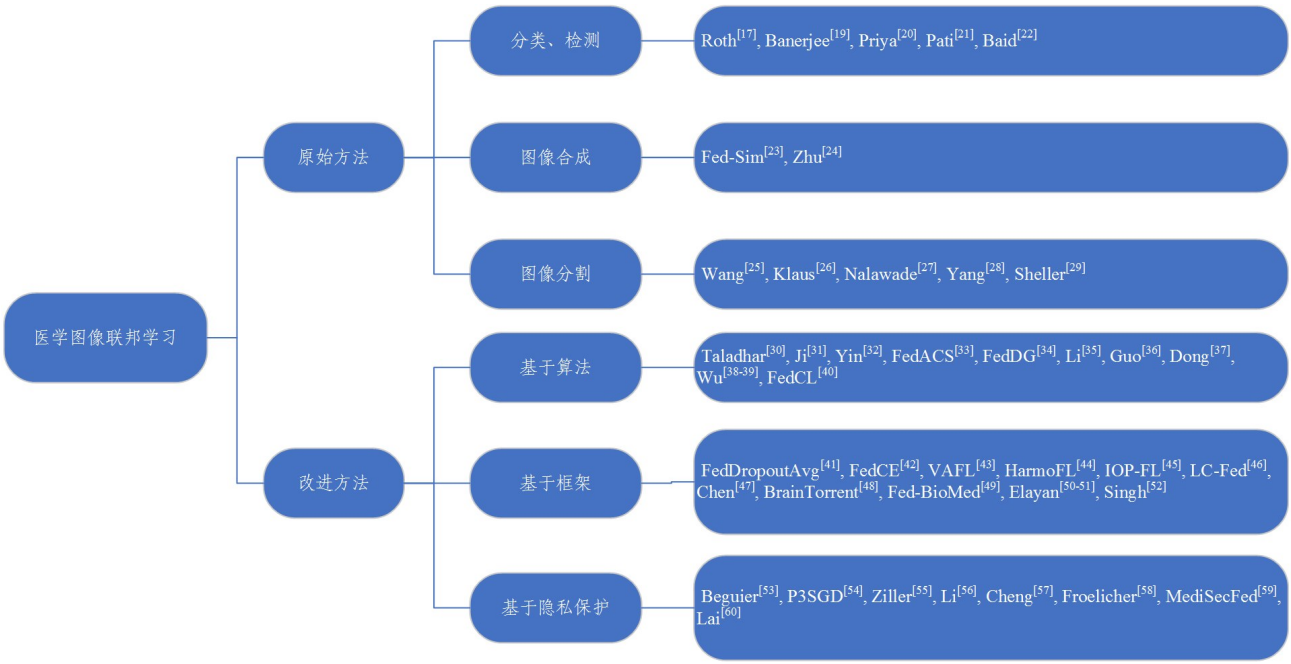


图 3 基于联邦学习的医学图像处理分类

Fig. 3 Classifications of medical image processing based on federated learning

3.1 原始方法

医学影像中最常见的应用是将联邦学习与传统的集中式数据分析方法在性能方面进行比较，或者使用联邦学习来应对面临的各种挑战(如领域偏移、标签缺失等)。下面将从几个具体的图像处理任务对这方面的工作进行介绍，该节涉及的参考文献在表 1 中汇总列出。

表 1 联邦学习在医学图像分析中的应用

Table 1 Application of federated learning in medical image analysis

任务类型	文献	目标任务	联邦框架	网络模型	对比方法	评价指标	定量结果（性能提升）	方法思想	存在问题
分类和病灶检测	Roth[17]	乳腺密度等级分类	FedAvg	DenseNet	单一机构数据训练	线性加权 Kappa	0.680（+0.040）	在非独立同分布的数据中实现联邦任务，模拟联邦学习的现实应用	数据之间的异质性并未解决，全局模型在本地数据的性能较差，同时也缺少隐私保护
	Banerjee[20]	肺炎分类检测	FedAvg	ResNet	集中训练	准确率（Accuracy）	0.983（+0.025）	采用预训练模型在联邦环境下使用迁移学习进行重新训练，并采取动量梯度下降进行参数更新	缺少对应的实验说明预训练和迁移学习的作用
	Priya[21]	胸部疾病多标签分类	—	DenseNet	CheXNet	准确率（Accuracy）	0.851（+0.097）	使用加权损失熵来平衡类不平衡问题	对单个数据集拆分后进行联邦训练，并未模拟现实情况中不同机构之间的数据异质性
	Pati[23]	胶质母细胞瘤检测	FedAvg	3D-ResUNet	公开训练模型	Dice 系数	0.832（+0.172）	通过大量不同的数据来进行医疗保健研究，确保对罕见疾病和代表性不足的人群有意义的结果，证明 FL 在复杂任务下的有效性	研究中缺少量化客户端对最终模型性能的贡献，单纯增大数据量并未给模型性能带来显著提升，反而因为部分低质量数据而出现性能的加入倒退
医学图像合成	Fed-Sim[24]	合成带标签的心脏 CT	—	Conditional GAN	SSM 随机生成形状	mIOU	0.789（+0.119）	将形状和材料的建模从成像传感器中抽象出来，以合成 CT 及其相应的标签，用作辅助标记数据集，训练下游机器学习模型	所提出的三维心脏模型表示能力有限，在参数设置上不够灵活，合成数据形状有一定局限性
	FedVSS[25]	虚拟图像合成	FedAvg	ResNet	FedAvg	准确率（Accuracy）	0.766（+0.041）	采用局部模型和全局模型相结合的方法合成虚拟训练样本，减轻了训练样本的异质性问题	将局部样本向全局模型对齐后，模型缺乏个性化，在特定站点机构的模型性能可能会下降
目标器官和病灶分割	Wang[26]	胰腺分割	—	C2FNAS	单一机构数据训练	Dice 系数	0.731（+0.128）	利用联邦学习框架处理客户端之间高度不平衡的数据分布，提供比独立训练更一般化的模型	不同机构数据集过于理想化，现实情况下不可能存在这样的划分
	Klaus[27]	前列腺分割	FedAvg	nnU-Net	集中训练	Dice 系数	0.906（+0.005）	通过在多站点前列腺分割数据集上进行内部和跨站点实验，创建了 nnU-Net 在多站点环境下应用的基准	没有解决类不平衡问题，模型性能提升不明显
	Nalawade[28]	脑肿瘤分割	—	ResUNet	—	Dice 系数	0.696	按照表现分配不同大小的权重，量化每个客户端的贡献	缺少与集中式学习等方法的对比，没有足够证据证明方法的先进性
	Pan[29]	颈椎 MRI 分割		改进 U-Net	其他模型	Dice 系数	86.86	通过标签分离对目标进行分割，同时实现多尺度输出	没有关注客户端与中心交互的安全性
	Yang[22]	肝脏肿瘤分割	FedAvg	MTANN	Res-U-Net 集中训练	Dice 系数	0.712（+0.059）	结合基于斑块的深度学习模型 MTANN 开发联邦框架	没有考虑到现实情况中的数据异构性问题
	Sheller[30]	脑肿瘤分割	—	U-Net	单一机构数据训练	Dice 系数	0.858（+0.126）	比较了不同的协作学习方法，证明了联邦学习的有效性	缺少对模型泛化性能的验证

3.1.1 分类和病灶检测

在几项研究中，联邦学习被用于图像的分类和病灶检测。Roth 等[17]使用来自 7 个客户端的数据集，研究在现实世界的协作环境中使用联邦学习进行乳房 X 光片 BI-RADS 分类，结果表明在数据之间存在差异的情况下使用联邦学习能得到泛化性更强的模型，但该方法没有研究数据分布差异对实验的影响，存在一定的类不平衡问题。Wei 等[19]在实际医学场景下进行了联邦学习的部署应用，验证了联邦学习在医学场景下进行图片分类进而诊断病症的可行性。Banerjee 等[20]使用迁移学习在胸部 X 光数据集上进行联邦训练，在肺炎的检测和分类任务中都取得了较好的效果。Priya 等[21]的研究则探究了从胸部 X 光中进行肺部多标签疾病分类的问题，同时分类预测多种慢性疾病，并使用了加权损失熵来平衡那些实例较少的疾病种类。Pati 等[23]利用来自七十多家医疗机构的数据进行胶质母细胞瘤检测，联邦学习使得初始的公共模型的性能得到了显著提升，也验证了罕见疾病和复杂任务下联邦学习的有效性，但研究中缺少客户端对模型性能提升的量化评价。

3.1.2 医学图像合成

由于医学图像获取难度较大且训练数据标记要求具备

一定的专业知识，目前已经有很多进行医学图像合成的研究，以此得到标记图像或扩充数据集，辅助完成进一步的分割等处理。Li 等[24]借助联邦学习获取不同机构数据的特征训练生成模型，生成图像加入训练有效缓解了数据分布偏差问题，但所提出的三维心脏模型生成在参数设置上不够灵活，合成数据形状有一定局限性。Zhu 等[25]同样通过训练联邦生成模型合成虚拟训练样本，以解决数据异构问题。

3.1.3 目标器官和病灶分割

为了帮助医生进行进一步诊断，医学图像处理更多的是分割目标器官或病灶。Wang 等[26]按照是否患有胰腺肿瘤对 CT 图像数据集进行划分以进行联邦训练，以验证数据收集标准不同的情况下联邦学习的有效性，实验结果表明联邦学习模型相较于单独训练模型具有更强的泛化能力，但这种数据集划分方式过于理想化，现实的联邦环境下几乎不可能存在。为了在临床环境中实现现实世界的联邦学习，Kades 等[27]扩展了已有的医学成像平台 Kaapana，使其能满足联邦学习通信要求并实现前列腺 MRI 分割，并在未参与训练的数据集上进行了泛化性验证，但由于没有控制通信成本和调整 nnU-Net 设置，分割精度提升十分有限。为了有效提升联邦模型性能，量化每个客户端的贡献，Nalawade 等[28]根据本地模型分割结果为每个合作者分配不同大小的权重，网络模型据此进行加权平均聚合，有助于较快取得更佳效果。Pan 等[29]利用联邦学习实现颈椎 MRI 图像的半监督分割，与基准模型相比准确性和鲁棒性均取得一定提升。

Yang 等[22]将联邦学习与基于图像块的 MTANN 网络结合进行 CT 肝脏肿瘤分割，使用随机采样的图像块使联邦学习实现了更好的隐私保护，重点关注了联邦学习与集中训练的时间及性能比较；而 Sheller 等[30]则比较了不同的协作学习方法，机构增量学习 IIL、循环机构增量学习 CIIL 会出现灾难性遗忘问题，联邦学习训练的模型则表现得更为稳定。

除了有常见医学图像处理用例外，联邦学习在数字切片和基因组图谱的应用也是研究热点。Baid 等[31]借助联邦学习框架对肿瘤全切片图像（WSI）进行浸润淋巴细胞检测，以帮助医生更好地进行免疫细胞治疗，具有极高的临床价值。

3.2 改进方法

到目前为止，我们关注的大部分工作都专注于借助联邦学习辅助进行研究任务，但也有很大一部分工作致力于对联邦学习进行改进，解决其目前面临的问题。本节将从基于算法的改进、基于框架的改进和基于隐私保护的改进 3 个方面对现有的相关研究进行详细阐述，涉及的文献方法如表 2 所列。

表 2 联邦学习在医学图像分析中的改进

Table 2 Improvements of federated learning in medical image analysis

改进方向	文献	目标任务	网络模型	对比方法	评价指标	定量结果（性能提升）	改进措施	存在的问题
基于算法的改进	Tuladhar[32]	脑肿瘤分割	3D-ResUNet	federated baseline	Dice 系数	0.674（+0.042）	调整学习率衰减策略、本地训练轮次和权重函数	手动调节参数的方法缺少鲁棒性，对于新的数据或任务需要重新调整
	Ji 等[33]	COVID-19 分类	FL-Resnet-CBAM	VGG16	准确率（Accuracy）	0.939（+0.082）	采用了混合注意力机制并引入局部模型的平均训练时间进行客户端选择	在提高安全性时会牺牲少量的准确性，方法有一定局限
	FedNorm[34]	脑肿瘤分割	nnU-Net	FedAvg	Dice 系数	0.743（+0.032）	设计张量归一化法来解决异构性，还提出客户端修剪策略以缓解培训时间不均匀对收敛时间的负面影响	设计的客户端选择策略降低了较难训练的数据对模型性能的贡献，并未考虑到模型处理复杂样本的能力
	FedACS[35]	胸部 X 光分类	ResNet	FedAvg	准确率（Accuracy）	0.745（+0.011）	提出了一种自适应客户端抽样算法，将课程学习策略应用于联邦学习	在新的数据集上及站点加入和退出时如何调整训练顺序并未得到解决
	FedDG[61]	眼底图像分割	ELCFS	FedAvg	Dice 系数	0.870（+0.020）	通过连续频率空间插值机制，在保护隐私的情况下在客户端之间传输分布信息，解决联邦域泛化问题	在进行振幅分量替换时如何选择阈值有待进一步研究
	Li[36]	fMRI 分类	MoE	FedAvg	准确率（Accuracy）	0.742（+0.008）	基于检测到的生物标志物来衡量模型性能，并制定了隐私保护和领域自适应机制	在不同站点的实验参数设置没有统一，使得模型性能提升较小
	FL-MR[38]	磁共振图像重建	U-Net	FedAvg	SSIM	0.911（+0.013）	设计了类似 GAN 生成器结构的特征提取网络实现特征交互	生成的数据未进行约束，由于 GAN 的机制可能导致数据无效
	FedMoCo[39]	COVID-19 检测	ResNet	FedAvg	准确率（Accuracy）	0.916（+0.120）		
	Wu 等[40]	皮肤病诊断	MoCo	FedSimCLR	召回率（Recall）	0.592（+0.006）	引入对比学习在保证隐私安全的前提下进行节点之间的特征交互	共享特性需要额外的通信，因此如何降低通信成本，保障隐私安全仍需要进一步探索
	Wu 等[41]	心脏 MRI 分割	U-Net	FedSimCLR	Dice 系数	0.894（+0.035）		
	Liu 等[42]	皮肤病分类	—	FedAvg	准确率（Accuracy）	0.892（+0.013）		

（续表）

改进方向	文献	目标任务	网络模型	对比方法	评价指标	定量结果（性能提升）	改进措施	存在的问题
基于框架的改进	Gunesli[43]	结肠肿瘤检测	ResNet18	FedAvg	F1 分数	0.910（+0.014）	提出 FedDropoutAvg 框架，采用神经网络中常用的 Dropout 机制减轻异构数据集学习的复杂性	没有检查所提出方法的隐私限制，也没有考虑模型反转攻击时模型参数的数据泄漏。
	FedCE[44]	视网膜眼底图像分割	—	FedAvg	Dice 系数	0.831（+0.048）	估计客户在梯度和数据空间中的贡献，通过贡献估计进行联邦训练同时优化两种类型的公平性	目前的应用范围存在一定限制，对具有噪声数据及对抗性的客户端的性能提升仍需进一步研究
	VAFL[45]	前列腺分割	PPWGAN-GP	FedAvg	准确率（Accuracy）	0.972（+0.009）	通过将所有客户端的图像转换到公共图像空间来最小化客户端之间的差异	CycleGAN 对数据配对程度要求较高，医学图像往往较难满足这一条件
	HarmoFL[46]	前列腺 MRI 分割	—	FedAvg	Dice 系数	0.943（+0.029）	引入 HarmoFL 协调框架，专注于处理本地和全局偏移。提出通过图像频域振幅的归一化来模拟统一的成像设置，从而在客户端之间生成协调的特征空间	权重扰动程度超参数的选择缺少鲁棒性，对不同数据需要进行相应的调整
	IOP-FL[47]	前列腺 MRI 分割	U-Net	FedDG	Dice 系数	0.893（+0.018）	使用轻量级的基于梯度的联邦框架，通过积累全局梯度和特定于客户端的局部梯度，为每个客户端生成个性化模型	将模型转移到未见过的客户端进行个性化建模。另外，模型共享过程引入了额外的通信成本
	FedLC[48]	前列腺 MRI 分割	—	FedAvg	IoU	0.842（+0.033）	通过个性化通道选择和头部校准，微调局部训练过程中的特征表示和预测	由于分割图缺乏测量预测级别不一致性的能力，头部校准模块的改进较小
	PRR-FL[49]	皮肤病诊断	PFA+DET	FedAvg	F1 分数	0.708（+0.192）	提出了一个个性化的倒退弹性框架，为每个客户端产生一个个性化模型	—
	Brain-Torrent[50]	脑 MRI 分割	DNN	FLS	Dice 系数	0.851（+0.079）	提出了一个去中心化的联邦框架，减少了中心服务器对联邦训练的影响	去中心化没有共同信赖的中心服务器，客户端之间的信任机制和通信成本仍是一大挑战
	Fed-BioMed[51]	脑成像数据分类	—	—	—	—	提出了一个基于通用架构的开源联邦学习前端框架，可以容纳不同的模型和优化方法	实验关注点集中在参数的演化和模型运行时间方面，缺少对性能提升的定量评价
	Elayan[52-53]	皮肤病检测	—	FedAvg	准确率（Accuracy）	0.974（+0.005）	提出了一个深度 FL 框架，用于使用物联网设备进行医疗保健数据监控和分析。此外，还对本地服务器数据采集进行了策略优化	整个联邦训练过程的通信成本增加，对底层硬件提出了更高的要求
	Singh[54]	—	sensor network	—	—	—	提出了用于智能医疗保健中的隐私保护的区块链和联邦学习安全架构，其中基于区块链的物联网云平台用于安全和隐私	所提出的模型仅限于理论模型，应用于实时区块链将由于额外的延迟而影响性能
基于隐私保护的改进	Beguier[55]	癌症预测	—	隐私预算超参数修改	准确率（Accuracy）	0.995（+0.060）	基于 DP-SGD 设计隐私保护，在准确性和隐私性之间保持了良好的平衡	隐私预算超参数的调整不具备鲁棒性
	P3SGD[56]	肾小球分类	ResNet18	SGD	准确率（Accuracy）	0.953（+0.021）	引入了一种新的 SGD 模式——P3SGD，以规范深度 CNN 的训练，同时在差分隐私内提供严格的隐私保护	—
	deepee[57]	肝脏分割	VGG-11	单一机构数据训练	Dice 系数	0.950（+0.007）	提供了在包含与差分隐私随机梯度下降不兼容的层的情况下自动修改神经网络结构的能力，有效避免了默认伪随机数生成器的相关漏洞	在保证严格的数据隐私时对模型性能牺牲较大，没有达到一个可接受的平衡
	Li 等[58]	脑肿瘤分割	DNN	FedAvg	Dice 系数	0.850（+0.044）	应用微分隐私技术保护患者信息	对隐私成本的分配较为保守
	Zhu 等[59]	多标签心电图诊断	—	FedAvg	F1 分数	0.875（+0.041）	通过实时 ECG 分析设计一种深度学习方法，用于心律或传导异常的自动多标签诊断	由于缺乏患者样本，一些类型的节律性和传导性心律失常未包括在内

（续表）

改进方向	文献	目标任务	网络模型	对比方法	评价指标	定量结果（性能提升）	改进措施	存在的问题
	FAMHE[60]	HIV-1 感染患者的宿主遗传研究	—	—	—	—	基于多方同态加密，以加密的形式实现中间结果的安全聚合，提供更严格的隐私保护	选择适合高维输出分析（如 GWAS）的 diffP 参数可能具有挑战性，需要进一步探索
基于隐私保护的改进	MediSecFed[62]	COVID-19 检测	—	单一机构数据训练	准确率（Accuracy）	0.742（+0.063）	依靠知识蒸馏和模型反演的思想来确保额外的安全和隐私保护	模型性能相比 FedAvg 较差
	Lai 等[63]	COVID-19 检测	ResNet18	FedAvg	准确率（Accuracy）	0.857（−0.024）	提出了一种轻量级的联邦学习方法，在联邦训练过程中，模型的参数不需要传输，本地客户端只上传每一类特征向量的平均值	由于减少了参数上传，模型性能受到了一定影响

3.2.1 基于算法的改进

深度学习中最常见的算法改进通常是对训练过程中的参数及模型进行调整，联邦学习中也是如此。Tuladhar 等[32]对学习率衰减策略、本地训练轮次和权重函数分别进行了探究，选出了最佳的组合方式，最大程度地提升了肿瘤分割准确性。

在现有的联邦学习中，参与每一轮训练的客户端数量一般是固定的。在实际应用中，受限于现实条件，联邦学习往往只是随机选择一部分客户端参与。但当一些客户端数据质量和计算、通信能力较差时，会对全局模型的训练效率和效果产生较大影响。为了寻找更合适的客户端选择方法，Ji 等[33]在联邦学习中采用了混合注意力机制并引入局部模型的平均训练时间进行客户端选择，解决了局部模型长时间不收敛导致全局模型无法收敛的问题，提高了模型训练的准确性和快速性。类似地，Yin 等[34]以每个客户端上一轮的训练和通信时间作为依据，对一些较慢的客户端进行自适应过滤，但是这样的客户端选择策略降低了较难训练的数据对模型性能的贡献，并未考虑到模型处理复杂样本的能力。Gu 等[35]提出了一种自适应客户端采样算法，创造性地将课程学习策略应用到联邦学习中，模仿人类学习过程让模型从易到难学习，训练前期选择简单数据加快收敛，随着训练轮次的增加引入训练难度较大的数据，较好地实现了训练速度和模型精度的平衡。

除了客户端选择问题，数据异构性也是联邦学习的一大挑战。不同设备采集的医学图像很难满足独立同分布的条件，为了缓解数据分布差异对联邦训练的影响，Liu 等[61]将图像进行傅里叶变换后对幅度谱进行插值合成，从生成数据中学习来自其他客户端的图像特征，实现领域泛化。Li 等[36]使用混合专家系统在保证全局模型性能良好的同时可以针对特定的数据集进行处理，另外引入了对抗性对齐的思想，设计了类似 GAN[37]的结构以实现领域自适应。Guo 等[38]同样设计了类似 GAN 生成器结构的特征提取网络，在保护原始数据的基础上实现不同客户端之间的特征交互，使得模型更好地适应不同数据分布。

还有一部分研究则考虑对比学习方法，通过拉近数据分布学习中的共同特征来缓解异构性难题。考虑单个客户端内样本较单一导致对比学习受限，一些研究[39-41]在保护数据隐私的前提下建立全局特征库，提供来自不同客户端的对比数据以进行更有效的对比学习，在不同客户端之间寻找统一的特征空间。特别地，Liu 等[42]将对比学习思想应用到了模型更新而非数据交互中，将局部模型和全局模型相结合进行对比学习，使局部模型随着交流次数的增加逐渐接近全局模型，提高了模型的泛化能力。

3.2.2 基于框架的改进

联邦学习中不同客户端间的公平性一直是一个重要课题。原始方法中客户端选择趋于随机，且在中央服务器进行参数聚合时往往依据不同客户端的数据集大小进行加权，预先固定权重很难对不同客户端进行合理的贡献估计。Gunesli 等[43]提出了 FedDropoutAvg 框架用于检测结肠组织切片图像中的肿瘤，引入神经网络中解决模型过拟合的 dropout 原理给客户端选择和参数聚合引入额外的随机性，而不是基于数据大小预先确定模型贡献权重，以减轻从不同客户端的不平衡和异构数据集学习的复杂性。Jiang 等[44]则设计了贡献估计联邦学习（FedCE），在梯度空间中监测每个客户端相对于其他客户端的梯度方向差异，在数据空间中则使用辅助模型测量客户数据的预测误差，将每个客户在梯度和数据空间的贡献估计作为全局模型聚合的权重值。

另外，全局模型为了提高泛化性经过了不同客户端参数的聚合，由于不同客户端数据的异构性，在特定的某一客户端上，全局模型较局部模型而言性能可能较差。为了解决这一问题，Yan 等[45]提出了一个变化感知联邦学习（VAFL）框架，通过将所有客户端的图像转换到公共图像空间来最小化客户端之间的差异。首先选择一个具有最低数据复杂度的客户端来定义目标图像空间，并通过被称为 PPWGAN-GP 的隐私保护生成对抗网络合成图像集合。然后，自动从这些合成图像中选择一个子集与其他客户端共享，该子集有效地捕获了原始图像的特征，并且与任何原始图像都有足够的区别。对于每个客户端，应用修改后的 CycleGAN 将其原始图像转换为由共享合成图像定义的目标图像空间，以实现不同客户端之间的数据分布对齐。Jiang 等[46]引入了一个新的 HarmoFL 协调框架，专注于处理本地和全局偏移。他们提出通过图像频域振幅的归一化来模拟统一的成像设置，从而在客户端之间生成协调的特征空间。

为了提升联邦学习针对特定客户端数据的性能，另一个思路是为每个客户端制定个性化策略。Jiang 等[47]使用一种轻量级的基于梯度的联邦框架，通过积累全局梯度和特定于客户端的局部梯度，为每个客户端生成局部适应模型。此外，重要的是，获得的局部个性化模型和全局模型可以形成多样化和

信息丰富的分布空间，为外部客户端定制自适应模型。Wang等[48]提出了一个带有局部校准的个性化联邦框架(LC-Fed)，以利用特征级别和预测级别的客户端间的不一致性来提高分割性能。一方面设计了对比学习和通道选择来校准编码特征，另一方面利用一致性预测水平的知识来指导对不明确区域(如解剖边界)的个性化建模，在多种医学图像分割任务中实现了更好的性能。Chen等[49]针对这种全局模型性能倒退现象提出了一个个性化的倒退弹性框架，在全局服务器端设计了渐进式傅里叶聚合(PFA)，通过将客户端模型从低频逐步集成到高频，实现了更稳定有效的全局知识收集。此外，通过引入代理模型来接收聚合的服务器模型，在客户端设计了代理增强转移(DET)策略，并通过恢复-交换-升华三步操作，通过全局知识的平滑转移来改进个性化的局部模型。

传统联邦学习框架依赖于中央服务器进行全局模型的聚合，这需要所有客户端信任一个中心机构，当该服务器出现问题时，所有客户端的训练过程将被破坏。Roy等[51]针对医疗应用提出了一个去中心化的联邦框架，称之为BrainTorrent，该框架将全局服务器从传统的联邦学习范例中移除，取而代之的是允许客户端直接相互通信它们的权重。该框架在全脑分割任务上进行了测试，效果优于使用全局服务器的传统联邦学习。

还有一些研究则针对医疗联邦学习产业落地。现有的联邦学习框架不能提供直接部署应用的环境，为了解决这一问题，Silva等[51]提出了一个开源的联邦学习前端框架，并在脑部图像进行了实际的应用测试。实验主要使用了VAE和联邦平均两种聚合方式，提出的框架完全可以扩展到其他的方法和任务中。而随着智能手机及平板等终端计算能力和成像水平的显著提高，移动医疗平台和可穿戴医疗设备的应用范围越来越广。Elayan等[52-53]提出了一个基于物联网的皮肤疾病检测分类联邦学习框架，进一步在这个联邦学习框架中利用迁移学习来规避对大量标记数据的需求。Singh等[54]为物联网医疗设备提供了一种基于区块链的分布式联邦学习架构，在物联网设备中训练机器学习模型，为手持医疗设备等提供技术支持。

3.2.3 基于隐私保护的改进

虽然联邦学习能够在不进行数据传输的前提下完成模型的协作训练，但它本身不能完全保证安全性和隐私性，其加密程度较低，容易导致攻击者从权重中反推出客户端数据，从而窃取节点隐私信息和干扰通信过程，因此需要借助隐私保护技术。目前联邦学习研究中常用的隐私保护技术主要是差分隐私和同态加密。

差分隐私是一种基于扰动的隐私保护方法，主要针对信息模糊，通过加入噪声使第三方无法根据输出的变化判断单个数据的更改或增删，从而达到隐私保护的目的。Beguier等[55]在两个客户端的联邦学习设置中实现了差分隐私随机梯度下降训练，并对隐私和准确性之间的权衡进行了广泛的研究。他们在准确性和隐私性之间取得了可接受的平衡，并对肿瘤基因分类实验进行了测试。Wu等[56]也通过在随机梯度下降的每次更新中按一定策略加入噪声，实现了基于差分隐私的数据保护，在临床数据集上的实验证明了训练的模型不仅能有效保护隐私，还能降低过拟合风险并抵抗模型逆向攻击。Ziller等[57]的研究支持加密安全的随机噪声生成，并提供了在包含与差分隐私随机梯度下降不兼容的层的情况下自动修改神经网络结构的能力，有效避免了默认伪随机数生成器的相关漏洞。Li等[58]在差分隐私保护的同时对局部网络模型权重只进行部分共享，进一步保证了数据的安全。

同态加密是一种特殊的加密方案，它允许任何第三方对加密数据进行操作，而无需事先对其进行解密。Cheng等[59]将区块链技术、同态加密技术和联合学习技术相结合，使用Paillier同态加密算法有效解决隐私问题。Froelicher等[60]基于多方同态加密，以加密的形式实现中间结果的安全聚合，提供更严格的隐私保护。

此外，还有不少学者在研究中借助其他方法来加强联邦学习中的隐私保护。Kumar等[62]利用知识蒸馏和模型反演的思想来确保数据安全，提出的方法实现了参与客户端之间的知识交换，而不是像之前一样共享模型参数，从而保护了本地数据对服务器的隐私性，并显著降低了通信成本。Lai等[63]展示了一种使用隐私保护层来防止访问中间模型权重的方法，攻击者也无法得到权重来反演出客户端的数据分布。

4 面临的挑战与未来研究方向

4.1 存在问题

由于医疗数据非常敏感，因此数据隐私成为在医疗保健中开发数据驱动模型的关键设置。联邦学习已经证明了数据隐私在支持医疗图像分布式学习设置方面的潜在用途。虽然联邦学习的研究已经十分广泛，但客户端异构性、通信效率和数据隐私仍然是非常具有挑战性和开放性的问题。

4.1.1 异构性问题

在联邦学习系统中，一个主要的问题就是客户端的异构性。由于不同客户端的设备条件不同，因此在进行数据存储、网络训练和联邦通信时存在异构性。

首先，由于设备和成像协议不同，医生标注手法也不同，不同医疗机构的同种数据在分布上也存在异质性，很难满足独立同分布的理想条件，这导致通过某些医疗机构的数据训练得到模型很难在其他医疗机构的数据上取得可靠的结果。其次，由于医学图像较难获取且医院并没有专业的网络训练设备，因此不同客户端数据集大小和硬件条件不统一。在参与训练时，每个客户端所用的时间不同，甚至个别客户端模型无法收敛，增大了全局模型训练难度。另外，在客户端和服务器交互时也会因为网络条件差异而产生异构性问题。

4.1.2 通信效率

机器学习算法，特别是复杂的深度学习算法，在训练的过程中需要训练大量的参数，联邦学习模型每一次更新可能需要传递上百万个参数；其次，网络通信的状态也可能导致通信成本很高，例如不稳定的网络情况、参数上传和下载的过程中速度不一致都会导致整个算法的模型训练成本过高。

4.1.3 隐私和安全

联邦学习可以在不直接获取数据源的基础上，通过客户端本地训练上传权重参数得到协作训练的全局模型，是一种高效的隐私保护技术，但仅靠联邦学习并不能保证数据的

绝对安全。此外,客户端的异构性加剧了隐私泄露的风险,当入侵者得到客户端的权重时,能直接通过分析其模型梯度来推断隐私信息。

4.1.4 技术限制

虽然大多数研究主要集中在算法设计上,但联邦学习在实际部署时往往会遇到较大的技术障碍。例如某些算法需要大量的计算资源,对医疗机构的底层硬件设施提出了挑战。另外,在医疗机构加入和退出联邦训练时,如何保证其数据安全也需要新的技术支持。

4.1.5 长期可行性

联邦学习不仅是一种新颖的机器学习方法,也是现实应用中的一种系统工程方法。在应用于医学图像分析时,必须关注联邦学习的长期可行性。在现实场景中,会出现不可预见的挑战,如何保证联邦学习的可扩展性、泛化性,适应不断发展的法律法规以及稳定地进行医学图像分析是一项较为复杂的工作。

4.2 可能的研究方向

4.2.1 解决异构性

解决异构性难题的一种有效的方法是优化客户端选择策略。我们注意到,每轮全局训练的响应延迟是由最慢的客户端决定的,在传统联邦学习随机选择客户端的策略下,当参与训练的客户端数量增加时,选中较慢的客户端的概率相当高,这大大增加了通信成本和复杂度。目前已经有一些关于医学图像联邦学习中的客户端选择策略的研究,但怎样平衡选择方法和模型性能仍需进一步探索。

医学图像的异构性还会使全局模型过于"平均",其针对某一客户端的性能比局部模型要差一些。为了解决这种性能倒退问题,可进行个性化的联邦学习,通过增加上下文、迁移学习、混合全局和局部模型或本地额外训练等方法为每个客户端生成在本地医学图像数据上表现更好的网络模型,将联邦学习方法推广到特定的局部数据分布中。

4.2.2 提高通信效率

提高通信效率需要考虑两个方面:减少交互轮次或者减少每轮传递信息量。同步交互能保证串行计算模型,但在不同的医疗机构间很难实现。异步交互策略可以减少等待时间,有效提高训练效率。

4.2.3 加强隐私保护

隐私保护在联邦学习中扮演着关键角色。虽然客户端通过不共享本地数据来维护隐私,但由于模型和梯度更新的记忆,以及信息反馈等原因,私有信息仍可能泄漏。针对这些问题,已有研究提出了差分隐私等隐私保护技术。然而,在实际异构场景中,不同客户端或数据样本的隐私关注各异,需要建立更严格、灵活的隐私约束策略。另一个挑战是处理医学图像数据时的隐私问题,如原始数据匿名化和特征保护。现有框架虽然采取了数据保持本地策略,但仍无法完全防止数据访问和分析。

4.2.4 增强泛化能力

由于医学图像数据分布的异质性,当联邦模型面对未参与训练的客户端数据时,不一定能获得理想的效果。尤其在医疗图像领域,域偏移问题更为严重。为了增强联邦学习领域泛化能力,可以考虑通过拉近不同域分布的距离或者引入目标客户端数据特征来提升联邦模型性能。

4.2.5 保证公平性

在现实世界中,参与协作学习的客户端对合作的贡献可能存在差异,并且这种差异可能因异构性而增大。同时,现有的联邦学习框架大多忽略了参与客户端在协作过程中的贡献差异。也可能会存在一些"搭便车"参与者,他们希望从联邦通信中学习而不贡献有用信息。此外,通过联邦训练获得的全局模型可能偏向数据量大或频繁出现的客户端,并且整体损失函数可能会对某些客户不利。因此,随着联邦学习在更多医疗机构中的实际部署,对公平性的研究也是不可缺少的。

结束语 本文全面回顾了近年来联邦学习在医学图像方向的最新进展,将基于联邦学习的医学图像处理研究分为3类:基于算法的改进、基于联邦框架的改进和基于隐私保护技术的改进,针对方法提升和解决的问题进行了阐述和分析。此外,本文还讨论了联邦学习面临的一些挑战,并提出了未来医学图像处理任务可能的研究方向和提升空间。当然联邦学习与智慧医疗的结合仍处于快速发展阶段,希望本文的总结和探讨能给相关研究人员提供一定的参考和帮助。

参 考 文 献

[1] KRIZHEVSKY A,SUTSKEVER I,HINTON G. ImageNet Classification with Deep Convolutional Neural Networks [J]. Communications of the ACM,2017,60(6):84-90.

[2] SIMONYAN K,ZISSERMAN A. Very Deep Convolutional Networks for Large-Scale Image Recognition [J]. arXiv: 1409.1556,2014.

[3] HE K,ZHANG X,REN S,et al. Deep Residual Learning for Image Recognition [C]// 2016 IEEE Conference on Computer Vision and Pattern Recognition. 2016.

[4] VASWANI A,SHAZEER N,PARMAR N,et al. Attention Is All You Need[C]// Proceedings of the 31st International Conference on Neural Information Processing Systems. 2017:6000-6010.

[5] DOSOVITSKIY A,BEYER L,KOLESNIKOV A,et al. An Image is Worth 16x16 Words:Transformers for Image Recognition at Scale [J]. arXiv:2010.11929,2020.

[6] DENG J,DONG W,SOCHER R,et al. ImageNet:A large-scale hierarchical image database [C]// 2009 IEEE Conference on Computer Vision and Pattern Recognition. 2009:248-255.

[7] KRIZHEVSKY A. Learning Multiple Layers of Features from Tiny Images[J/OL]. https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf.

[8] ZHOU B,ZHAO H,PUIG X,et al. Semantic Understanding of Scenes Through the ADE20K Dataset [J]. International Journal of Computer Vision,2016,127:302-321.

[9] LIU T,SIEGEL E,SHEN D. Deep Learning and Medical Image Analysis for COVID-19 Diagnosis and Prediction [J]. Annual review of biomedical engineering,2022,24:179-201.

[10] QIU Z,XU T,LANGERMAN J,et al. A Deep Learning Approach for Segmentation,Classification,and Visualization of 3-D High-Frequency Ultrasound Images of Mouse Embryos [J].

IEEE Transactions on Ultrasonics, Ferroelectrics, and Frequency Control, 2021, 68: 2460-2471.

[11] TALEB A, LIPPERT C, KLEIN T, et al. Multimodal Self-Supervised Learning for Medical Image Analysis [C]// Information Processing in Medical Imaging. 2019.

[12] ZHU W, LIAO H, LI W, et al. Alleviating the Incompatibility between Cross Entropy Loss and Episode Training for Few-shot Skin Disease Classification [C]// International Conference on Medical Image Computing and Computer-Assisted Intervention. 2020.

[13] KIRILLOV A, MINTUN E, RAVI N, et al. Segment Anything [J]. arXiv: 2304. 02643, 2023.

[14] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-Efficient Learning of Deep Networks from Decentralized Data [C]// International Conference on Artificial Intelligence and Statistics. 2016.

[15] LIU Y, FAN T, CHEN T, et al. FATE: An Industrial Grade Platform for Collaborative Learning With Data Protection [J]. The Journal of Machine Learning Research, 2021, 22(1): 10320-10325.

[16] ZILLER A, TRASK A, LOPARDO A, et al. PySyft: A Library for Easy Federated Learning [M]// Federated Learning Systems. 2021: 111-139.

[17] ROTH H R, CHANG K, SINGH P, et al. Federated Learning for Breast Density Classification: A Real-World Implementation [C]// DART/DCL@MICCAI. 2020.

[18] JU C, ZHAO R, SUN J, et al. Privacy-Preserving Technology to Help Millions of People: Federated Prediction Model for Stroke Prevention [J]. arXiv: 2006. 10517, 2020.

[19] WEI Z Y, TANG Y, TENG Z, et al. Artificial intelligence federated learning system based on chest X-ray films for pathogen diagnosis of community-acquired pneumonia in children[J]. Chinese Journal of Interventional Imaging and Therapy, 2024, 21(6): 368-373.

[20] BANERJEE S, MISRA R, PRASAD M, et al. Multi-diseases Classification from Chest-X-ray: A Federated Deep Learning Approach [C]// Australasian Conference on Artificial Intelligence. 2020.

[21] PRIYA K V, PETER J D. A federated approach for detecting the chest diseases using DenseNet for multi-label classification [J]. Complex & Intelligent Systems, 2021, 8: 3121-3129.

[22] YANG Y, JIN Z, SUZUKI K. Federated Tumor Segmentation with Patch-Wise Deep Learning Model [C]// MLMI@MICCAI. 2022.

[23] PATI S, BAID U, EDWARDS B, et al. Federated learning enables big data for rare cancer boundary detection [J]. arXiv: 2204. 10836, 2022.

[24] LI D, KAR A, RAVIKUMAR N, et al. Fed-Sim: Federated Simulation for Medical Imaging [J]. arXiv: 2009. 00668, 2020.

[25] ZHU W, LUO J. Federated Medical Image Analysis with Virtual Sample Synthesis [C]// International Conference on Medical Image Computing and Computer-Assisted Intervention. 2022.

[26] WANG P, SHEN C, ROTH H R, et al. Automated Pancreas Segmentation Using Multi-institutional Collaborative Deep Learning [J]. arXiv: 2009. 13148, 2020.

[27] KADES K, SCHERER J, ZENK M, et al. Towards Real-World Federated Learning in Medical Image Analysis Using Kaapana [C]// DeCaF/FAIR@MICCAI. 2022.

[28] NALAWADE S, GANESH C, WAGNER B C, et al. Federated Learning for Brain Tumor Segmentation Using MRI and Transformers [C]// BrainLes@MICCAI. 2021.

[29] PAN E Y, ZHONG Y, LI P. Semi-Supervised Cervical Spine MRI Segmentation Model in Federated Heterogeneous Data[J]. Computer Engineering, 2024, 50(9): 367-376.

[30] SHELLER M J, EDWARDS B, REINA G A, et al. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data[J/OL]. https://www.nature.com/articles/s41598-020-69250-1.pdf.

[31] BAID U, PATI S, KURÇ T M, et al. Federated Learning for the Classification of Tumor Infiltrating Lymphocytes [J]. arXiv: 2203. 16622, 2022.

[32] TULADHAR A, TYAGI L, SOUZA R, et al. Federated Learning Using Variable Local Training for Brain Tumor Segmentation [C]// BrainLes@MICCAI. 2021.

[33] JI C, CHENG B, GAO Z, et al. COVID-19 Classification Algorithm Based on Privacy Preserving Federated Learning [C]// International Conference on Pervasive Computing Technologies for Healthcare. 2022.

[34] YIN Y, YANG H, LIU Q, et al. Efficient Federated Tumor Segmentation via Normalized Tensor Aggregation and Client Pruning [C]// BrainLes@MICCAI. 2021.

[35] GU Y, HU Q, WANG X, et al. FedACS: an Efficient Federated Learning Method Among Multiple Medical Institutions with Adaptive Client Sampling [C]// 2021 14th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics(CISP-BMEI). 2021: 1-6.

[36] LI X, GU Y, DVORNEK N C, et al. Multi-site fMRI Analysis Using Privacy-preserving Federated Learning and Domain Adaptation: ABIDE Results [J]. Medical image analysis, 2020, 65: 101765.

[37] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks [J]. Commun ACM, 2020, 63(11): 139-144.

[38] GUO P, WANG P, ZHOU J, et al. Multi-institutional Collaborations for Improving Deep Learning-based Magnetic Resonance Image Reconstruction Using Federated Learning [C]// 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition(CVPR). 2021: 2423-2432.

[39] DONG N, VOICULESCU I. Federated Contrastive Learning for Decentralized Unlabeled Medical Images [J]. arXiv: 2109. 07504, 2021.

[40] WU Y, ZENG D, WANG Z, et al. Federated Contrastive Learning for Dermatological Disease Diagnosis via On-device Learning [J]. arXiv: 2202. 07470, 2022.

[41] WU Y, ZENG D, WANG Z, et al. Federated Contrastive Learning for Volumetric Medical Image Segmentation [C]// International Conference on Medical Image Computing and Computer-Assisted Intervention. 2022.

[42] LIU Z, WU F, WANG Y, et al. FedCL: Federated contrastive learning for multi-center medical image classification [J]. Pattern Recognition, 2023, 143: 109739.

[43] GUNESLI G N, BILAL M, RAZA S E A, et al. A Federated Learning Approach to Tumor Detection in Colon Histology Images [J]. Journal of Medical Systems, 2023, 47: 1-15.

[44] JIANG M, ROTH H R, LI W, et al. Fair Federated Medical Image Segmentation via Client Contribution Estimation [C]// 2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2023: 16302-16311.

[45] YAN Z, WICAKSANA J, WANG Z, et al. Variation-Aware Federated Learning With Multi-Source Decentralized Medical Image Data [J]. IEEE Journal of Biomedical and Health Informatics, 2020, 25: 2615-2628.

[46] JIANG M, WANG Z, DOU Q. HarmoFL: Harmonizing Local and Global Drifts in Federated Learning on Heterogeneous Medical Images [C]// AAAI Conference on Artificial Intelligence. 2021.

[47] JIANG M, YANG H, CHENG C, et al. IOP-FL: Inside-Outside Personalization for Federated Medical Image Segmentation [J]. IEEE Transactions on Medical Imaging, 2022, 42: 2106-2117.

[48] WANG J, JIN Y, WANG L. Personalizing Federated Medical Image Segmentation via Local Calibration [C]// European Conference on Computer Vision. 2022.

[49] CHEN Z, ZHU M, YANG C, et al. Personalized Retrogress-Resilient Framework for Real-World Medical Federated Learning [C]// International Conference on Medical Image Computing and Computer-Assisted Intervention. 2021.

[50] ROY A G, SIDDIQUI S, PöLSTERL S, et al. BrainTorrent: A Peer-to-Peer Environment for Decentralized Federated Learning [J]. arXiv: 1905.06731, 2019.

[51] SILVA S, ALTMANN A, GUTMAN B, et al. Fed-BioMed: A General Open-Source Frontend Framework for Federated Learning in Healthcare [C]// DART/DCL@MICCAI. 2020.

[52] ELAYAN H, ALOQAILY M, GUIZANI M. Deep Federated Learning for IoT-based Decentralized Healthcare Systems [C]// 2021 International Wireless Communications and Mobile Computing (IWCMC). 2021: 105-109.

[53] ELAYAN H, ALOQAILY M, GUIZANI M. Sustainability of Healthcare Data Analysis IoT-Based Systems Using Deep Federated Learning [J]. IEEE Internet of Things Journal, 2021, 9: 7338-7346.

[54] SINGH S, RATHORE S, ALFARRAJ O, et al. A framework for privacy-preservation of IoT healthcare data using Federated Learning and blockchain technology [J]. Future Generation Computer Systems, 2021, 129: 380-388.

[55] BÉGUIER C, TERRAIL J O D, MEAH I, et al. Differentially Private Federated Learning for Cancer Prediction [J]. arXiv: 2101.02997, 2021.

[56] WU B, ZHAO S, SUN G, et al. P3SGD: Patient Privacy Preserving SGD for Regularizing Deep CNNs in Pathological Image Classification [C]// 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019: 2094-2103.

[57] ZILLER A, USYNIN D, BRAREN R F, et al. Medical imaging deep learning with differential privacy [J]. Scientific Reports, 2021, 11: 13524.

[58] LI W, MILLETARì F, XU D, et al. Privacy-preserving Federated Brain Tumour Segmentation [C]// MLMI@MICCAI. 2019.

[59] CHENG W H, OU W, YIN X D, et al. A Privacy-Protection Model for Patients [J]. Security and Communication Networks, 2020, 2020: 1-12.

[60] FROELICHER D, TRONCOSO-PASTORIZA J R, RAISARO J L, et al. Truly privacy-preserving federated analytics for precision medicine with multiparty homomorphic encryption [J]. Nature Communications, 2021, 12: 5910.

[61] LIU Q, CHEN C, QIN J, et al. FedDG: Federated Domain Generalization on Medical Image Segmentation via Episodic Learning in Continuous Frequency Space [C]// 2021 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2021: 1013-1023.

[62] KUMAR A, PUROHIT V, BHARTI V, et al. MediSecFed: Private and Secure Medical Image Classification in the Presence of Malicious Clients [J]. IEEE Transactions on Industrial Informatics, 2022, 18: 5648-5657.

[63] LAI W L, YAN Q. Federated Learning for Detecting COVID-19 in Chest CT Images: A Lightweight Federated Learning Approach [C]// 2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC). 2022: 146-149.

LIU Yuming, born in 1999, postgraduate, is a member of CCF (No. R7056G). His main research interests include federated learning and image segmentation.

DAI Yu, born in 1981, professor, is a member of CCF (No. L4837M). His main research interests include image processing and intelligent technology for surgical robot.

(责任编辑:何杨)